개인정보 보호 인증(PIPL) 안내서

2013. 11.

NIA 한국정보화진흥원

편집상 비워둔 페이지입니다.

1 개인정보 보호 인증 개요

2 개인정보 보호 인증절차

3 개인정보 보호 인증 심사기준

< 개인정보 보호 관리체계 구축 >

< 개인정보 보호대책 구현 >

제1장 개인정보 보호 인증 개요

제1절 제도개요

1.1 도입배경

❍ 「개인정보 보호법」은 개인정보의 무분별한 수집과 이용, 오·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 규정하기 위해 2011년에 제정되었다.

❍ 「개인정보 보호법」 시행이후 국민들의 개인정보 보호에 대한 인식과 관심은 크게 높아졌지만, 이에 비해 개인정보를 관리하는 기업이나 기관들의 개인정보 보호수준은 상대적으로 낮은 수준에 머물러 있다.

❍ 350만개에 달하는 개인정보처리자를 일일이 규제하고 단속하기에는 한계가 있으므로, 개인정보 보호에 대한 일회성 관리가 아닌 개인정보처리자 스스로 체계적이고 지속적인 유지관리 활동을 촉진할 수 있는 제도의 마련이 필요하였다.

❍ 이에, 「개인정보 보호 인증(PIPL)」 제도를 통하여 개인정보처리자에게는 개인정보 보호 활동의 기준을 제시하여 자율적으로 일정 수준이상의 개인정보 보호가 가능하도록 하고, 정보주체에게는 본인의 개인정보가 안전하게 관리되고 있음을 인식할 수 있는 기준을 제공하게 되었다.

개인정보 보호 인증제의 법률적 근거
📖 「**개인정보 보호법**」 **제13조(자율규제의 촉진 및 지원)** 안전행정부장관은 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하고 지원하기 위하여 다음 각 호의 필요한 시책을 마련하여야 한다. **3. 개인정보 보호 인증마크의 도입·시행 지원** 📖 「**개인정보 보호 인증제 운영에 관한 규정**」 <안전행정부고시 제2013-45호>

1.2 개념

❍ ‘개인정보 보호’는 개인정보 보호 관리체계의 수립, 개인정보 처리단계별 기준·절차의 준수 및 안전한 관리, 정보주체의 권리보장 등을 지속적으로 수행하는 일련의 조치와 활동을 말한다.

❍ 「개인정보 보호 인증(PIPL)」은 「개인정보 보호법」의 도입 취지에 따라 개인정보처리자의 개인정보 보호 관리체계 구축 및 개인정보 보호조치 사항을 이행하고 일정한 보호수준을 갖춘 경우 인증마크를 부여하는 제도이다.

- 개인정보 보호 인증의 적용대상은 업무를 목적으로 개인정보를 처리하는 공공기관, 민간기업, 법인, 단체 및 개인 등 모든 공공기관 및 민간 개인정보처리자를 대상으로 한다.

※ PIPL : Personal Information Protection Level

<참고> 해외의 개인정보 보호 인증제도 현황

❍ 영국은 2009년 「데이터보호 - 개인정보 관리체계 규격(BS10012)」을 제정하였으며, 개인정보 관리체계의 수립 및 이행, 관리활동에 대한 감사 및 경영검토 등 총 6개 분야로 구성된 심사항목을 기준으로 인증을 실시하고 있다.

※ BS10012 : Data protection - Specification for a personal information management system

❍ 일본은 「개인정보에 관한 컴플라이언스(Compliance) 프로그램의 요구사항(JIS Q 15001)」을 제정하고, 개인정보의 적절한 보호를 위한 체제를 정비하고 있는지 여부를 심사하여 프라이버시마크(P-Mark)를 부여하는 제도로 민간기업에 활성화되어 있다.

1.3 기대효과

❍ 개인정보 보호 인증과정을 통해 개인정보 보호 관련 법령에서 요구하는 기준을 기관 내부에서 준수하는지 여부를 점검하고, 조직 내부 구성원에게 개인정보 보호에 대한 중요성을 전파하고, 인식 및 역량을 제고할 수 있다.

❍ 지속적이고 체계적인 개인정보 보호 활동을 수행함에 따라 개인정보취급자의 부주의, 안전성 확보조치 미흡 등으로 발생할 수 있는 개인정보 침해 가능성을 최소화할 수 있다.

❍ 또한, 개인정보 보호 인증을 통해 부여받은 인증마크를 활용하여 국민 및 고객의 개인정보 보호에 대한 신뢰성을 높여 인증취득기관의 대외 이미지를 제고할 수 있다.

1.4 인증취득기관에 대한 혜택

❍ 인증취득기관에게 「개인정보 보호법」에 따라 실시하는 기획점검 대상 제외 또는 실시 유예, 행정처분 감경 등의 혜택이 있다.

❍ 또한, 개인정보 보호 우수기관 포상, 개인정보 보호 인증 관련 교육기회 및 정보제공, 행사 참여기회 제공 등의 혜택을 받을 수 있다.

「개인정보 보호 인증제 운영에 관한 규정」에 따른 근거
제28조(인증취득기관의 혜택) ① 안전행정부장관은 인증취득기관에게 「개인정보 보호법」에 따라 실시하는 기획점검 대상 제외 또는 실시 유예, 행정처분 감경 등의 혜택을 줄 수 있다. ② 안전행정부장관은 인증취득기관에게 개인정보 보호 우수기관 포상, 개인정보 보호 인증 관련 교육기회 및 정보제공, 행사 참여기회 제공 등의 혜택을 줄 수 있다.

1.5 책임 및 한계

❍ 개인정보 보호 인증제도는 인증 신청기관이 결정한 인증 대상범위에 대해 인증심사 시점에서 인증기준 부합여부를 심사하는 것으로서 인증을 취득한 이후라도 개인정보와 관련된 어떠한 침해나 유출사고가 발생하지 않는다는 것을 담보하는 것은 아니다.

※ 인증심사는 인증기준 및 법률 요구사항을 준수하기 위해 신청기관 스스로 구축한 개인정보 보호 관리체계의 적절성, 보호대책 구현에 대한 이행현황을 샘플링 기법으로 점검하는 과정

1.6 용어정의

❍ 개인정보 보호

- 개인정보 보호 관리체계의 수립·운영, 개인정보 처리단계별 기준·절차의 준수 및 안전한 관리, 정보주체의 권리보장 등을 지속적으로 수행하는 일련의 조치와 활동을 말한다.

❍ 개인정보 보호 인증

- 신청기관의 개인정보 보호를 위한 일련의 조치와 활동이 인증심사기준에 부합하다고 승인하는 것을 말한다.

❍ 개인정보처리자

- 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

❍ 인증기관

- 신청기관에 대한 인증심사 및 인증 등 개인정보 보호 인증제도의 운영을 전담하는 기관을 말한다. 「개인정보 보호 인증제 운영에 관한 규정」(이하 「인증제 고시」라 한다) 제3조제1항에 따라 인증기관은 한국정보화진흥원으로 지정되어 있다.

❍ 개인정보 보호 인증위원회

- 인증기관이 실시한 인증심사의 적정성 및 인증심사 실시 결과보고서 등에 관한 사항을 심의·의결하기 위해 「인증제 고시」 제5조제1항에 따라 인증기관에서 설치한 위원회를 말한다. (이하 “인증위원회”라 한다.)

❍ 인증취득기관

- 신청기관 중 인증심사를 통과하여 인증을 부여받은 기관으로, 인증서가 유효한 기관을 말한다.

❍ 신청기관

- 인증을 받고자 인증심사를 신청한 개인정보처리자를 말한다. 신청기관의 유형은 공공기관, 대기업, 중소기업, 소상공인으로 구분된다.

❍ 인증심사

- 개인정보 보호 인증심사기준에 부합하는지의 여부를 확인·판단하는 일련의 과정과 활동을 말한다.

❍ 유지관리심사

- 인증취득기관이 인증 유효기간 중 인증심사 기준을 유지하는지 여부에 대해 연 1회 이상 받아야 하는 심사를 말한다.

❍ 갱신심사

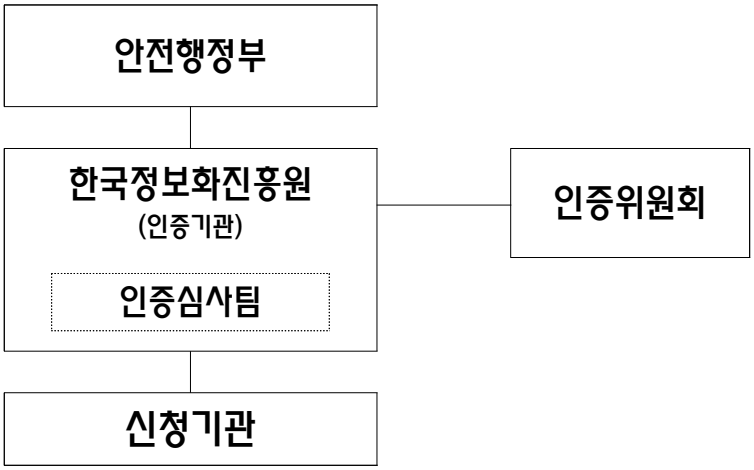
- 인증취득기관이 인증 유효기간의 만료 90일 전에 인증기관에 인증의 갱신을 신청한 심사를 말한다.

❍ 변경심사

- 인증취득기관이 신규 시스템을 도입하는 등 인증대상의 범위가 확대 또는 축소되거나, 개인정보 보호 관리체계가 변경되는 등의 사유가 발생한 경우 신청하는 심사로, 변경심사로 인증을 취득한 경우 인증의 유효기간은 인증서 변경발급일로부터 3년이 된다.

제2절 추진체계

□ 인증체계

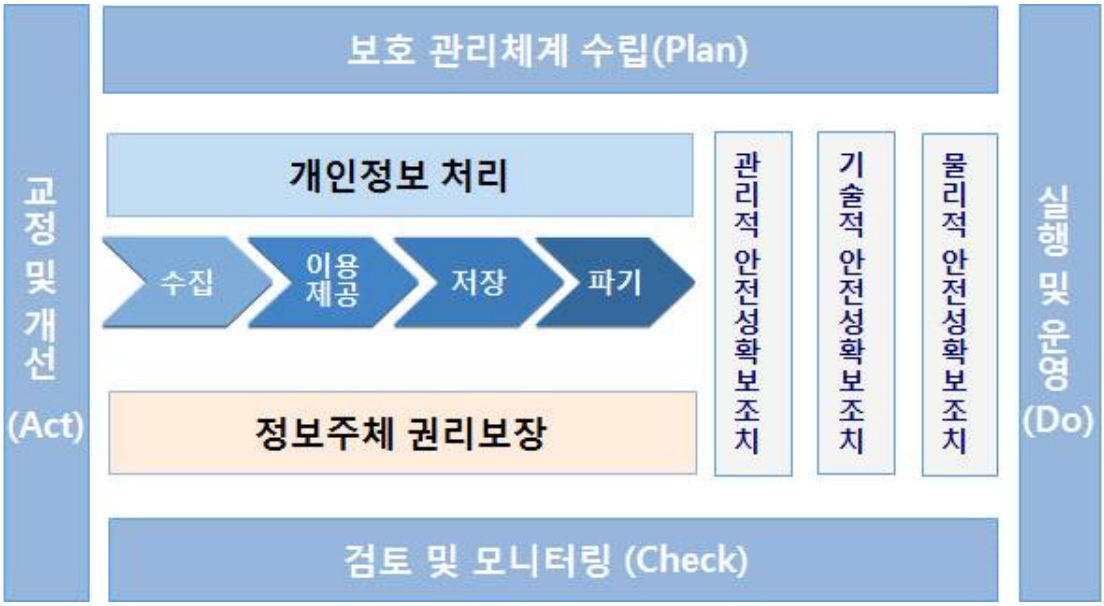


□ 기관별 책임 및 역할

담당기관	책임 및 역할
안전행정부	ㅇ 인증 관련 법·제도 개선 및 정책 결정
한국정보화진흥원 (인증기관)	ㅇ 인증심사 신청 접수 ㅇ 인증심사의 실시 ㅇ 인증위원회의 구성·운영 ㅇ 인증 부여 및 인증마크 발급 ㅇ 인증심사원 양성 및 관리 ㅇ 인증심사팀 구성·운영 ㅇ 인증 심사기준 및 지침개발 등
인증위원회	ㅇ 인증심사 결과 심의·의결 ㅇ 이의신청 사항에 대한 심의·의결 ㅇ 인증 취소에 대한 심의·의결 등
인증심사팀	ㅇ 인증심사 실시 ㅇ 인증심사 실시 결과보고서 작성
신청기관	ㅇ 개인정보 보호 관리체계 구축·운영 ㅇ 인증심사 신청 ㅇ 인증 취득 및 유지관리 등

제3절 인증 프레임워크

❍ 인증심사기준은 크게 '개인정보 보호 관리체계' 분야와 '개인정보 보호대책' 분야로 구성되어 있다.



<개인정보 보호 인증 프레임워크>

- '개인정보 보호 관리체계' 분야는 PDCA(Plan-Do-Check-Act)의 관점에서 '보호 관리체계의 수립(Plan),' '실행 및 운영(Do)', '검토 및 모니터링(Check)' 그리고 '교정 및 개선(Act)'으로 심사영역이 구성되어 있다.
- '개인정보 보호대책' 분야는 '관리적, 기술적, 물리적 안전성 확보조치' 등과 같은 보호조치뿐만 아니라 법적으로 요구되는 '개인정보의 처리', '정보주체 권리보장'등에 대한 항목을 포함하여 심사영역이 구성되어 있다.

분야	개인정보 보호 관리체계	개인정보 보호대책
심사영역	ㅇ 보호 관리체계 수립 ㅇ 실행 및 운영 ㅇ 검토 및 모니터링 ㅇ 교정 및 개선	ㅇ 개인정보 처리 ㅇ 정보주체 권리보장 ㅇ 관리적 안전성 확보조치 ㅇ 기술적 안전성 확보조치 ㅇ 물리적 안전성 확보조치

❍ 인증심사기준은 심사영역, 심사목적, 심사항목으로 구성되어 있다.

- 심사영역, 심사목적, 심사항목은 「인증제 고시」의 [별표 1] 개인정보 보호 인증심사 기준에 정의되어 있다.

구분	설명	비고
심사영역	ㅇ 필수적인 요구사항이거나 개인정보 보호를 위한 기초적인 구성 요소이며, 개인정보처리자가 개인정보 보호 요구사항을 구현하는데 기반이 됨	9개
심사목적	ㅇ 개인정보처리자가 개인정보 보호체계 수립을 위해 달성되어야 하는 목표 ㅇ 한 개 또는 그 이상의 심사항목이 적용될 수 있음	26개
심사항목	ㅇ 심사목적을 만족하기 위한 정의된 요구사항	65개

제4절 인증심사대상

4.1 신청기관의 범위

❍ 「개인정보 보호법」 제13조에 따라 개인정보 보호 인증제가 시행되면서 「개인정보 보호법」에 적용되는 모든 개인정보처리자(공공기관, 민간기업, 법인, 단체 및 개인)는 신청기관이 될 수 있다.

- 다만, 「인증제 고시」 제8조에서는 인증을 취득하고자 하는 개인정보처리자는 공공기관, 대기업, 중소기업, 소상공인 중 신청기관에 해당하는 유형의 인증을 신청할 수 있다.

유 형	관련근거
공공기관	「개인정보 보호법」 제2조제6호에 따른 공공기관에 해당하는 개인정보처리자
대기업	「대.중소기업 상생협력 촉진에 관한 법률」 제2조제2호에 따른 대기업에 해당하는 개인정보처리자
중소기업	「중소기업기본법」제2조에 따른 중소기업에 해당하는 개인정보처리자
소상공인	「소기업 및 소상공인 지원을 위한 특별조치법」제2조제2호에 따른 소상공인에 해당하는 개인정보처리자 및 그 밖의 개인정보처리자

❍ 공공기관, 대기업, 중소기업 및 소상공인에 대한 범위는 아래와 같으며, 구체적인 범위는 해당 법률을 참조하여 확인한다.

- **(공공기관)** 「개인정보 보호법」 및 동법 시행령에서 공공기관의 범위를 정하고 있으며, 아래의 표와 같다.

「개인정보 보호법」에 따른 공공기관
ㅇ 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관 ㅇ 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관 포함) 및 그 소속 기관 ㅇ 지방자치단체 ㅇ 「국가인권위원회법」 제3조에 따른 국가인권위원회 ㅇ 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관 ㅇ 「지방공기업법」에 따른 지방공사 및 지방공단 ㅇ 특별법에 따라 설립된 특수법인 ㅇ 「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 각 급 학교

- **(대기업)** 「대·중소기업 상생협력 촉진에 관한 법률」 제2조제2호에 따라 '중소기업이 아닌 기업'을 말한다.
- **(중소기업)** 「중소기업기본법」 제2조에 따른 중소기업의 범위를 만족하는 기업을 말한다.

「중소기업법」 상의 중소기업
ㅇ 아래의 요건을 모두 갖추고 영리를 목적으로 사업을 하는 기업 1. 업종별로 상시 근로자 수, 자본금, 매출액 또는 자산총액 등이 대통령령으로 정하는 기준에 맞을 것 2. 지분 소유나 출자 관계 등 소유와 경영의 실질적인 독립성이 대통령령으로 정하는 기준에 맞을 것
ㅇ 「사회적 기업 육성법」 제2조제1호에 따른 사회적 기업 중에서 대통령령으로 정하는 사회적 기업
ㅇ 중소기업이 그 규모의 확대 등으로 중소기업에 해당하지 아니하게 된 경우 그 사유가 발생한 연도의 다음 연도부터 3년이 초과되지 않은 기업 - 다만, 중소기업 외의 기업과 합병하거나 그 밖에 대통령령으로 정하는 사유로 중소기업에 해당하지 아니하게 된 경우는 제외됨.

- **(소상공인)** 「소기업 및 소상공인 지원을 위한 특별조치법」 제2조제2호에 따른 소상공인의 범위

「소기업 및 소상공인 지원을 위한 특별조치법」상의 소상공인
ㅇ 소기업 중 상시 근로자가 10명 미만인 사업자로서 아래의 기준에 해당하는 자 1. 광업·제조업·건설업 및 운수업의 경우에는 10인 미만 2. 제1호외의 업종의 경우에는 5인 미만

4.2 신청기관 유형별 심사기준

❍ 인증심사기준은 신청기관 유형별(공공기관, 대기업, 중소기업, 소상공인)로 적용하도록 「인증제 고시」의 [별표 1] 개인정보 보호 인증심사 기준에 제시되어 있다.

- 다만, 「인증제 고시」에서는 편의상 공공기관과 대기업을 하나의 유형으로 구분하여 인증심사항목을 구분하였으나, 인증 심사항목 중에는 '개인정보 파일관리', '개인정보 영향평가' 등 공공기관을 대상으로 한 제도적 측면에서의 요구사항은 대기업에는 필수 심사항목으로 적용하지 않는 것으로 하였다.

유형	적용기준	항목수
공공기관 대기업	ㅇ 개인정보 보호법 기반의 법적 요구사항 ㅇ 개인정보 보호체계(관리체계) 수립 및 이행 ㅇ 개인정보 흐름분석을 통한 위험분석 및 위험관리 ㅇ 경영진 참여 및 의사결정 ㅇ 개인정보 보호 강화를 위한 보호대책	65
중소기업	ㅇ 개인정보 보호법 기반의 법적 요구사항 ㅇ 개인정보 보호체계(관리체계) 수립 및 이행 ㅇ 개인정보 보호 강화를 위한 보호대책	52
소상공인	ㅇ 개인정보 보호법 기반의 법적 요구사항	33

❍ 신청기관 유형별로 심사항목 자체에 차이가 있는 것은 아니며, 심사항목의 적용 유무로 구분되어 있다. 신청기관 유형별 인증심사 기준은 아래와 같다.

분야	심사영역	심사내용	심사항목	유형별 심사항목		
				공공기관 대기업	중소기업	소상공인
개인정보 보호 관리체계	1. 보호 관리체계의 수립	ㅇ 개인정보 보호 관리계획 수립, 개인정보 보호 조직 구축, 경영진의 책임부여	5	5	3	-
	2. 실행 및 운영	ㅇ 보호체계의 문서화, 개인정보자산 식별, 위험관리방안 수립 및 보호대책 이행	6	6	3	-

분야	심사영역	심사내용	심사 항목	유형별 심사항목		
				공공기관 대기업	중소기업	소상공인
	3. 검토 및 모니터링	○ 개인정보 보호 관리계획과 보호체계 이행간의 일치 여부 검토	2	2	-	-
	4. 교정 및 개선	○ 주기적인 개선활동 여부 및 각종 개인정보 보호 관리계획의 공유 상황 검토	2	2	2	-
	소계		15	15	8	-
개인정보 보호 대책	5. 개인정보 처리	○ 개인정보 처리단계별 보호조치 여부	14	14	13	12
	6. 정보주체 권리보장	○ 정보주체의 열람, 정정, 삭제, 처리정지 요구 등의 처리	3	3	3	3
	7. 관리적 안전성 확보 조치	○ CPO 지정, 개인정보 보호 교육 및 훈련 실시, 위탁업무 관리현황, 유출사고 대응 절차 마련	10	10	10	8
	8. 기술적 안전성 확보 조치	○ 접근권한 및 접속기록관리, 암호화 적용여부 등	16	16	13	7
	9. 물리적 안전성 확보 조치	○ CCTV 설치 및 운영, 출입통제장치의 구비 등	7	7	5	3
	소계		50	50	44	33
합계			**65**	**65**	**52**	**33**

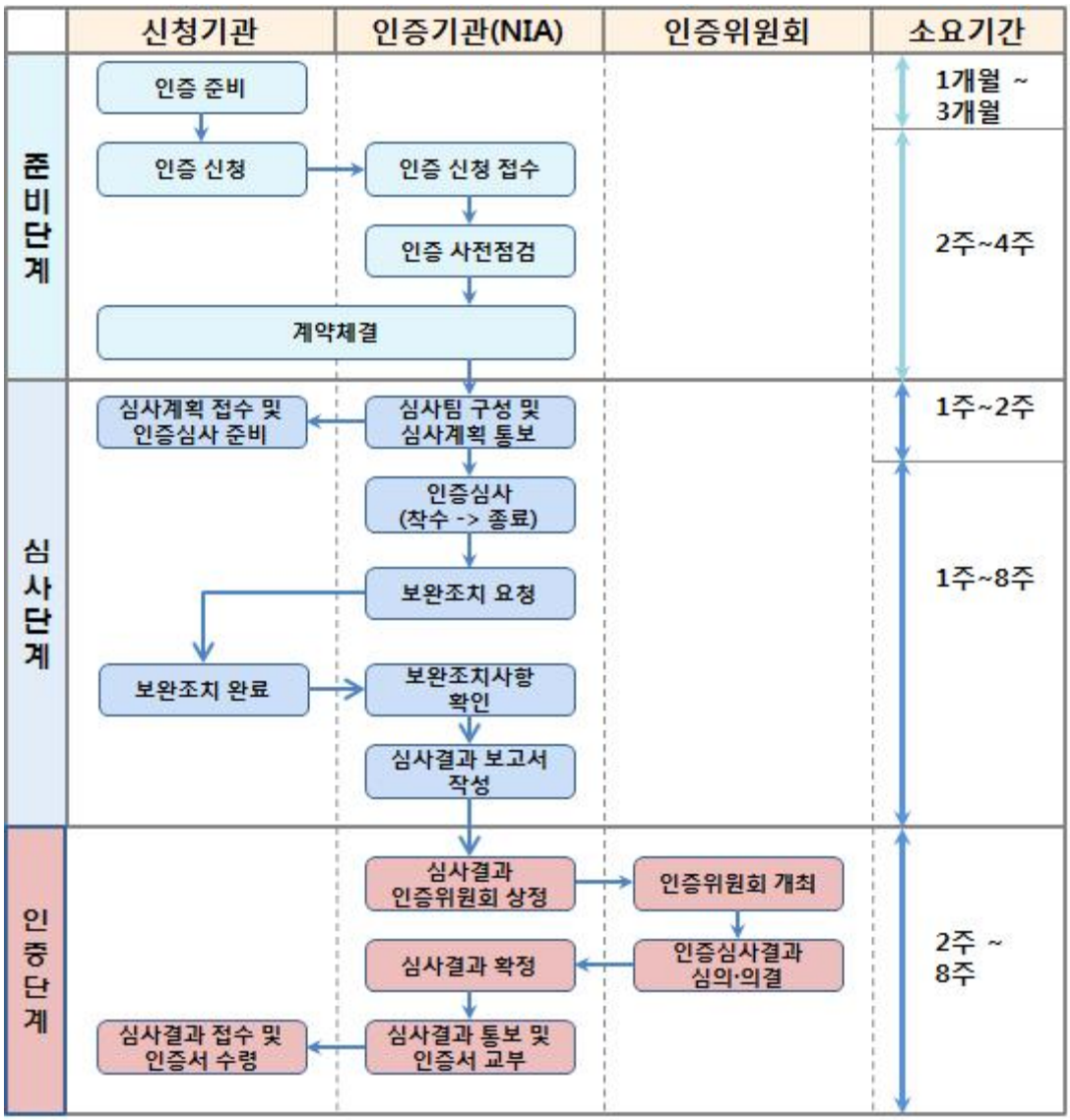
❍ 인증기관은 신청기관과 협의하여 개인정보 처리규모, 업무특성 등을 고려하여 인증심사항목을 추가 또는 조정할 수 있다.

※ 인증기준은 신청기관에 해당되는 유형에 따라 결정되며 신청기관의 의사에 따라 유형을 선택하는 것은 아니다.

제2장 개인정보 보호 인증절차

제1절 인증심사 절차

❍ 개인정보 보호 인증절차는 인증심사 준비단계, 심사단계, 인증단계로 구성되며, 인증유지관리를 위한 유지관리단계가 있다.



< 단계별 인증심사 절차 >

제2절 단계별 세부절차

2.1 준비단계

❍ 준비단계는 인증심사를 위해 사전에 준비하는 단계이다.

- 신청기관은 인증심사 준비를 완료하여 인증기관에 인증신청을 하고, 인증기관은 신청기관의 인증준비 상태를 사전에 점검하여 인증심사 준비여부를 확인한 후에 계약을 체결하게 된다.

□ 인증 준비

❍ 신청기관은 기관의 개인정보 처리 현황을 파악하여 인증대상 범위를 설정해야 한다.

❍ 신청기관은 인증대상 범위에 대해 개인정보 보호 관리체계를 구축하고, 보호 관리체계에 따라 보호대책을 수립하여 일정기간(3개월) 이상 이행실적을 관리하여야 한다.

※ 소상공인이나 이행실적 및 증적자료의 준비가 완료된 기관은 3개월 이내에도 신청이 가능

❍ 신청기관은 관련 법령 및 인증심사기준에 부합하는 개인정보 보호 관리계획, 개인정보 자산목록, 위험평가보고서, 내부감사보고서 등의 인증심사관련 문서를 작성하여야 한다.

□ 인증 신청

❍ 인증을 취득하고자 하는 기관은 신청기관의 유형(공공기관, 대기업, 중소기업, 소상공인)에 맞게 인증심사를 신청할 수 있다.

- 인증심사를 신청하고자 하는 신청기관은 공식적인 문서로 인증신청서[별지 제1호 서식]와 인증심사에 관련된 인증신청 내역서[별지 제2호 서식]를 제출해야 한다.

❍ 인증 신청기관은 인증범위의 대상을 기관·기업·사업부문 전체 또는 특정 서비스·업무로 구분하여 신청할 수 있다.

- 특정 서비스·업무로 신청하는 경우 인증범위 내의 개인정보 흐름 및 연결 관계를 고려하여 명확하게 구분지어 범위를 지정할 수 있다.

❍ 신청서류를 접수한 인증기관은 접수증[별지 제3호 서식]을 신청기관에 교부한다. 인증기관은 신청기관이 제출한 신청 서류를 검토하여 누락한 서류가 있는 경우 보완을 요청할 수 있다.

- 신청기관은 보완 요청이 있을 경우 빠른 시일 안에 이를 보완하여 신청서류를 재구비하여 제출해야 한다.

□ 사전 점검

❍ 인증기관은 신청기관이 제출한 인증신청서 및 관련 서류를 검토하고 인증심사 실시 전 심사수행에 문제가 없는지를 점검한다. 이때 인증기관은 신청기관에게 다음의 사항을 요청할 수 있다.

- 인증심사를 위한 관련 문서 및 증거자료 등의 열람제공을 요청할 수 있다.
- 인증심사를 수행하기 위하여 필요한 장소·시설·장비·기자재 등의 확보를 요청할 수 있다.
- 그 밖에 신청기관은 인증심사를 원활하게 수행하기 위하여 인증기관이 요구하는 사항에 대해서 최대한 협조해야 한다.

❍ 인증기관은 신청기관의 준비가 미흡하여 인증심사를 정상적으로 진행할 수 없는 경우에 이를 보완할 것을 요구할 수 있으며, 신청기관은 인증기관의 요구사항에 맞게 준비해야 한다.

□ 계약 체결 및 수수료 산정

❍ 인증기관은 신청기관이 제출한 신청서 및 관련 서류를 검토하고 신청기관의 인증심사 준비현황을 파악한 후 인증심사 계약[별지 제

4호 서식]을 체결한다.

- 인증심사에 필요한 인증심사의 기간·장소, 인증심사원의 수, 인증심사 수수료(이하 “수수료”이라 한다), 그밖에 인증에 필요한 사항을 인증기관과 신청기관 간에 협의하여 인증심사 계약을 체결한다.

❍ 인증심사 수수료는 직접인건비, 직접경비, 기술료, 제경비를 고려하여 산정한다.

인증심사 수수료 = 직접인건비 + 직접경비 + 기술료 + 제경비

- 직접인건비는 인증심사에 투입되는 인증심사원에 대한 인건비로 산정한다.

직접인건비 = 심사원 등급 단가 × 투입공수

- 투입공수 산정은 다음과 같다.

투입공수 = (개인정보처리시스템 수에 따른 투입공수 + 개인정보취급자 수에 따른 투입공수 + 위탁기관 수에 따른 투입공수 + 정보주체 수에 따른 투입공수) × (1 + 가중치)

- 직접경비는 인증심사업무의 수행에 따라 발생하는 교통비, 숙박비 및 식대 등 심사업무에 소요되는 직접적인 경비를 산정한다.
- 기술료는 최대 (직접인건비 + 제경비) × 20% 로 산정한다.
- 제경비는 최대 직접인건비 × 110% 로 산정한다.

※ 상세내용은 [별표 1] 인증심사 수수료 산정기준 참조

❍ 인증심사 수수료 산정에 있어 개인정보 보호 우수기관, 영세사업자 등의 경우에는 수수료를 감경할 수 있다.

- 수수료 감경의 대상 및 기준은 인증기관의 장이 별도로 정하고 있다.

❍ 신청기관은 인증심사 계약을 체결한 날로부터 5일 이내에 수수료를 인증기관에 납부하여야 한다. 다만, 신청기관은 천재지변 등

불가피한 사유가 있는 때에는 수수료 납부 시기를 인증기관과 협의하여 조정할 수 있다.

2.2 심사단계

❍ 인증 심사단계에서는 인증심사팀 구성 및 심사계획 통보, 인증심사 수행, 보완조치 요청 등이 심사단계에 포함된다.

□ 인증심사팀의 구성 및 심사계획 통보

❍ 인증기관은 인증심사 수행을 위하여 인증심사원 관리대장에 등재된 인력으로 인증심사팀을 구성·운영한다.

- 신청기관의 소속직원 또는 신청기관의 인증취득을 위하여 신청기관에 자문·기술지원 등을 제공한 인증심사원은 인증심사팀의 구성원이 될 수 없다.

❍ 인증기관은 신청기관이 수수료를 납부한 날로부터 15일 이내에 인증심사 실시계획서[별지 제5호 서식]를 신청기관에 통보한다.

- 인증기관의 심사팀장은 심사계획에 인증심사팀 구성, 심사 일정, 심사 시 준비사항 등을 포함한 계획을 수립한다.

❍ 신청기관은 인증심사 계획을 전달 받고 인증심사의 원활한 진행을 위하여 심사와 관련된 제반사항을 준비해야 한다.

- 신청기관은 인증심사팀의 인증심사 수행을 위한 적절한 장소와 관련 문서 및 증빙자료 등을 준비하고 면담 예정자에게 인증심사 기간 중에 협조할 수 있는 등의 조치를 취해야 한다.

□ 착수회의

❍ 착수회의 시 신청기관은 인증범위 내의 개인정보 보호 구축현황 및 운영 내역에 대해 설명을 해야 하고 인증기관이 추가적으로 요청하는 자료나 세부 설명자료를 제출해야 한다.

❍ 인증기관은 인증제에 대한 소개와 인증심사의 진행 과정에 대해 간략하게 설명하고 인증대상 범위에 대해 설명을 한다.

□ 인증심사

❍ 인증심사는 신청기관에 대한 서면심사와 현장심사로 이루어진다.

- 서면심사는 신청기관의 제출서류를 확인하여 개인정보 보호 인증심사기준에 부합하는지를 심사한다.
- 현장심사는 서면심사의 결과를 검증하기 위하여 신청기관이 운영 중인 개인정보 보호 관리체계 및 보호대책의 구현 현장을 방문하거나 시스템 등의 실사를 통해서 서면심사 결과와의 일치 여부를 확인하고 개인정보 보호 인증심사기준에 부합하는지 여부를 심사한다.
- 서면심사와 현장심사는 인증심사원이 제출된 서류를 통해서 서면심사를 하고, 현장실사를 반영한 현장심사를 통하여 상호보완적으로 심사를 수행한다.

□ 부적합 보고서 작성

❍ 인증심사팀은 심사 진행 중에 발견된 문제점 및 개선해야 할 사항에 대하여 확인 및 증빙 자료를 확보하고 부적합 사항을 검토하고 심사팀 내부에서 부적합 사항을 정리해야 한다.

- 다음과 같은 문제점이 발견되었을 때 부적합 사항으로 지적할 수 있다.
  ① 개인정보 보호대책 중 선택한 유형에 맞게 보호대책을 적절히 시행하지 않는 경우
  ② 개인정보 보호 관리체계 산출물의 일관성이 부족한 경우
  ③ 개인정보 보호 관리체계 산출물의 추적성이 부족한 경우
  ④ 기타 심사팀이 개인정보 보호 관리체계에 부적합 사항이 있다고 판단한 경우

❍ 신청기관은 부적합 보고서[별지 제6호 서식] 검토를 위해 심사기간 동안에 발견된 문제점 및 개선해야 할 사항 등 보고서 내용의 적정성에 대해 인증기관과 상호 협의해야 한다.

- 신청기관은 심사팀이 잘못 이해하고 있거나 사실과 다르게 기술되어 있는지 검토하고 부적합 사항에 대해 증빙할 수 있는 자료를 제출하여 부적합 사항에 대해 이의를 제기할 수 있다.

□ 종료회의 및 보완조치 요청

❍ 인증심사팀은 신청기관을 대상으로 인증심사에 대한 결과를 정리하는 공식적인 종료회의를 수행한다.

- 인증심사팀은 인증심사 결과에 대한 부적합 사항 및 개선 권고사항을 설명하고 신청기관의 개인정보 보호 관리체계에 대한 운영현황 및 심사이후 일정계획을 설명한다.
- 심사종료 이후 심사팀은 신청기관이 제출한 자료를 모두 반납하고 심사원의 전산장비(노트북 등)에서 인증심사와 관련된 모든 자료를 삭제한다.

❍ 인증기관은 인증심사 과정에서 발견한 부적합 사항이 보완조치가 필요하다고 판단될 때에는 보완요청서[별지 제7호 서식]에 따라 신청기관에 보완조치를 요청할 수 있다.

- 신청기관은 요청받은 날로부터 30일 이내 보완조치를 완료하고 그 보완조치 내역서[별지 제8호 서식] 및 증빙자료를 제출한다.
- 인증기관은 보완조치 결과를 확인하기 위하여 신청기관에 방문하여 현장을 확인할 수 있으며 보완조치 결과를 확인한 때에는 보완조치 내역확인서[별지 제9호 서식]에 신청기관 담당자와 인증심사팀장이 서로 서명하여 이를 인증기관에 제출한다.

□ 심사의 중단

❍ 인증기관은 인증심사를 실시하면서 다음의 사유가 발생한 경우에는 인증심사를 중단할 수 있다.

① 신청기관이 고의로 인증심사의 실시를 지연 또는 방해하거나 신청기관의 귀책사유로 인하여 인증심사를 계속 진행하기가 곤란하다고 인정되는 경우

② 신청기관이 제출한 관련 자료 등을 검토한 결과 인증을 받기 위한 준비가 되었다고 볼 수 없는 경우

③ 신청기관이 부적합 사항의 보완조치 요청에 따른 보완조치가 이루어지지 않은 경우

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

❍ 인증기관은 인증심사를 중단하게 될 경우에는 그 사유를 신청기관에 서면으로 통보할 수 있다.

- 심사 중단 사유가 해소되거나 신청기관의 이의신청에 따른 이의제기 처리결과에 따라 인증심사를 재개하거나 종결할 수 있다.

2.3 인증 단계

□ 인증위원회 운영

❍ 인증기관은 인증심사 결과의 적정성을 심의하기 위하여 개인정보 보호 인증위원회를 운영한다. 인증위원회는 다음의 사항을 심의·의결한다.

- 인증기관이 실시한 인증심사의 적정성 및 인증 부여에 관한 사항
- 이의신청에 관한 사항
- 인증의 취소에 관한 사항

- 그 밖에 인증과 관련하여 인증기관 또는 인증위원회의 위원장이 필요하다고 인정하는 사항

□ 심의·의결 및 인증 부여

❍ 신청기관이 인증심사에 따른 부적합 사항에 대해 보완 조치한 결과가 이상이 없는 경우 인증기관은 인증심사의 결과를 인증위원회에 제출하여 인증 심사결과에 대한 심의·의결을 요청한다.

- 인증위원회는 인증심사가 관련법령 및 규정에 따라 적정하게 수행되었는지 여부와 신청기관의 인증심사기준 부합여부 등을 종합적으로 검토한 후 심의·의결한다.

❍ 인증기관의 장은 인증위원회가 인증을 부여하기로 의결한 때에는 15일 이내에 개인정보 보호 인증서[별지 제10호 서식]를 신청기관에 부여한다.

❍ 인증기관은 인증취득기관의 인증이력 및 이에 부수되는 사항을 관리한다.

- 인증취득기관은 인증서의 분실, 인증서 기재사항의 변경 등으로 인하여 인증서를 재발급 받고자 하는 때에는 인증기관에 그 사실을 신고하고 재발급 신청을 할 수 있다.

□ 이의신청

❍ 신청기관 또는 인증취득기관이 인증심사 결과 또는 인증 취소처분에 관하여 이의가 있는 때에는 그 결과를 통보받은 날로부터 15일 이내에 인증기관에 이의신청[별지 제11호 서식]을 할 수 있다.

- 인증기관은 이의신청이 이유가 있다고 인정되는 경우에는 인증위원회에 재심의를 요청할 수 있다

❍ 인증기관은 신청기관이 이의신청을 제기한 날로부터 30일 이내에

그 이의신청에 대한 처리결과를 신청기관 또는 인증취득기관에 서면으로 통지한다.

- 다만, 부득이한 사유로 정해진 기간이내에 결정할 수 없는 때에는 그 기간의 만료일 다음 날부터 기산하여 15일 이내의 범위에서 연장할 수 있다.

□ 인증의 유효기간 및 인증마크 표시

❍ 인증의 유효기간은 인증서 발급일로부터 3년으로 한다. 다만, 변경심사를 통하여 인증을 취득한 경우에는 인증서 변경발급일로부터 3년으로 한다.

❍ 인증기관은 인증취득기관에 그 인증심사 신청 유형에 해당하는 개인정보 보호 인증마크를 교부한다.

- 인증마크의 표시는 아래와 같이 하며, 인증의 표시를 교부·사용하는 때에는 인증번호와 인증범위를 함께 표시하여야 한다.

< 인증마크 도안모형 >

〈 공공기관용 〉 〈 대기업용 〉 〈 중소기업용 〉 〈 소상공인용 〉

인증마크 표시방법 및 홍보
① '개인정보 보호 인증마크'의 크기와 위치는 표시물 대상의 크기나 표시장소의 여건에 따라 조정할 수 있으며, 같은 비율로 축소 또는 확대하여 표시하도록 한다. ② 인증표시는 지정된 색상으로 사용한다. 또한 색상이 명확하게 나타날 수 있는 바탕색 위에 사용하거나 표시된 인쇄물의 주된 단일색상으로 사용할 수 있다. ③ 인증번호 및 인증범위, 인증유형을 함께 표시하여 사용하여야 한다. 1. 인증번호 : "인증□□□□-○○○○" (□□□□ : 인증취득년도, ○○○○ : 인증일련번호) 2. 인증범위 : "인증범위:_____" (인증취득기관의 전체 혹은 개별서비스 단위) 3. 인증유형 : ◇◇◇◇ 《예》 소상공인, 중소기업, 대기업, 공공기관 ④ 인증마크는 기관의 홈페이지 또는 인증을 취득한 서비스 제공 등에 필요한 경우와 일반문서, 봉투, 송장, 홍보책자 등의 홍보에 사용할 수 있다. ⑤ 인증의 홍보는 인증 받은 해당범위에 한하여 가능하며 인증서를 발급받은 날로부터 인증유효기간 동안에만 사용이 가능하다. 유효기간을 초과하거나 인증이 취소된 경우에는 사용을 중단하여야 한다.

- 인증취득기관의 사업 환경의 변화에 따라 취득기관의 상호명, 대표자 성명, 소재지 등의 변경에 따라서 기 취득한 인증서 내용의 변경이 필요하거나 인증서의 추가 발급이 필요한 경우에는 개인정보 보호 인증서 재발급 신청서[별지 제12호 서식]를 작성한 후에 인증기관에 요청하면 된다.

2.4 유지관리 단계

❍ 인증취득기관은 인증서를 취득한 이후 연간 1회 이상 정기적으로 유지관리심사를 받아야 하고 인증 유효기간 만료 90일 전까지 인증기관에 인증의 갱신을 신청할 수 있다. 또한, 인증을 받은 개인정보 보호 관리체계 범위 등에 중대한 변경이 발생한 경우에는 그 사유가 발생한 날로부터 90일 이내에 변경심사를 신청하여야 한다.

< 인증심사의 주기 >

□ 유지관리심사

❍ 인증취득기관은 인증 유효기간 중 연 1회 이상 유지관리심사[별지 제1호 서식]를 인증기관에 신청한다.

- 유지관리심사에서 인증취득기관의 개인정보 보호조치 및 활동이 지속적으로 유지되지 않는다고 판단되는 경우 인증기관은 인증취득기관에 그 사실을 통보하고 30일의 유예기간을 두어 보완조치할 것을 요청할 수 있다.
- 인증기관은 인증취득기관이 특별한 이유 없이 1년 이상 유지관리심사를 받지 않거나 보완조치를 하지 않은 경우에 인증위원회의 심의·의결을 거쳐 인증을 취소할 수 있다.

□ 갱신심사

❍ 인증취득기관은 인증 유효기간의 만료 90일 전까지 인증기관에 인증의 갱신[별지 제1호 서식]을 신청할 수 있다.

- 인증을 갱신하고자 하는 인증취득기관의 인증대상이 인증심사기준에 부합하는 경우에는 인증위원회의 심의·의결을 거쳐 인증의 유효기간을 3년간 연장할 수 있다.
- 인증취득기관이 인증의 갱신을 신청하지 않고 인증의 유효기간이 경과한 때에는 인증의 효력은 상실된다.
- 인증서 유효기간이 3년간 연장된 경우에는 기존 유효기간에 이어서 유효기간을 설정한다.

□ 변경심사

❍ 인증취득기관은 다음의 사유에 해당하는 경우에 그 사유가 발생한 날로부터 90일 이내에 인증기관에 변경심사[별지 제1호 서식]를 신청하여야 한다.

① 인증취득기관의 새로운 서비스의 도입·운영, 설계의 변경 등에 따라 인증 받은 인증대상의 범위가 확대 또는 축소 변경된 경우

② 인증취득기관의 사업장 변경, 합병 등 개인정보 보호 관리체계가 변경된 경우 등

❍ 인증기관은 인증취득기관으로부터 변경심사 신청을 받은 경우 변경심사 여부를 결정하여 그 결과를 인증취득기관에 통보하고 변경심사를 실시한다.

- 인증취득기관이 변경심사 사유가 발생하였음에도 불구하고 변경심사를 신청하지 않은 경우에 인증기관은 인증취득기관에 변경심사의 신청을 요구할 수 있으며, 요구를 받은 인증취득기관은 이에 응해야 한다.

□ 인증의 취소

❍ 인증기관은 인증취득기관에서 다음에 해당하는 사유가 발생할 때에는 인증위원회의 심의·의결을 거쳐 인증을 취소할 수 있다.

① 거짓 혹은 부정한 방법으로 인증을 취득한 경우

② 개인정보 유출·침해 사고가 발생한 경우

③ 인증 받은 내용을 홍보하면서 인증의 범위 또는 인증번호를 허위로 표기하거나 누락한 경우

④ 인증취득기관이 유지관리심사를 받지 않았거나 보완조치를 하지 않은 경우

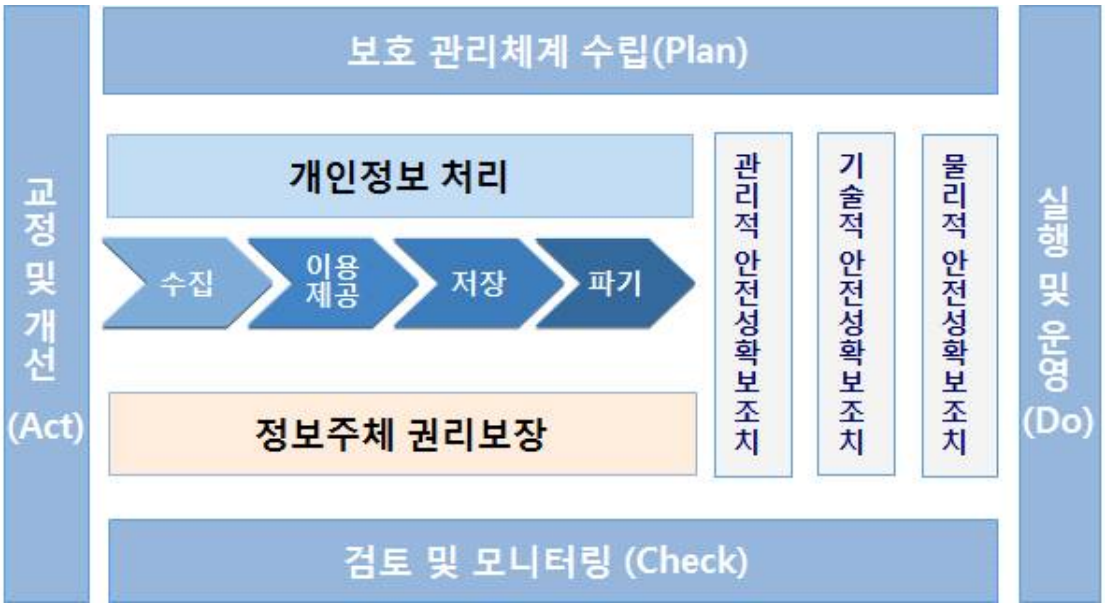
⑤ 인증취득기관이 변경심사를 받지 않은 경우

⑥ 그 밖에 인증과 관련하여 개인정보 보호 관련 법령 및 규정을 중대하게 위반한 경우

❍ 인증기관은 인증을 취소한 경우에 인증취득기관에 통지하고, 발급한 인증서를 회수한다.

제3장 개인정보 보호 인증 심사기준

이 장에서는 신청기관이 개인정보 보호 인증을 받기 위해 개인정보 보호 관리체계 구축 단계별 요구되는 인증 심사항목을 설명한다.



< 개인정보 보호 인증 프레임워크 >

❍ 개인정보 보호 인증심사는 개인정보 보호 관리체계와 개인정보 보호대책 구현 두 가지 분야를 대상으로 심사가 이루어진다.

❍ 개인정보 보호 관리체계 분야는 4단계의 PDCA 관리체계 사이클로 이루어져 있으며 총 4개 영역 15개의 심사항목으로 구성되어 있다. 개인정보 보호대책 구현 분야는 총 5개 영역 50개 심사항목으로 구성되어 있으며 신청기관의 상황에 따라 일부 조정되어 적용될 수 있다.

※ 개인정보 보호 관리체계는 개인정보 보호 인증을 위한 필수적인 사항이나, 신청기관의 유형에 따라 적용이 제외될 수 있다. (소상공인 유형에 해당하는 경우 적용 제외)

□ 개인정보 보호 관리체계

❍ ‘개인정보 보호 관리체계’ 분야는 PDCA(Plan-Do-Check-Act)의 관점에서 ‘보호 관리체계의 수립(Plan),’ ‘실행 및 운영(Do)’, ‘검토 및 모니터링(Check)’ 그리고 ‘교정 및 개선(Act)’의 심사영역으로 구성되어 있다.

<개인정보 보호 관리체계 구축 영역>

개인정보 보호 관리체계 영역	내 용
보호 관리체계의 수립	개인정보 보호를 위해 관리계획을 수립하고 개인정보 보호 조직을 구성하는 단계
실행 및 운영	수립된 보호 관리체계에 의하여 위험을 관리하고 보호대책을 구현하는 단계
검토 및 모니터링	보호 관리체계 수립 및 운영을 모니터링하여 미흡하거나 개선할 사항에 대해 검토하는 단계
교정 및 개선	개인정보 보호 관리체계를 지속적으로 개선 및 보완하여 조직에 적합한 수준으로 적용하는 단계

□ 개인정보 보호대책 구현

❍ 개인정보 보호대책 구현은 보호 관리체계의 수립에 따라 개인정보의 처리단계(수집, 이용 및 제공, 저장, 파기)에 따른 법적 요구사항 및 정보주체의 권리보장을 위한 보호대책 구현과 관리적·기술적·물리적 보호대책 구현을 위한 세부사항을 정하고 있다.

<개인정보 보호대책 구현 영역>

개인정보 보호대책 구현 영역	내 용
개인정보 처리	개인정보 처리단계별(수집·이용·저장·파기) 법적 요구사항 및 보호조치 사항을 정함
정보주체 권리보장	정보주체의 권리보장을 위한 열람·정정·삭제, 처리정지 등의 요구에 대한 법적 요구사항 및 보호조치 사항을 정함
관리적 안전성 확보조치	개인정보 보호책임자 지정, 교육 및 훈련, 개인정보 유출사고 대응에 대한 보호조치 사항을 정함
기술적 안전성 확보조치	개인정보의 안전한 처리를 위한 접근통제, 운영관리, 개발보안, 암호화, 모니터링 등에 대한 보호조치 사항을 정함
물리적 안전성 확보조치	CCTV의 설치 및 운영에 대한 보호조치 및 물리적 출입통제 등에 대한 보호조치 사항을 정함

제1절 보호 관리체계 수립

개인정보 보호 인증을 위한 개인정보 보호 관리체계 구축의 첫 번째 단계는 신청기관에서 개인정보 보호활동을 위한 근거를 확보하는 일이다.

신청기관의 관련 조직 및 조직 구성원들이 이행하여야 하는 개인정보 보호정책 및 관리계획을 수립하고 조직의 개인정보 보호목표를 효율적으로 수행할 수 있는 조직을 구성하여야 한다.

또한, 신청기관이 수립한 내부정책 및 관리계획에 따라 개인정보 보호 활동이 지속적으로 수행될 수 있도록 조직의 구성, 관련 예산의 확보 등 경영진의 관심과 참여가 뒷받침되어야 한다.

1.1 관리계획

1.1.1	관리계획 수립

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
개인정보 보호 관리계획 수립을 통해 명확한 방침 및 방향 제시를 보증하여야 하며, 이에 대해 개인정보 보호책임자의 검토와 승인을 거쳐야 한다.	개인정보 보호 관리체계를 고려한 개인정보 보호 관리계획을 수립하고 있는가?

❍ 개인정보 보호 관리계획은 신청기관의 경영목표를 지원할 수 있도록 개인정보 보호의 법적, 규제적 요건과 전략적 정책 또는 정책의 목표를 달성하기 위한 지침이나 절차 등을 포함한다.

- 개인정보 보호 관리계획은 개인정보 보호책임자가 승인함으로서 신청기관의 전체 조직(임직원 및 위탁업체 등)에 대해 강제화할 수 있다.

※ 개인정보 보호 관리계획은『개인정보 보호법』에서 개인정보의 안전성 확보를 위해 요구하는 "내부관리계획"을 의미하는 것은 아니며, 개인정보 보호 관리체계 수립 및 운영(위험관리, 내부감사 등)에 필요한 제반 사항을 정의하여야 하므로 "내부관리계획"을 포함한 보다 넓은 의미의 정책, 지침, 절차 등을 의미한다.

1.1.2	범위 설정

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
개인정보처리자의 서비스에 중대한 영향을 미치는 요소를 고려하여 개인정보 보호 관리체계의 범위를 설정하여야 한다.	개인정보 처리조직 및 업무를 고려하여 개인정보 보호 관리체계의 범위를 명확하게 정의하고 있는가? 만일 정의된 범위 내에서 예외사항이 있을 경우 그 이유를 명확히 설명하고 있는가?

❍ 개인정보 보호 관리체계 범위설정은 조직의 핵심 업무기능을 수행하거나 위험이 높은 부분을 반드시 포함하여 선정하여야 한다. 또한, 개인정보를 처리하는 업무부서 및 개인정보처리시스템, 관련서비스, 개인정보취급자 등을 포함하여야 한다.

- 개인정보는 다양한 조직에 의해 처리될 수 있으므로, 인증범위가 특정 서비스 부문이더라도 조직적인 범위는 전사(全社) 수준에 해당할 수 있다. 서비스부문의 인원관리를 위한 인사부서, IT부서, 마케팅부서, 상담부서, 계약부서 등 다양한 조직과 조직이 관리·운용하는 자산들을 범위에 포함하여야 한다.

※ 개인정보 보호 관리체계 범위는 개인정보 보호 인증 신청 시 인증신청서와 함께 첨부하여야 하는 필수 서류인 "개인정보 보호 인증심사 내역서"에 조직적 범위, 물리적 범위, 해당되는 자산의 범위를 포함하여 신청하여야 하며, 인증범위에서 제외한 조직이나 물리적 범위, 자산 등은 그 사유를 기록하여 함께 제출하여야 한다.

1.2 조직

1.2.1	조직과 책임

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
개인정보 보호 활동을 수행하고 관리하는 구성원들에 대한 책임, 역할 및 권한을 정의하여야 한다.	개인정보 보호 조직과 관련한 구성원의 책임, 역할 및 권한을 명확히 정의하고 있는가?

❍ 개인정보 보호활동을 책임있게 수행할 수 있도록 개인정보 보호 조직을 구성하고, 구성원의 책임과 역할을 개인정보 보호정책 또는 관리계획에 명시하여야 한다.

- 개인정보 보호 조직의 구성원에 대한 책임과 역할은 직무기술서 등으로 문서화하여 직무자가 해당 직무를 명확히 인식할 수 있도록 하여야 한다.
- 개인정보 보호 조직에는 개인정보 보호책임자를 비롯하여 전사적 개인정보 보호를 위한 전담조직을 구성하여 개인정보 보호 전담 관리자 및 담당자를 지정하고 개인정보 취급부서별로 개인정보 보호담당자를 지정하여 운영할 수 있다.

1.3 경영진의 책임

1.3.1	경영진의 참여

공공기관	대기업	중소기업	소상공인
●	●		

심사내용	세부내용
개인정보 보호책임자는 개인정보 보호 관리체계 수립 및 운영 등 조직이 수행하는 개인정보 보호 활동 전반에 경영진의 참여가 이루어질 수 있도록 보고, 검토 및 승인 절차를 수립하여야 한다.	개인정보 보호활동을 원활히 수행하기 위해 개인정보 보호책임자를 포함한 경영진이 개인정보 보호활동에 관한 의사결정에 적극적으로 참여할 수 있는 보고, 검토 및 승인 절차를 수립하고 있는가?

❍ 개인정보 보호 관리체계 수립 및 운영을 위한 개인정보 보호정책 및 관리계획의 제·개정 승인 및 공표, 위험관리, 내부감사 등과 같은 중요한 사안에 대해 경영진이 참여하여 의사결정을 할 수 있도록 경영진의 책임과 역할을 개인정보 보호 관리계획에 명시하여야 한다.

※ 경영진 : 민간기업의 경우는 CEO 및 CEO의 위임을 받은 CISO, CPO 등의 임원진이 될 수 있으며, 공공기관의 경우 기관장 및 기관장의 위임을 받은 책임자가 될 수 있다.

1.3.2	자원의 확보

공공기관	대기업	중소기업	소상공인
●	●		

심사내용	세부내용
개인정보 보호를 위해 필요한 자원(예산, 인력)을 반영하고, 검토하여야 한다.	개인정보 보호 관리체계를 효율적으로 운영·관리하기 위한 개인정보 보호 투자계획(예산) 및 인적자원 확보계획을 기관의 규모 및 실현 가능성 등을 고려하여 수립하고 있는가?

❍ 경영진은 개인정보 보호 관리체계 구축 및 운영을 하는데 필요한 자원을 파악하여 예산 및 인력확보 운영계획을 승인하여야 한다.

- 개인정보 보호 예산 및 인력의 확보에 대한 계획은 위험분석 및 위험평가를 통하여 식별된 위험에 대한 위험관리 계획에 반영하여 수립할 수 있다.
- 예산 및 인력의 확보는 즉시 시행이 불가능한 경우 차년도 사업계획에 반영하여야 한다.

제2절 실행 및 운영

개인정보 보호활동을 위한 근거로서 개인정보 보호 관리계획을 수립하고 개인정보 보호 조직을 구성하였다면 두 번째 단계는 개인정보 처리와 관련된 정보자산을 식별하고 식별된 자산에 기초하여 위험관리를 수행한다.

위험관리는 개인정보처리자의 서비스를 고려하여 위험관리 전략 및 계획을 수립하고, 위험평가를 수행하여 적합한 보호대책을 수립하고 이행하여야 한다.

2.1 문서화

2.1.1	문서화

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
효율적인 보호 관리체계 수립 및 운영을 위해 문서화 과정이 필요하고, 이러한 문서들과 기록을 관리하여야 한다.	개인정보 보호 관리체계의 운영을 확인할 수 있는 문서 또는 전산자료를 기록하고 있는가?
	개인정보 보호 관리체계 요구사항에 맞도록 관련 문서에 대한 이력 및 변경사항 등을 기록하여 관리하고 있는가?

❍ 개인정보 보호 관리체계의 운영을 확인할 수 있는 문서 또는 전산자료를 기록하여 문서화하여야 한다.

- 개인정보 보호 관리체계 수립 및 운영에 대한 내용이 문서화되어야 하며, 문서의 내용은 실제 업무를 반영하여 업무와의 일관성을 유지하고, 관리계획, 책임자의 결정, 위험관리 결과 등에 따라 개인정보 보호 관리체계 운영 활동을 추적할 수 있어야 한다.

❍ 개인정보 보호 관리체계의 운영에 대한 기록 및 문서의 제·개정, 변경사항 등에 대해 기록하고 그 이력을 관리하여야 한다.

개인정보 보호 관리체계 문서 예시
- 개인정보 보호 내역서 - 개인정보 내부관리계획 - 개인정보 보호 규정(정책 및 관련 표준, 지침, 절차 등) - 개인정보 위험관리 방법론(지침, 절차 등) - 개인정보 위험관리 계획서/보고서/이행계획 및 이행조치 확인서 - 개인정보 자산목록 - 개인정보 흐름도/개인정보 흐름표 - 개인정보 내부감사 보고서 - 개인정보 보호 인증심사기준 운영현황 보고서

2.2 개인정보 식별

2.2.1	개인정보 식별

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
개인정보처리자가 처리하는 서비스와 관련한 개인정보처리시스템/개인정보DB/개인정보파일 등 각각에 따른 개인정보 자산현황(자산명, 용도, 도입일자, 관리자 등)을 작성하여 관리하여야 한다.	조직의 업무 수행과 관련된 개인정보 자산을 식별하여 목록을 관리하고 있는가?
	개인정보 자산 항목별 형태, 소유자, 관리자, 사용자 특성 등을 포함한 목록을 지속적으로 관리·통제하고 있으며 책임소재가 명확한가?
	식별된 개인정보 및 관련 자산을 조직과 업무에 미치는 보안 특성과 영향, 법적 준수사항 등을 고려하여 중요도를 결정하였는가?

❍ 개인정보 처리를 위한 개인정보 자산의 분류기준을 정하고 분류기준에 따라 모든 개인정보 자산을 식별하여 목록으로 관리하여야 한다.

- 개인정보 자산의 분류기준은 신청기관의 특성에 따라 다를 수 있으나 일반적으로 개인정보(데이터), 정보시스템(PC, 서버, 네트워크, DBMS 등), 정보보호시스템(침입차단시스템, 침입탐지시스템 등), 문서, 소프트웨어, 웹 사이트 등으로 분류할 수 있다.

- 신규 도입, 변경, 폐기되는 개인정보 자산 현황을 확인 할 수 있도록 정기적으로 개인정보 자산 조사를 수행하고 개인정보 자산 목록을 최신으로 유지하여야 한다.

자산목록표 예시

순번	자산번호	HOST NAME	(운영)취급자 -Admin	(관리)책임자 -부서(팀)장	소유주체 -회사,타사	용도 (OO서비스, OO업무용 등)	운영체제	주요 어플리케이션	위치	중요도 산정			보안 등급
										C	I	A	
1	ABC-SVR-001	host001	홍길동	강감찬	㈜가나다	abc 웹 서비스	Cent OS 5 x64	Apache	IDC	1	2	2	2등급
2	ABC-SVR-002	host002	홍길동	강감찬	㈜가나다	abc 사용자 DB #01	CentOS 5.8 x86_79	Mysql	IDC	3	3	3	1등급
3	ABC-SVR-003	host003	홍길동	강감찬	㈜가나다	abc 사용자 DB #02	CentOS 5.8 x86_80	Mysql	IDC	3	3	3	1등급
4	ABC-SVR-004	host004	홍길동	강감찬	㈜가나다	abc 웹 서비스	Debian Squeeze amd64	Apache	IDC	1	2	2	2등급
5	ABC-SVR-005	host005	홍길동	강감찬	㈜가나다	웹 Login	Debian Squeeze amd64		IDC	1	2	2	2등급
6	ABC-SVR-006	host006	홍길동	강감찬	㈜가나다	통계 DB	Debian Squeeze amd64	Mysql	IDC	1	2	2	2등급
7	ABC-SVR-007	host007	홍길동	강감찬	㈜가나다	통계 DB	Debian Squeeze amd64	Mysql	IDC	3	1	3	1등급
8	ABC-SVR-008	host008	홍길동	강감찬	㈜가나다	통계 DB	Debian Squeeze amd64	Mysql	IDC	3	1	3	1등급
9	ABC-SVR-009	host009	홍길동	강감찬	㈜가나다	통계 DB	Debian Squeeze amd64	Mysql	IDC	3	1	3	1등급
10	ABC-SVR-010	host010	홍길동	강감찬	㈜가나다	통계 DB	Debian Squeeze amd64	Mysql	IDC	3	1	3	1등급
11	ABC-SVR-011	host011	홍길동	강감찬	㈜가나다	통계 DB	Debian Squeeze amd64	Mysql	IDC	3	1	3	1등급
12	ABC-SVR-012	host012	홍길동	강감찬	㈜가나다	통계 DB	Debian Squeeze amd64	Mysql	IDC	3	1	3	1등급
13	ABC-SVR-013	host013	홍길동	강감찬	㈜가나다	통계 DB	Debian Squeeze amd64	Mysql	IDC	3	1	3	1등급
14	ABC-SVR-014	host014	홍길동	강감찬	㈜가나다	통계 DB	Debian Squeeze amd64	Mysql	IDC	3	1	3	1등급
15	ABC-SVR-015	host015	홍길동	강감찬	㈜가나다	통계 DB	Debian Squeeze amd64	Mysql	IDC	3	1	3	1등급
16	ABC-SVR-016	host016	홍길동	강감찬	㈜가나다	통계 DB	Debian Squeeze amd64	Mysql	IDC	3	1	3	1등급
17	ABC-SVR-017	host017	홍길동	강감찬	㈜가나다	통계 DB	Debian Squeeze amd64	Mysql	IDC	3	1	3	1등급
18	ABC-SVR-018	host018	홍길동	강감찬	㈜가나다	통계 DB	Debian Squeeze amd64	Mysql	IDC	3	1	3	1등급

❍ 식별된 정보자산에 대한 정보 자산명, 용도, 책임자 및 관리자, 관리부서, 보안등급 등의 정보자산 정보를 확인할 수 있도록 목록으로 관리하여야 한다.

❍ 개인정보의 유출, 장애 및 침해 발생 시 조직에 미치는 영향을 고려하여 식별된 개인정보 자산의 중요도를 평가할 수 있도록 기준을 수립하여야 한다.

- 일반적으로 기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 평가기준을 마련할 수 있다. 그 외에 서비스 영향, 이익손실, 고객상실, 대외 이미지 등도 추가적으로 고려할 수 있다.

2.3 위험관리

2.3.1	위험관리 계획

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
개인정보처리자는 개인정보를 취급하는 업무(서비스)에 대하여 적합한 위험관리 계획을 수립하고, 위험관리 계획에 따라 보호대책을 수립하여야 한다.	위험관리절차(방법론)가 존재하며 관리적·기술적·법적 요구사항을 포함하는 위험관리계획을 수립하는가?

❍ 신청기관의 개인정보 보호 목표 및 정책, 법적 요구사항 등을 고려한 조직, 역할, 책임, 주요과정을 포함하여 적절한 위험관리 방법을 선택하고 그에 따른 계획을 수립하여야 한다.

- 조직의 규모, 업종 유형, 개인정보 처리 서비스 종류, 조직구조 및 소요자원 대비 효과성 등을 고려하여 적합한 위험관리 방법론을 선택하여야 한다.
- 위험관리계획에는 신청기관이 준수해야 하는 「개인정보 보호법」 및 개인정보 보호와 관련된 법적 요구사항(정보통신망법, 신용정보보호법, 의료법 등)에 대한 위험이 식별될 수 있도록 하여야 한다.

※ 중소기업의 경우 인증기준 및 법적 준거성에 대한 위험식별을 위해 체크리스트 기반의 위험분석을 실시하여 보호대책을 수립할 수 있다.

2.3.2	위험평가 수행

공공기관	대기업	중소기업	소상공인
●	●		

심사내용	세부내용
식별된 개인정보 자산에 영향을 줄 수 있는 모든 위협과 취약성, 위험을 개인정보의 흐름에 따라 식별하고 분류하여야 하며, 이 개인정보 자산의 가치와 위험을 고려하여 잠재적 손실에 대한 영향을 식별·분석하여야 한다.	개인정보의 흐름에 따라 개인정보 흐름도(흐름표)를 작성하여 위험을 식별하고 있는가?
	수립된 위험관리계획에 따라 위험평가를 수행하고 보고하였는가?
	개인정보 유출·침해사고 방지가 가능한 합리적인 목표 위험수준을 설정 하였는가?
	개인정보 흐름도는 주기적 또는 필요 시 재검토되어 최신성을 유지하는가?

❍ 개인정보의 처리단계(수집, 이용 및 제공, 저장, 파기)에 따른 위험을 식별하기 위해 개인정보 처리업무에 따른 개인정보 흐름도를 작성하여야 한다.

- 개인정보 처리단계에서 도출될 수 있는 이슈 및 위험을 식별하기 위해 업무 절차도, 개인정보 흐름표 등과 함께 개인정보 흐름도를 작성하여 위험을 식별하여야 한다.

❍ 승인된 위험관리계획에 따라 위험평가를 수행하여야 하며 위험평가 결과를 경영진에 보고하여야 한다.

- 위험평가는 유출 위험도(발생가능성, 피해 영향정도 등) 등을 고려하여 위험도를 산정할 수 있다.
- 위험평가 결과에 대해서는 개인정보 보호책임자를 포함한 경영진에 보고하여야 하며 이때에는 경영진이 쉽게 이해할 수 있도록 작성하여야 한다.

❍ 위험평가를 수행한 결과 식별된 위험에 대하여 개인정보 보호정책과 목적에 부합하도록 위험을 허용 가능한 수준으로 감소시키기 위한 위험관리 전략을 수립하여야 한다.

- 위험에 따라 위험처리, 위험수용, 위험회피, 위험전가 등 위험관리 전략을 수립하여야 한다.
- 허용 가능한 위험수준(DoA : Degree of Assurance)을 선정하는

경우 개인정보 침해위험을 방지할 수 있는 합리적인 수준으로 결정하여야 한다.

- 허용 가능한 위험수준 이하의 위험들은 더 이상 위험을 경감하기 위한 별다른 조치를 취하지 않게 되므로 타당한 수준으로 결정하여야 한다.
- 허용 가능한 위험수준의 결정은 사업 수행부서의 요구사항을 고려하여 개인정보 소유자, 사용자, 기타 관련자의 합의로 결정하고 해당 사항에 대해서는 개인정보 보호책임자 등 경영진의 최종 승인을 받도록 하여야 한다.

❍ 개인정보 흐름도는 조직의 내·외부적 환경변화, 개인정보 취급업무의 변경 등을 반영할 수 있도록 주기적으로 검토되고 갱신되어야 한다.

- 조직변경, 개인정보처리시스템의 도입 및 변경, 수탁사 변경 등이 발생할 수 있으므로 개인정보 흐름도를 주기적으로 갱신하여 이를 반영하여야 한다.

2.3.3	위험평가 이행계획

공공기관	대기업	중소기업	소상공인
●	●		

심사내용	세부내용
위험평가 이행계획에 따라 보호대책을 구현하고, 보호대책의 효과성에 대하여 주기적인 검토를 하여야 한다.	위험평가 이행계획 수립 시 보호대책의 효과성을 검토하였는가?
	위험평가 이행계획을 적절하게 수립하여 승인받고 있는가?

❍ 위험평가 결과에 근거하여 위험수준의 감소를 위하여 선정한 보호대책은 위험처리의 시급성, 예산 할당, 구현에 요구되는 기간 등을 고려하여 효과성을 검토하여야 한다.

- 허용 가능한 위험수준(DoA)을 초과하지 않은 위험 중 신청기관 및 외부환경에 따라 위험수준이 상승할 가능성이 높거나 조직이 중요하다고 판단하는 부분에 대해서는 필요 시 보호대책을 추가

적으로 수립할 수 있다.

❍ 위험평가 결과에 따라 보호대책이 선정되었다면 보호대책 구현을 위한 구체적인 이행계획을 수립하여 경영진의 승인을 받아야 한다.

- 위험평가 이행계획에는 이행담당자, 이행일정, 이행방법, 소요예산 등을 구체적으로 명시하는 등의 구체적인 계획이 포함되어야 한다.

2.3.4	이행계획에 따른 보호대책 구현	공공기관	대기업	중소기업	소상공인
		●	●		

심사내용	세부내용
개인정보 보호 우선순위, 일정계획, 예산, 책임, 운영계획 등을 포함한 위험평가 이행계획에 의해 적절히 구현되어야 한다.	위험평가 이행계획에 따라 보호대책을 적절히 구현하였는가?

❍ 위험평가 이행계획에 따라 보호대책을 구현하여야 한다.

- 식별된 위험에 대한 위험수준이 감소되었음을 보장하기 위하여 개인정보 보호책임자 등 경영진은 보호대책이 이행계획에 따라 빠짐없이 효과적으로 이행되었는지 여부를 검토 및 확인하여야 한다.

※ 이행계획에 따른 보호대책의 효과적 구현에 대한 사항은 인증심사기준 “보호대책 구현”부문의 각 심사항목별 명세서를 작성하여 인증신청 시 함께 제출하여야 한다.

제3절 검토 및 모니터링

개인정보 보호 관리체계를 수립하고 구현한 보호대책에 대한 문제점을 발견하여 개선하기 위하여 지속적으로 모니터링하고 점검하여야 한다.

3.1 개인정보 보호 관리체계의 검토 및 모니터링

3.1.1	보호 관리체계 검토

공공기관	대기업	중소기업	소상공인
●	●		

심사내용	세부내용
개인정보 보호 관련 법령에서 요구하는 사항을 내부규정 및 관리계획에 포함하여야 하며, 이를 주기적으로 검토하여야 한다.	개인정보 보호 관리체계의 주기적인 검토를 위한 절차가 존재하는가?
	법, 규제, 계약상의 요구사항들이 내부규정 및 관리계획에 반영되었는지 주기적으로 검토하였는가?

❍ 조직의 업무, 개인정보처리시스템, 법·제도 등의 대내외적 환경 변화와 내부 이행점검 및 모니터링, 보안사고 결과 등을 반영하여 개인정보 보호 관리체계를 공식적이고 정기적으로 재검토하는 절차를 수립하여야 한다.

- 개인정보 보호정책 및 관리계획에 관리체계의 재검토 요건, 재검토 주기, 검토 결과에 따른 보고절차 및 개선활동 등을 포함하여야 한다.

❍ 신청기관의 개인정보 보호 관리체계 재검토 절차에 따라 주기적인 검토를 이행하여야 한다.

- 조직이 준수해야 할 법규가 존재하는 경우 법적 요구사항을 명시한 문서(지침 등)와 해당 법규 준거성을 점검하기 위한 체크리스트는 최신 법규 사항을 반영하고 있어야 한다.

3.1.2	내부 모니터링

공공기관	대기업	중소기업	소상공인
●	●		

심사내용	세부내용
개인정보처리자의 개인정보 보호 관리체계가 계획된 절차에 따라 효과적으로 실행되는지를 점검하기 위하여 감사의 기준, 범위, 주기 및 방법을 규정하고, 계획된 주기로 내부감사를 수행하여야 한다.	개인정보 보호 관리체계 감사 계획(기준, 범위, 주기, 방법 등)을 수립하고 있는가?
	개인정보 보호 감사는 계획에 따라 주기적으로 수행되고 감사결과에 따른 개선활동이 이루어지고 있는가?

❍ 조직 내 수립된 개인정보 보호정책 및 법적 요구사항에 따라 개인정보 보호 관리체계 활동이 효과적으로 수행되는지 여부를 검토하기 위하여 내부감사 지침 또는 계획을 수립하여야 한다.

- 내부감사 지침 또는 계획에는 내부감사 기준, 범위, 수행주기, 감사인력의 자격요건 등에 대하여 정의하여야 한다.

※ 내부감사는 조직이 스스로 보안활동에 대한 점검을 수행하는 보안점검과는 구별하여야 한다. 따라서 감사조직은 감사대상 조직에 대해 중립성을 보장할 수 있도록 구성하여야 한다.

- 내부감사 지침 또는 계획에 따라 연 1 회 이상 감사가 수행될 수 있도록 연간 계획을 수립한 후 개인정보 보호책임자 등 경영진에게 보고하여 승인을 득한 후 계획에 따라 내부감사를 수행하여야 한다.

❍ 내부감사 중 지적사항이 발견된 경우 일정 기간 동안 피감사 부서 혹은 담당자가 대책을 마련하여 보완하도록 한 후 보완조치 여부를 확인하여야 한다.

- 내부감사 결과는 감사일정 및 범위, 감사결과, 지적사항 및 보완조치 내용(보완조치 완료에 대한 확인 여부)을 포함하여 개인정보 보호책임자 등 경영진에게 보고하여야 한다.

※ 내부감사 결과보고서에는 감사계획에서 정한 감사범위, 감사대상, 감사방법 등에 따라 내부감사가 실시되었는지를 확인할 수 있도록 이행현황, 문제점, 개선사항 등이 포함되어야 한다.

제4절 교정 및 개선

개인정보 보호 예방, 교정, 개선활동을 주기적으로 이행하고 그 실적을 관리하여야 한다.

4.1 교정 및 개선활동

4.1.1	개인정보 보호 개선활동

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
개인정보 보호활동을 지속적으로 점검·개선하고, 그 실적이 주기적으로 관리되어야 한다.	조직 내외부에 개인정보 수집, 이용, 제공 시 필요 이상의 정보를 처리한 실적 등을 주기적으로 점검하고 개선하고 있는가?
	개인정보 보호를 위한 관리적·기술적·물리적인 보호조치를 강구하고 이에 대해 주기적으로 점검하고 개선하고 있는가?

❍ 조직 내외부에서 개인정보 처리(수집, 이용 및 제공, 저장, 파기) 시, 필요 이상의 정보를 처리한 경우, 해당 실적 등을 주기적으로 점검하고 개선(필요정보 최소화 등)하여야 한다.

- 개인정보 보호 조직은 개인정보 처리와 관련하여 개인정보 보호 정책 및 관리계획에서 정의한 목적과 법률 요구사항에 대한 개인정보 처리부서의 이행여부를 주기적으로 점검하고 그 결과를 기록하고 유지하여야 한다.

❍ 개인정보 보호정책 및 관련 법률에서 정의한 관리적·기술적·물리적 요구사항에 대해 주기적으로 점검하고 개선하여야 한다.

※ 개인정보 처리 및 관리적·기술적·물리적 보호대책에 대한 주기적인 점검을 위한 점검방법, 점검자, 점검주기, 점검항목 등을 사전에 정의하고 이에 따라 점검을 실시하여야 한다.

4.2 내부공유 및 인식제고

4.2.1	내부 공유 및 인식제고

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
개인정보 보호 관리계획은 조직 내 모든 임직원 및 관련자에게 배포되고, 모든 임직원 및 개인정보취급자 등은 해당 내용을 이해하여야 한다.	개인정보 보호 관리계획은 조직 내 모든 임직원 및 관련자에게 배포되고, 모든 임직원 및 개인정보취급자 등은 해당 내용을 이해하고 있는가?

❍ 개인정보 보호정책 및 관리계획은 신청기관 조직 내 모든 임직원 및 관련 외부자가 해당 내용을 이해하고 인식할 수 있도록 배포하고 교육하여야 한다.

- 개인정보 보호정책(관리계획 등)의 배포는 책자 배포, 이메일 통지, 그룹웨어에 등록 및 전체 공지 등의 다양한 방법으로 배포할 수 있다.
- 개인정보 보호정책의 변경 또는 개정 시에는 최신본을 재배포하여야 하며 전체 임직원에 대해 재교육을 실시하여야 한다.
- 조직의 위험분석 및 위험관리 결과에 따른 보호대책 선정 및 이행계획을 수립한 경우 관련부서 및 담당자를 대상으로 교육을 재실시할 수 있다

※ 개인정보 보호 교육에 대한 세부사항은 보호대책 구현의 7. 관리적 안전성 확보조치 영역의 7.2 교육 및 훈련을 참고

제5절 개인정보처리

❍ 개인정보 보호대책 구현을 위한 개인정보처리 심사영역은 개인정보 처리단계별 개인정보의 수집, 이용 및 제공, 저장, 파기 등의 법적 요구사항 및 보호조치 사항을 정하고 있다.

5.1 개인정보 수집 시 보호조치

5.1.1	개인정보 수집제한

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보처리자는 서비스 제공을 위해 필요한 최소한의 정보만을 수집하고, 목적 내에서만 개인정보를 수집하여야 한다.	개인정보 수집 목적 및 수집항목을 명확히 하여 수집하고, 정보주체 및 법정대리인으로부터 법령에 근거한 범위 내에서 수집하고 있는가?
	서비스 제공을 위해 필요한 최소한의 정보만을 수집하는가?

❍ 정보주체의 개인정보를 수집하는 경우에는 정보주체의 동의를 받거나 관련 법률에 근거하여서만 수집하여야 한다.

❍ 개인정보처리자는 정보주체의 개인정보를 수집하는 경우에는 필요한 최소한의 정보를 수집하여야 한다.

- 서비스 제공을 위해 필요한 최소한의 정보만을 수집하고, 추가적 정보의 수집을 원할 경우, 정보주체가 선택 제공할 수 있도록 필수와 선택사항으로 구분하여 기재할 수 있도록 하여야 하며, 선택 사항의 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하여서는 안 된다.

5.1.2	정보주체의 동의

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보는 법령에 특별한 규정이 있는 경우를 제외하고는 정보주체의 동의를 얻은 후에 수집하여야 한다.	개인정보 수집 시 주요 고지내용을 정보주체에게 알리고 동의를 받는가?
	개인정보 수집 동의를 득할 때 이용자에게 고지한 사항 중 변경이 발생한 경우 정보주체에게 고지내용을 알리고 동의를 얻는가?
	개인정보 수집에 대해 동의 받는 방법은 적절한가?
	정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 수집하는가?
	법정대리인 또는 정보주체의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받는가?
	정보주체의 개인정보를 이용하여 재화나 서비스를 홍보하거나 판매를 권유하는 경우 정보주체가 이를 명확하게 인지할 수 있도록 알려 주었는가?

❍ 정보주체의 개인정보를 이용하려고 수집하는 경우에는 주요 고지내용을 반드시 정보주체에게 알리고 동의를 받아야 한다.

❍ 정보주체로부터 수집하는 고지항목에 대한 변경이 발생한 경우에는 변경사항을 정보주체에게 알리고 동의를 받아야 한다.

❍ 개인정보처리자가 정보주체로부터 동의를 받을 때에는 개인정보를 수집·이용하는 것에 대한 정보주체의 자발적인 승낙의 의사표시를 명확하게 확인할 수 있어야 한다.

❍ 개인정보를 처리하기 위하여 정보주체의 동의를 얻고자 하는 경우에는 정보주체의 동의가 필요한 경우와 필요하지 않은 경우를 구분하고, 후자의 경우에는 정보주체의 동의 없이 개인정보를 처

리할 수 있다는 점과 그 사유를 알리고 수집하여야 한다.

❍ 정보주체의 동의를 받을 때에는 정보주체와의 계약 체결 등을 위하여 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 한다.

- 정보주체로부터 별도의 동의를 받고자 하는 경우에는 정보주체가 다른 개인정보처리의 목적과 별도로 동의여부를 표시할 수 있도록 조치를 취하고 동의를 받아야 한다.

❍ 재화나 서비스를 홍보하기 위해 개인정보를 이용하는 경우 정보주체가 명확하게 인식할 수 있도록 알리고 동의를 받아야 한다.

5.1.3	법정대리인 동의 및 고지

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
만14세 미만의 아동의 개인정보를 수집 할 경우 법정대리인에게 필요한 사항을 고지하고 동의를 받아야 한다.	만14세 미만 아동의 개인정보를 수집하는 경우 법정 대리인에게 필요한 사항을 고지하고 동의를 받고 있는가?

❍ 만 14세 미만의 아동으로부터 개인정보를 수집 시에는 법정대리인에게 필요한 사항을 고지하고 동의를 받아야 한다.

- 법정대리인의 동의를 받을 때에는 법정대리인의 진위여부 및 자격 등을 확인하여야 한다.

- 법정대리인의 동의를 받을 때에는 법정대리인이 진정으로 동의하였음을 확인할 수 있는 방법으로 하여야 한다.

5.1.4	민감정보 및 고유식별 정보의 수집제한

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
정보주체의 권리 이익이나 사생활을 뚜렷하게 침해할 우려가 있거나, 그 자체로 개인을 식별할 수 있는 고유식별정보는 수집하지 않아야 하며, 필요한 경우 정보주체로부터 별도의 동의를 받아야 한다.	사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 민감정보를 수집하는 경우 정보주체로부터 별도의 동의를 받거나 관련 법령에 근거하여 수집하고 있는가?
	주민등록번호를 제외한 고유식별정보를 수집하는 경우 정보주체로부터 별도의 동의를 받거나 관련 법령에 근거하여서만 수집하고 있는가?
	개인정보처리자가 주민등록번호를 처리하는 경우 관련 법령에 따라 처리하고 있는가 ?

❍ 개인정보처리자는 정보주체로부터 별도의 동의를 받거나 다른 법률에 특별히 수집대상 개인정보로 허용된 경우에 한하여 민감정보를 수집하여야 한다.

- 고유식별정보와 민감정보의 수집이 반드시 필요하여 정보주체의 동의를 받아야 하는 경우 다른 수집정보와 동의 항목을 구분하여 별도의 동의를 받아야 함

※ '일반정보', '고유식별정보', '민감정보'의 동의 항목을 반드시 구분

❍ 별도로 정보주체의 동의를 받은 경우와 법령에서 고유식별정보의 처리를 요구하거나 허용하고 있는 경우를 제외하고는 원칙적으로 고유식별정보를 처리할 수 없다.

❍ 개정된 개인정보 보호법('14년 8월 7일 시행)에서 주민등록번호는 관련 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용하는 경우 외에는 주민등록번호를 수집할 수 없도록 규정하고 있다.

주민등록번호 처리제한
제24조2(주민등록번호 처리제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다. 1. 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우 2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우 3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 안전행정부령으로 정하는 경우 [시행일 : 2014.8.7]

※ 주민등록번호의 수집에 대해서는 법 시행일(2014. 8. 7)이전의 경우에는 다른 고유식별정보의 수집과 동일하게 적용한다.

5.1.5	간접수집 보호조치

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
시스템에 의한 수집 또는 개인정보 처리를 통해 생성한 간접 수집 개인정보에 대하여 요구 시 정보주체에게 고지하여야 한다.	간접 수집하는 개인정보에 대해 정보주체의 요구가 있는 경우 즉시 정보주체에게 이를 고지하고 있는가?

❍ 정보주체로부터 직접 수집하는 정보가 아닌 시스템 또는 개인정보 처리를 통해 생성되어 간접 수집된 정보들은 정보주체의 요구가 있을 시 정보주체에게 알려야 한다.

- 간접 수집정보 : 제 3자로부터 제공받은 정보, 신문, 잡지, 인터넷 등 공개된 소스로 부터 수집된 정보

정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지
제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지) ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 다음 각 호의 모든 사항을 정보주체에게 알려야 한다. 1. 개인정보의 수집 출처 2. 개인정보의 처리 목적 3. 제37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실

5.1.6	대체가입수단의 제공

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
인터넷 홈페이지 회원 가입 시 주민등록번호에 대한 대체가입 수단을 제공하여야 한다.	인터넷 홈페이지를 통해 회원으로 가입할 경우 주민등록번호를 대체하는 가입 수단을 제공 하는가?

❍ 공공기관 및 일정 규모 이상의 개인정보를 처리하는 개인정보처리자는 개인정보 수집 시 주민등록번호의 수집을 최소화 또는 대체할 수 있는 수단(아이핀 등)을 제공하여야 한다.

※ 일정 규모 이상의 개인정보처리자 : 인터넷 홈페이지를 운영하는 개인정보처리자로서 전년도 말 기준 직전 3개월간 그 인터넷 홈페이지를 이용한 정보주체의 수가 하루 평균 1만 명 이상인 개인정보처리자 (시행령 제20조)

5.1.7	개인정보처리방침의 수립 및 공개

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보처리자는 개인정보 처리방침을 수립하여 정보주체가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하여야 한다.	개인정보 처리방침을 수립하거나 변경하는 경우에 정보주체가 언제든지 쉽게 확인할 수 있도록 적절한 방법으로 공개하였는가?
	개인정보의 처리방침이 법적 요구사항 및 운영에 필요한 사항을 포함하여 작성되었는가?
	개인정보 처리방침을 변경하는 경우 그 변경사항 및 이력을 정보주체가 확인할 수 있도록 하는가?

❍ 개인정보의 수집 장소와 매체 등을 고려하여 개인정보처리방침을 공개하되, 그 명칭을 '개인정보 처리방침'이라고 표시하여야 한다.

❍ 정보주체의 개인정보를 취급하는 경우, 법률에서 정한 내용을 모두 포함한 개인정보 처리방침을 마련하여야 한다.

개인정보 처리방침에 포함되어야 할 사항

○ 개인정보 처리방침의 필수적, 임의적 기재사항

필수적 기재사항	임의적 기재사항
1. 개인정보의 처리 목적 2. 개인정보의 처리 및 보유 기간 3. 개인정보의 제3자 제공에 관한 사항 (해당되는 경우에만 정함) 4. 개인정보처리의 위탁에 관한 사항 (해당되는 경우에만 정함) 5. 정보주체의 권리.의무 및 그 행사방법에 관한 사항 6. 처리하는 개인정보의 항목 7. 개인정보의 파기에 관한 사항 8. 개인정보 보호책임자에 관한 사항 9. 개인정보 처리방침의 변경에 관한 사항 10. 개인정보의 안전성 확보조치에 관한 사항	1. 정보주체의 권익침해에 대한 구제방법 2. 개인정보의 열람청구를 접수.처리하는 부서 3. 영상정보처리기기 운영.관리에 관한 사항 (개인정보 보호법 제25조제7항에 따른 '영상정보처리기기 운영.관리방침'을 개인정보처리방침에 포함하여 정하는 경우)

※ **필수적 기재사항**이란 개인정보 보호법 제30조, 시행령 제31조, 표준 개인정보 보호지침 제37조에 따라 「개인정보 처리방침」에 반드시 모두 포함해야 하는 사항임

※ **임의적 기재사항**이란「개인정보 처리방침」에 포함시킬지 여부를 개인정보처리자가 개인정보 처리현황을 고려하여 자율적으로 정할 수 있는 사항임

❍ 개인정보처리방침을 변경하는 경우 이전 개인정보처리방침과 변경사항을 정보주체에게 공지하여야 한다.

5.2 개인정보 이용 및 제공 시 보호조치

5.2.1	개인정보 제3자 제공

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보를 제3자에게 제공 시 정보주체로부터 동의를 받은 후에 개인정보에 대한 적절한 보호조치 및 3자 제공을 하여야 한다.	개인정보를 제3자에게 제공 또는 공유할 경우 법령에 근거하거나 주요 고지 사항을 정보주체에게 알리고 동의를 받고 있는가?
	이미 고지한 제3자 제공 동의 사항 중 변경이 발생한 경우에도 정보주체에게 이를 알리고 동의를 받고 있는가?
	개인정보를 제공받은 경우, 제공받은 목적 외의 용도로 이용하지 않는가?

❍ 정보주체의 개인정보를 제3자에게 제공하는 경우에는 법령에 근거하거나, 정보주체에게 다음 사항을 고지하고 동의를 받아야 한다.

- 개인정보를 제공받는 자
- 개인정보를 제공받는 자의 개인정보 이용 목적
- 제공하는 개인정보의 항목
- 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
- 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

❍ 개인정보의 제3자 제공과 관련하여 사전에 정보주체에게 고지한 사항 중 변경이 발생한 경우 정보주체에게 이를 알리고 동의를 얻어야 한다.

❍ 제공받은 개인정보를 정보주체의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우를 제외하고는 제공받은 목적 외의 용도로 이용하지 않아야 한다.

5.2.2	개인정보 목적 외 이용 및 제공

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보는 정보주체에게 고지하고 동의 받은 범위를 벗어나 이용하지 않아야 하고, 만약 동의 범위를 벗어나 이용할 경우 정보주체로부터 추가적으로 동의를 획득하고, 개인정보에 대한 적절한 보호조치를 취해야 한다.	개인정보를 목적 외의 용도로 이용하는 경우, 법령에 근거하거나 정보주체의 동의 획득 등 사실이 명확한가?
	개인정보를 목적 외의 용도로 이용하는 경우, 주요 고지사항을 정보주체에게 알리고 별도 동의를 받는가?
	개인정보를 목적 외의 용도로 제3자에게 제공하는 경우, 제공받는 자가 보호조치를 취하도록 하거나, 이용목적·방법 등을 제한하도록 요청하고 있는가?
	공공기관이 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우, 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 관보 또는 인터넷 홈페이지 등에 게재하고 있는가?
	공공기관이 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우, 대장관리(이력관리)를 하고 있는가?

❍ 개인정보를 수집 목적 외로 이용하고자 하는 경우에는 정보주체로부터 별도의 동의를 받거나 법률에 근거하여야 한다.

- 단, 통계작성 및 학술연구 등 법 제18조제2항에서 정한 경우는 예외로 적용한다.

❍ 개인정보를 수집목적의 범위를 벗어나 이용하기 위해서는 정보주체의 동의를 받아야 하며, 이때 ① 개인정보의 이용목적, ② 이용하는 개인정보의 항목, ③ 개인정보의 보유 및 이용기간, ④ 동의거부권이 있다는 사실 및 동의거부에 따른 불이익에 관한 사항을 알려야 한다. 알려야 할 사항에 변경이 있는 때에도 이를 다시 알리고 동의를 받아야 한다.

❍ 개인정보를 수집 목적외로 이용하거나 제공하는 경우 다른 개인정보의 처리에 대한 동의와 분리해서 목적 외 이용·제공에 대해 별도의 동의를 받아야 한다.

❍ 개인정보처리자는 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다. 이 경우 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다.

❍ 공공기관이 개인정보를 목적외로 이용하거나 제3자에게 제공하는 경우에는 법 제18조제4항에 따라 관보 또는 인터넷 홈페이지 등에 30일이내에 게재하여야 한다.

❍ 공공기관의 경우 개인정보를 목적 외 이용 및 제공하는 경우 '개인정보 목적 외 이용·제공대장'에 기록 관리하여야 한다.

※ 개인정보 보호법 시행규칙 [별지 제1호 서식] '개인정보 목적 외 이용.제공대장'

5.2.3	개인정보의 이전

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보처리자가 양도·합병으로 인해 개인정보를 이전 하거나 받는 경우 또는 개인정보를 국외의 제3자에게 제공 또는 공유하는 경우 적절한 보호조치를 하여야 한다.	영업의 양도, 합병 등으로 개인정보를 이전받은 경우 양도자가 정보주체의 개인정보를 이용하거나 제공할 수 있는 당초의 목적 범위 안에서만 개인정보를 이용하거나 제공하는가?
	영업의 양도, 합병 등으로 개인정보를 이전하려는 (또는 이전 받는) 경우 미리 주요 사항을 해당 정보주체에게 알렸는가?
	개인정보처리자가 개인정보를 국외의 제3자에게 제공 또는 공유하는 경우 주요 고지 사항을 정보주체에게 알리고, 동의를 요구하고 있는가?

❍ 양수자는 양도자가 정보주체의 개인정보를 이용하거나 제공할 수 있는 당초의 목적 범위 안에서만 개인정보를 이용하거나 제공하여야 한다.

- 영업의 양도·합병 등으로 개인정보를 이전받은 경우에는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공할 수 있다. 이 경우 개인정보를 이전받는 자는 개인정보처리자로 본다.

❍ 개인정보를 이전하는 자 또는 개인정보를 이전받는 자의 영업양도·양수 등의 사실을 정보주체에게 통지할 때에는 다음 각 호의 사항을 서면 등의 방법으로 해당 정보주체에게 알려야 한다.

1. 개인정보를 이전하려는 사실
2. 개인정보를 이전받는 자의 성명, 주소, 전화번호 및 그 밖의 연락처
3. 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차

- 개인정보를 이전하는 자는 과실 없이 서면 등의 방법으로 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다.

❍ 수집된 개인정보를 국외로 이전할 계획이 있다면 이에 대한 사항을 정보주체에게 미리 고지하고 동의를 얻어야 한다.

5.3 개인정보 보유 시 보호조치

5.3.1	개인정보 품질보장

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보처리자가 처리하고 있는 개인정보는 정확성, 완전성, 최신성을 유지하여야 한다.	개인정보처리자가 처리하고 있는 개인정보가 정확하고 최신의 상태로 유지되는가?

❍ 수집한 개인정보는 정확하고 최신의 상태로 유지되어야 한다.

- 개인정보의 정확성과 최신성을 확보하기 위하여 개인정보 입력 시 입력내용을 사전에 확인하는 절차, 개인정보에 대한 열람 및 정정 요구 등을 통해 정확한 정보를 입력할 수 있는 절차나 방법 등을 마련하여야 한다.

5.3.2	개인정보 파일관리

공공기관	대기업	중소기업	소상공인
●			

심사내용	세부내용
개인정보파일을 운용하는 공공기관은 그 현황을 안전행정부에 등록하여야 하고, 변경사항 발생 시 이를 고지하여야 한다.	공공기관의 장이 개인정보파일을 운용하는 경우, 안전행정부장관에게 등록 또는 변경사항을 고지하였는가?

❍ 공공기관의 장이 개인정보파일을 운용하는 경우에는 안전행정부 장관에게 그 사실을 등록하여야 한다. 등록된 사항에 변경이 있는 경우에도 역시 그 내용을 등록하여야 한다.

- 개인정보파일 등록업무를 실제 수행하는 것은 해당 공공기관의 개인정보 보호책임자이다. 개인정보파일을 운용하는 공공기관의 개인정보 보호책임자는 그 현황을 안전행정부에 등록하여야 한다.

※ 개인정보파일 등록은 공공기관만 부담하는 의무이며 민간 부문의 기업·단체 등은 개인정보파일 등록의무가 적용되지 않는다.

5.4 개인정보 파기 시 보호조치

5.4.1	개인정보 파기 절차

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
개인정보처리자는 개인정보의 파기에 관한 사항을 기록 관리하여야 하며, 파기 시행 후 파기결과를 확인하여야 한다.	개인정보를 파기하는 경우 파기에 관한 사항을 기록 관리하고 있으며, 개인정보 보호책임자가 파기결과를 확인하고 있는가?

❍ 개인정보가 저장된 저장매체, 종이문서 등의 파기는 개인정보 보호책임자 책임하에 파기하고 그 기록을 유지하여야 한다.

- 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하고 개인정보파일 파기 관리대장을 작성하여야 한다.

5.4.2	개인정보 파기

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보처리자는 개인정보 파기에 관한 관리계획을 수립하고, 관리계획에 따라 개인정보의 수	개인정보의 보유기간 경과, 수집 및 이용목적이 달성된 경우 지체 없이 개인정보를 파기하는가?

집 목적이 달성된 경우, 개인정보를 안전한 방법으로 지체 없이 파기하여야 한다.	개인정보의 파기 방법은 복구 불가능한 수준의 안전한 방법으로 파기하고 있는가?
	개인정보의 수집목적이 달성된 경우에도 타 법령에 근거하여 개인정보를 전부 또는 일부 보유한다면 보유 근거법령 및 보유기간 등을 정보주체에게 명확히 공개하고 해당 개인정보를 별도로 분리·보관하도록 하고 있는가?

❍ 개인정보처리자는 처리목적이 달성되거나, 해당 서비스 및 사업이 종료된 경우, 정당한 사유가 없는 한 지체없이(5일 이내) 개인정보를 파기하여야 한다.

❍ 개인정보를 파기할 때에는 다시 복원하거나 재생할 수 없는 형태로 파기하여야 한다.

- 하드디스크, CD/DVD, USB메모리 등의 매체에 전자기(電磁氣)적으로 기록된 개인정보는 다시 재생시킬 수 없는 기술적 방법으로 삭제하거나 물리적인 방법으로 매체를 파괴하여 복구할 수 없도록 하여야 한다.
- 종이와 같이 출력물의 형태로 되어 있는 경우에는 물리적으로 분쇄하거나 소각하는 방법으로 해당 개인정보를 완전히 파기하여야 한다.

❍ 개인정보처리자는 법령에 따라 개인정보를 파기하지 않고 보존하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장·관리하여야 한다.

- 개인정보의 수집목적이 달성된 경우에도 개인정보를 전부 또는 일부 보유한다면 별도의 DB 등에 분리하여 보관하여야 한다.

제6절 정보주체 권리보장

❍ 개인정보 보호대책 구현을 위한 정보주체 권리보장 심사영역은 정보주체의 권리보장을 위한 열람·정정·삭제, 처리정지 등의 요구에 대한 법적 요구사항 및 보호조치 사항을 정하고 있다.

6.1 권리보장

6.1.1	개인정보의 열람·정정·삭제

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보의 열람·정정·삭제 개인정보처리자는 정보주체의 개인정보에 대한 열람·정정·삭제 방법 및 절차를 제공하고, 정정·삭제 요구 시 지체 없이 처리하고 기록을 남겨야 한다.	정보주체 또는 정보주체의 법정 대리인이 정보주체 자신의 개인정보에 대한 열람 또는 이용 및 제공내역을 요구할 수 있는 방법 또는 절차를 제공하는가?
	개인정보처리자가 개인정보에 대한 열람 또는 이용 및 제공내역을 요구받을 경우 기간 내에 열람 가능하도록 처리하고, 열람할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리는가?
	정보주체 또는 정보주체의 법정 대리인으로부터 정보주체의 개인정보 정정 또는 삭제에 대한 요구가 있는 경우 일정 기한 내에 필요한 조치를 취하고, 정보주체에게 알리는가?
	정보주체에 의해 정정 또는 삭제 요구된 개인정보가 법령에서 정한 수집대상으로 명시되어 있어 삭제할 수 없는 경우 그 내용을 정보주체에게 알리는가?
	개인정보를 정정·삭제하여야 하는 경우, 위탁사에게 제공한 개인정보도 함께 지체 없이 처리하는가?

❍ 개인정보처리자는 정보주체가 자신의 개인정보에 대한 열람 또는

이용 및 제공내역을 요구할 수 있는 방법 또는 절차를 제공하여야 한다.

❍ 개인정보처리자가 정보주체로부터 개인정보 열람을 요구받았을 때에는 10일 이내에 정보주체가 해당 개인정보를 열람할 수 있도록 조치하여야 한다.

❍ 개인정보처리자가 정보주체로부터 개인정보 열람을 요구받았지만 10일 이내에 열람을 하게 할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리고 열람을 연기할 수 있다. 개인정보 열람을 연기한 후 그 사유가 소멸하였을 경우 연기사유가 소멸한 날로부터 '10일 이내'에 열람하도록 하여야 한다.

❍ 정보주체 또는 정보주체의 법정 대리인으로부터 정보주체의 개인정보 정정 또는 삭제에 대한 요구가 있는 경우 일정 기한 내에 필요한 조치를 취하여야 한다.

- 개인정보처리자는 조사결과 정보주체의 요구가 정당하다고 판단되면 개인정보 정정·삭제 요구서를 받은 날부터 10일 이내에 그 개인정보를 조사하여 정보주체의 요구에 따라 해당 개인정보의 정정·삭제 등의 조치를 한 후 그 결과를 안전행정부령으로 정하는 개인정보 정정·삭제 결과통지서로 해당 정보주체에게 알려야 한다.

❍ 개인정보처리자는 법 제35조제4항에서 정한 개인정보 열람 제한·거절의 사유에 해당하는 경우에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다.

- 열람 요구 사항 중 일부가 해당하는 경우에는 그 일부에 대하여 열람을 제한할 수 있으며, 열람이 제한되는 사항을 제외한 부분에 대해서는 열람할 수 있도록 하여야 한다.

❍ 외부위탁 또는 제3자에게 제공한 개인정보에 대한 정정요청 및 동의 철회 시에는 수탁사 또는 제3자에게 연락하여 이에 대한 조치를 요청하여야 한다.

6.1.2	개인정보의 처리정지

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보처리자는 정보주체의 개인정보에 대한 처리정지 방법 및 절차를 제공하고, 처리정지 요구사항을 처리하고 기록을 남겨야 한다.	개인정보에 대한 처리정지의 요구, 처리정지의 거절, 통지 등의 방법 및 절차를 제공하는가?
	정보주체로부터 개인정보처리 정지요구를 받았을 때 이를 처리하는가?
	정보주체에 의한 처리정지 요구를 거절하는 정당한 사유가 있을 때, 그 내용을 정보주체에게 알리는가?

❍ 개인정보에 대한 처리정지의 요구, 거절, 통지 등의 방법 및 절차를 제공하여야 한다.

❍ 개인정보처리자는 개인정보 처리정지 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다.

- 이 경우 정보주체는 '개인정보 처리정지 요구서'를 받은 날부터 10일 이내에 처리정지 조치를 한 사실을 및 그 이유와 이의제기 방법을 기록한 개인정보 처리정지 요구에 대한 결과 통지서로 해당 정보주체에게 알려야 한다.

❍ 개인정보처리자가 정보주체로부터 개인정보 처리정지 요구를 받았을 때 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.

- 이 경우 개인정보처리자는 정보주체로부터 '개인정보 처리정지 요구서'를 받은 날부터 10일 이내에 처리정지 요구를 거절하기로 한 사실 및 그 이유와 이의제기 방법을 적은 '개인정보 처리정지 요구에 대한 결과 통지서'를 해당 정보주체에게 알려야 한다.

6.1.3	권리행사의 방법 및 절차

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
정보주체가 열람등 요구에 대한 거절 등 조치에 이의를 제기할 수 있도록 필요한 절차를 마련하여야 한다.	정보주체가 열람등(열람 및 존재확인) 요구에 대한 거절 등 조치에 대하여 이의사항이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하는가?
	정보주체의 열람, 정정·삭제, 처리정지 등의 요구를 받은 경우 적절한 방법으로 본인여부를 확인하는가?

❍ 열람등의 요구에 대한 거절 조치에 대하여 이의사항이 있는 경우 정보주체가 이의를 제기할 수 있도록 개인정보처리자는 필요한 절차를 마련하고 안내하여야 한다.

- 정보주체의 권리행사 방법 및 절차는 최소한 개인정보 수집절차 또는 회원가입 절차에 준해서 알기 쉽고 편리해야 하며, 개인정보 수집 시에 요구되지 않았던 증빙서류 등을 요구하거나 추가적인 절차를 요구해서는 안 된다.

❍ 개인정보처리자는 개인정보 열람요구, 정정·삭제요구, 처리정지 요구 등을 받은 때에는 열람등의 요구를 한 자가 본인이거나 적법한 법정대리인 여부를 확인하여야 한다.

- 대리인의 경우에는 대리인 자신에 관한 신원확인뿐만 아니라 정보주체와 대리인 사이의 대리관계를 증명할 수 있는 위임장 및 인감 또는 법정대리인의 경우에는 법정대리인임을 확인할 수 있는 서면(주민등록등본, 가족관계증명서 등)을 추가로 확인하여야 한다.

제7절 관리적 안전성 확보조치

❍ 개인정보 보호대책 구현을 위한 관리적 안전성 확보조치 심사영역은 개인정보 보호책임자 지정, 교육 및 훈련, 개인정보 유출사고 대응에 대한 보호조치 사항을 정하고 있다.

7.1 개인정보 보호책임자의 지정

7.1.1	개인정보 보호 책임자의 지정

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보 보호책임자를 지정하고, 적절한 책임, 권한 및 역할을 정의하여야 한다.	개인정보 보호책임자의 자격 요건은 법령에 따른 자격요건을 충족하는 자를 정하고 이에 적합한 자를 지정하고 있는가?
	개인정보 보호책임자의 개인정보 보호에 관한 역할 및 책임이 정의되었는가?
	개인정보 보호책임자는 개인정보 보호 역량을 강화하기 위해 노력하고 있는가?
	개인정보 보호책임자는 개인정보 보호와 관련한 법령의 위반사실을 알게 된 경우 개선조치 하였는가?

❍ 조직의 개인정보 보호를 책임지고, 정보주체의 개인정보 보호 및 고충처리를 담당하는 개인정보 보호책임자를 지정하여야 한다. 상시종업원 수가 5명 미만인 소상공인의 경우에는 지정하지 않을 수 있다.

❍ 개인정보 보호 책임자의 역할 및 책임에 대해 법 제31조제2항에서 요구하는 사항을 반영하여 개인정보 보호 관리계획에 명시하여야 한다.

❍ 개인정보 보호책임자는 외부교육 수강, 워크숍 및 컨퍼런스 참여 등을 통해 개인정보 보호 역량 강화를 위해 노력하여야 한다.

❍ 개인정보 보호책임자는 개인정보 보호와 관련하여 법률 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요 시 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다.

7.2 교육 및 훈련

7.2.1	교육 및 훈련 시행

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보 보호 인식제고 및 실제 운영에 필요한 교육·훈련 계획을 수립하여 이행하여야 하고, 교육의 대상 및 내용이 적절하여야 한다.	교육내용은 개인정보 보호 관련 법률 및 제도, 사내 규정, 관리적·기술적 조치사항 및 이를 수행하기 위한 방법 등 개인정보 취급자가 필수적으로 알아야 하는 사항을 포함하는가?
	개인정보 보호 교육 대상은 개인정보 보호책임자 및 개인정보취급자(수탁직원 포함)를 포함하는가?
	개인정보 보호정책의 중대한 변경, 신규입사자, 조직 내·외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생할 경우 추가 교육을 수행하는가?

❍ 개인정보취급자를 대상으로 매년 개인정보 보호 교육계획을 수립하여야 한다.

❍ 개인정보 보호 교육내용은 관련 법령, 규제, 사내규정, 보호조치 방법 등을 포함해야 하며, 특히 개인정보취급자가 정보주체의 개인정보를 유출할 경우에는 중벌에 처해진다는 사실을 주지시키는 것은 개인정보 보호책임자의 의무이므로 이러한 사항을 교육 내용에 포함해야 한다.

❍ 개인정보 보호 교육 대상은 개인정보 보호책임자, 개인정보취급자, 수탁자 등으로 한다.

❍ 개인정보 보호정책 및 조직의 변경, 보안사고 발생 등 개인정보처리자의 내·외부 환경에 중대한 변화가 있는 경우 추가교육을 실시하여야 한다.

7.2.2	교육 및 훈련 평가

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
개인정보 보호 교육 및 훈련 시행에 대한 기록을 남기고 그 결과를 평가하여 다음 교육 및 훈련에 반영하여야 한다.	개인정보 보호 교육 및 훈련이 계획에 따라 주기적으로 시행되고, 이에 대한 기록을 유지하는가?
	개인정보 보호 교육 및 훈련의 효과를 측정, 분석한 결과를 차기 교육계획에 반영하고 있는가?

❍ 개인정보 보호 교육계획에 따라 년 1회 이상 교육을 실시하고 그 기록을 유지하여야 한다.

❍ 개인정보 보호 교육 시 사전에 마련된 평가기준에 따라 결과를 측정하고, 측정된 결과를 분석하여 개선사항을 차기 계획에 반영하여야 한다.

7.3 개인정보취급자 관리

7.3.1	개인정보취급자 감독

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보취급자를 최소한으로 제한하고, 목록화하여 관리하여야 한다.	업무상 개인정보를 취급해야 하는 개인정보취급자는 최소한으로 제한하고 있는가?
	개인정보취급자 명단 관리 등 관리방안을 마련하고 있는가?

❍ 업무상 개인정보를 처리하는 개인정보취급자를 최소한으로 제한하고, 개인정보취급자의 개인정보 처리권한도 업무상 필요한 최소한으로 부여하여야 한다.

❍ 업무상 개인정보를 처리하는 개인정보취급자에 대해서는 목록으로 관리하여야 한다.

- 개인정보취급자 목록에는 개인정보 처리업무에 대한 위탁을 받은 수탁사의 개인정보취급자도 포함하여야 한다.

※ 수탁사의 개인정보취급자 중 개인정보처리시스템에 접근권한이 없는 개인정보취급자에 대한 목록관리는 수탁사 자체적으로 관리할 수 있다. 이 경우 관리·감독에 대한 부분은 <7.4.3 위탁자 관리·감독> 참조

7.3.2	보안서약서

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
조직에서 임직원들의 기밀정보 유출 위험을 최소화하고, 임직원에게 개인정보 보호에 대한 책임을 명확히 주지시키기 위해 보안	내부직원(정규직/계약직/임시직)의 개인정보 처리업무 시작 시 개인정보 보호에 관한 책임 및 의무를 고지한 개인정보 보호 서약서를 제출하도록 관리하고 있는가?

서약서에 서명토록 해야 한다.	개인정보를 처리하는 외부직원(위탁직원 포함) 등에 대하여 위탁계약서에 책임과 의무를 명시하고 개인정보 보호 서약서를 제출하도록 관리하고 있는가?

- ❍ 개인정보취급자는 최초 개인정보 처리업무를 할당받을 때 개인정보 보호서약서의 내용을 숙지하고 서명하여야 한다. 만약, 보안서약서에 개인정보 보호에 대한 책임 및 법적 처벌규정이 명시되었을 경우 보안서약서로 대체 가능하다.
- ❍ 제3자 등 외부 인원이 조직내부의 개인정보 처리시스템을 접근하는 일을 수행할 경우, 개인정보 보호에 관련된 사항을 계약서에 반영하여야 하며, 접근자에 대해 개인정보 보호 서약서에 서명을 받아야 한다.

7.4 위탁업무 관리

7.4.1	외부위탁계약

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
신청기관의 개인정보 처리업무를 외부 위탁하는 경우에는 개인정보 보호에 관한 요구사항 및 관리감독에 관한 사항을 계약서 등에 문서화하여야 한다.	개인정보 처리업무를 위탁하는 경우 문서화된 계약서 등에 의하여 이루어지고 있는가?
	위탁계약서에 위탁업무 목적 외 처리금지, 개인정보의 안전성 확보조치 등 법률에서 정한 사항들을 포함하고 있는가?

- ❍ 개인정보처리자는 개인정보 처리업무 위탁 시 계약서 및 서비스 수준 협약에 수탁사의 책임, 범위 등을 명시하고, 이에 근거하여 수탁사를 관리 감독하여야 한다.

❍ 위탁 계약을 체결하는 때에는 수탁자와 다음의 사항을 합의하여 계약서를 작성하여야 한다.

1. 위탁업무의 목적 및 범위
2. 재위탁 제한에 관한 사항
3. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
4. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
5. 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

7.4.2	정보주체고지

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보 처리업무 위탁시 관련 사항을 정보주체에게 알리고 필요한 경우 동의를 받아야 한다.	개인정보처리자(위탁자)는 정보주체가 언제든지 수탁자의 정보를 확인할 수 있도록 관보 또는 인터넷 홈페이지에 게재하는 등의 방법으로 공개하고 있는가?
	개인정보처리자(위탁자)가 재화 또는 서비스를 홍보하는 등 그 업무범위에서 제3자에게 업무를 위탁하는 경우, 위탁업무의 내용과 수탁자의 정보 등을 정보주체에게 서면, 전자우편 등의 방법으로 알리고 있는가?

❍ 개인정보 처리 업무를 위탁하는 개인정보처리자(위탁자)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(수탁자)를 정보주체가 언제든지 쉽게 확인할 수 있도록 자신의 인터넷 홈페이지(개인정보 처리방침 등)에 지속적으로 게재하는 방법으로 공개하여야 한다.

❍ 제3자에게 정보주체의 개인정보를 수집·보관·처리·이용·제공·관리·파기 등을 할 수 있도록 업무를 위탁하는 경우에는 다음 각 호의 사항을 정보주체에게 알려야 한다.

1. 개인정보처리 위탁을 받는 자(이하 수탁자)
2. 개인정보처리 위탁을 하는 업무의 내용

❍ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 서면, 전자우편, 모사전송, 전화, 문자전송 또는 이에 상당하는 방법으로 위탁하는 업무의 내용과 수탁자의 정보를 정보주체에게 알려야 한다.

※ 개인정보 처리업무 위탁시 동의를 받는 사항은 필수사항이 아님

7.4.3	위탁자 관리·감독	공공기관	대기업	중소기업	소상공인
		●	●	●	●

심사내용	세부내용
외부위탁 업체가 계약서 등에 명시된 사항을 충분히 이행하는지 주기적으로 관리 감독하여야 한다.	개인정보처리자(위탁자)는 수탁자가 개인정보를 안전하게 처리하는지를 주기적으로 감독하는가?
	개인정보처리자(위탁자)는 개인정보 처리목적을 미리 정하고, 수탁자가 처리목적을 벗어나서 정보주체의 개인정보를 처리하지 않도록 관리하는가?

❍ 개인정보처리자(위탁자)는 외부위탁 업체의 요구사항 준수여부를 정기적으로 보고 받고 관리 감독하며, 정기 및 수시점검 또는 감사를 수행하여야 한다.

※ 수탁자의 의무 : 개인정보 처리업무 수탁자는 개인정보 처리업무에 관하여 수집.이용, 제공, 보관 등과 관련하여 개인정보처리자에게 부과되는 의무를 준수하여야 함

- 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 개인정보 보호법을 위반하여 발생한 손해배상 책임에 대하여는 수탁자를 개인정보처리자(위탁자)의 소속직원으로 본다.

❍ 개인정보처리자(위탁사)는 개인정보 처리 목적을 미리 정하여야 하며, 수탁사는 이 목적을 벗어나서 정보주체의 개인정보를 처리하지 않아야 한다.

7.5 개인정보 유출사고 대응

7.5.1	개인정보 유출사고 대응계획 수립 및 운영

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
개인정보의 유출사고에 대응하기 위한 긴급 연락체계, 개인정보 보호 사고 발생 시 보고 및 대응 절차, 사고 대응 조직의 구성 등을 포함한 개인정보 사고 대응 계획을 수립하고, 계획에 따라 대응체계를 운영하여야 한다.	개인정보 유출사고 대응계획이 수립되어 있고, 대응계획에 역할 및 책임이 명확히 기술되어 있는 등 필요한 내용이 충분히 반영되어 있는가?
	개인정보 유출사고를 대응할 수 있는 체계를 구축하고 있으며, 모니터링 및 대응방법, 절차, 보고 및 승인 방법 등을 포함하고 있고 실제로 운영하고 있는가?

❍ 개인정보 유출사고의 정의 및 범위, 긴급연락체계 구축, 개인정보 사고 발생 시 보고 및 대응 절차, 사고 대응조직의 구성, 교육계획 등을 포함한 개인정보 유출사고 대응 절차 및 계획이 마련되어야 한다.

- 시스템 일시정지, 암호 등의 변경, 유출 원인 분석, 기술적 보안조치 강화, 시스템 변경, 기술지원 의뢰 및 복구 등과 같은 임시 대응조치에서부터 유사사고 발생 방지대책 수립 및 시행 등과 같은 피해 예방조치가 포함 될 수 있다.

❍ 개인정보 유출사실을 지체 없이 피해고객에게 통지하고, 피해고객으로부터 개인정보 유출로 인한 피해 현황을 접수받을 수 있는 창구를 마련해야 한다.

❍ 또한, 신속하고 적절한 피해확산을 방지하고 피해를 복구하기 위하여 개인정보 유출을 야기한 직·간접적인 사고발생 원인을 즉시 제거하고, 미비한 기술적·관리적·물리적 보호조치를 보완하며, 유출된 개인정보의 악용 또는 도용을 막을 수 있는 대책 마련(모니터링 및 대응방법, 절차, 보고 및 승인 방법)등의 조치를 취해야 한다.

7.5.2	개인정보 유출사고 대응

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
피해를 최소화하기 위한 적절한 보호조치를 마련하고, 개인정보 유출사고 대응 및 통지, 신고절차 및 방법에 따라 신속히 수행하여야 한다.	개인정보가 유출되었음을 알게 되었을 때, 지체 없이 해당 정보주체에게 유출사실을 알릴수 있는 체계를 마련하고 있는가?
	개인정보가 유출되었음을 알게 되었을 때, 정보주체에 대한 유출사실의 통지시기, 방법 및 절차 등을 적절하게 수립하고 있는가?
	1만 명 이상 정보주체의 개인정보가 유출된 경우, 개인정보처리자는 관계기관에 신고하기 위한 절차가 있는가?
	개인정보가 유출된 경우, 그 피해를 최소화하기 위한 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등의 보호조치를 마련하고 있는가?

❍ 개인정보 유출 및 침해사고 발생 시 피해확산을 방지하고 피해를 복구하기 위한 절차를 수립하여야 한다.

- 개인정보가 유출되었을 것으로 의심되는 개인정보처리시스템의 접속권한 삭제·변경 또는 폐쇄 조치
- 네트워크, 방화벽 등 대·내외 시스템 보안점검 및 취약점 보완 조치 후 수사에 필요한 외부의 접속기록 등 증거 보존 조치
- 정보주체에게 유출 관련 사실을 통지하기 위한 유출확인 웹페이지 제작 등의 통지방법 마련 조치
- 기타 개인정보의 유출확산 방지를 위해 필요한 기술적·관리적 조치

❍ 개인정보 유출되었음을 알게 되었을 때 지체 없이(5일 이내) 다음의 사항에 대하여 알려야 한다.

1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

❍ 1만 명 이상 개인정보가 유출된 경우 유출 통지 및 조치 결과를 지체 없이 안전행정부 또는 전문기관에 신고하는 절차가 수립돼 있어야 한다.

신고기관	• 안전행정부(개인정보 보호 종합지원시스템) • 한국정보화진흥원 • 한국인터넷진흥원
신고시기	5일 이내(정보주체에 대한 통지 및 조치결과 신고)
신고내용	기관명, 통지여부, 유출된 개인정보 항목.규모, 유출시점.경위, 유출피해 최소화 대책.조치 및 결과, 정보주체가 할 수 있는 피해 최소화 방법 및 구제절차, 담당부서, 담당자 및 연락처 등
신고방법	• 전자우편, 팩스 인터넷사이트를 통해 유출사고 신고 및 신고서 제출 • 시간적 여유가 없거나 특별한 사정이 있는 경우: 전화를 통하여 통지내용을 신고한 후, 유출 신고서를 제출할 수 있음

제8절 기술적 안전성 확보조치

❍ 개인정보 보호대책 구현을 위한 기술적 안전성 확보조치 심사영역은 개인정보의 안전한 처리를 위한 접근권한, 접속기록 관리, 접근통제, 운영관리, 개발보안, 암호화, 모니터링 등에 대한 보호조치 사항을 정하고 있다.

8.1 접근권한 관리

개인정보처리시스템에 대한 접근 권한은 서비스 제공을 위하여 필요한 최소한의 인원에게만 부여하고, 그 내역을 기록 관리 및 검토 하여야 한다.

8.1.1	개인정보취급자 등록

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보 처리시스템과 서비스에 접근을 허용하거나 취소하기 위한 공식적인 사용자 등록 및 해지절차를 마련하여야 한다.	개인정보처리시스템과 서비스에 접근을 허용하거나 취소하기 위한 공식적인 사용자 등록 및 해지 절차가 있는가?

❍ 개인정보취급자의 접근권한 등록 및 해지를 위한 공식적인 절차가 마련되어야 한다.

- 공식적인 절차라고 하면 “계정 등록/해지 신청서” 또는 온라인 신청서와 같은 양식을 통한 신청과 적절한 승인과정을 말하며, 이를 통해 증적 자료를 기록 보관 하여야 한다.
- 또한, 계약직, 외부인력, 단기 아르바이트에 대한 계정 발급 신청 과정이 정직원과 동일한 절차로 이루어 져야 한다.

8.1.2	개인정보취급자 권한관리

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보 처리시스템에 대한 접근 권한이 서비스 제공을 위하여 필요한 최소한의 인원에게만 부여하여야 하고, 기록을 보관하여야 한다.	개인정보 처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하고 있는가?
	개인정보취급자의 퇴직, 계약 종결 또는 직무 변경 시 접근권한을 제거 또는 변경하고 있는가?
	권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하고 있는가?
	하나의 계정으로 다수가 동일 시스템에 접속하거나 동시 접속할 수 없도록 조치하고 있는가?

❍ 개인정보 처리시스템에 대한 접근권한 부여는 최소한의 원칙에 따라 업무상 필요한 개인정보 보호책임자 또는 개인정보취급자에게만 부여하여야 하며, 업무에 따라 권한을 차등 부여 하는 기준을 마련하여 이에 따라 차등 부여 하여야 한다.

- 개인정보 처리시스템의 권한 등급은 개인정보취급자의 업무 분장, 직무기술에 따라서 적절하게 부여하여야 하며 허가된 접근권한이 적절한 지 검토하는 절차가 있어야 한다.

❍ 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보취급자의 접근권한을 변경 또는 말소 하여야 한다.

❍ 개인정보 처리시스템의 개인정보취급자 권한 부여, 변경 또는 말소에 대한 내역을 기록 관리하고 최소 3년간 보관하여야 한다.

- 기록 관리는 기관의 상황에 맞게 신청서 또는 관리대장 등 수기를 통한 방식과 개인정보처리시스템에서 자동으로 전자적 기록(로그)으로 남는 방식으로 운영할 수 있다.

❍ 개인정보취급자별로 한 개의 유일한 계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

- 또한, 하나의 계정으로 다수가 동일시스템에 동시 접속할 수 없도록 하여야 한다.

8.1.3	접근권한 검토

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
개인정보취급자에게 부여된 접근권한 현황에 대해 정기적으로 점검을 하여야 한다.	개인정보취급자의 접근권한을 주기적으로 검토하고 있는가?
	특수 접근권한의 할당이나 사용을 제한하고 주기적으로 점검하고 있는가?
	접근권한 검토 결과 적정성이 의심될 경우 그에 따른 조치가 이루어지고 있는가?

❍ 개인정보처리시스템에 대한 접근권한을 주기적으로 검토하는 절차를 수립하고 이행하여야 한다.

❍ 반드시 필요한 경우에만 특수 접근권한(개인정보처리시스템 관리자, 서버 관리자, DB관리자 계정 등)을 할당하여 사용을 제한하여야 하고 특수 접근권한을 부여 받은 계정은 식별이 가능하도록 하며 주기적으로 검토하여야 한다.

- 또한, 정보보호시스템(침입차단시스템 등), 응용프로그램 등의 관리자 계정 또한 특수 목적을 위한 계정으로 인식하고 관리하여야 한다.

❍ 다음과 같은 항목을 기준으로 접근권한 부여의 적정성을 검토하여 의심이 되는 경우에는 삭제, 회수 및 비활성화 등 그에 따른 조치를 취하여야 한다.

- 공식적인 절차에 따른 접근권한 부여 여부
- 접근권한에 대한 직무 및 보안정책 부합 여부

- 접근권한 부여 승인자에 대한 적절성
- 직무변경 시 접근권한 변경 여부
- 업무 목적 이외의 과도한 접근권한 부여

8.2 접속기록 관리

8.2.1	개인정보처리시스템 접속기록 관리

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보처리시스템의 접속기록은 보관되고, 보호조치에 의해 관리되어야 한다.	개인정보처리시스템의 접속기록이 위·변조되지 않도록 별도 저장장치에 백업 보관하고 있는가?
	개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관·관리하고 있는가?

❍ 개인정보처리시스템의 접속기록은 위·변조 되지 않도록 별도 저장장치에 백업하여 보관하고, 분실되지 않도록 안전하게 보관하여야 한다.

❍ 개인정보취급자가 개인정보처리시스템에 접근한 접속기록, 위탁업체 및 제3자의 개인정보처리시스템에 접속에 대한 일시, 내역 등 접속기록을 최소 6개월 이상 저장하여야 한다.

8.2.2	접속기록 검토

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
개인정보 열람기록 및 처리기록을 주기적으로 분석하고 검토하여야 한다.	개인정보취급자의 열람 기록 및 접속기록을 분석하고 주기적으로 검토하고 있는가?

❍ 개인정보 열람기록을 주기적으로 검토하여 반복적인 권한 없는 열람 시도뿐만 아니라 권한이 있는 열람의 경우에도 추이분석 등을 통하여 오남용으로 나타날 수 있는 이상 징후를 찾아 점검하여야 한다.

- 열람이 허가된 개인정보취급자의 경우에도 오남용을 방지하기 위하여 개인정보 열람에 대한 취급자, 일시, 대상 등의 기록을 남겨야 한다.

※ 개인정보취급자의 열람/접속 기록은 오류 및 부정행위가 발생하거나 예상되는 경우 즉각적인 보고 및 대응 조치를 하고 기록관리 하여야 한다.

8.3 운영보안

8.3.1	비밀번호 관리

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보처리시스템 접속 시 안전한 비밀번호를 사용하여야 한다.	개인정보취급자가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 관리 절차를 수립하고 있는가?
	개인정보취급자가 비밀번호관리 절차를 이행하고 있는가?

❍ 개인정보취급자의 안전한 비밀번호 사용을 위해 패스워드 작성규칙, 변경주기 등을 포함한 관리절차를 수립하여야 한다.

❍ 개인정보취급자는 자신의 개인정보처리시스템과 패스워드 관리 책임이 자신에게 있음을 주지하여야 한다.

8.3.2	악성소프트웨어 통제

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
바이러스 등의 악성 소프트웨어로부터 개인정보처리시스템을 보호하기 위해 악성 소프트웨어들을 예방하고 탐지, 대응하는 대책을 이행하여야 한다.	악성 소프트웨어를 차단하기 위한 관리방안을 수립하고 이행하고 있는가?
	백신 소프트웨어 등 보안프로그램은 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하도록 설정하고 있는가?
	개인정보처리시스템, 개인정보취급자의 PC에 P2P, 웹 하드 등과 같은 비인가 프로그램 설치를 금지하고 있는가?

❍ 바이러스 등의 악성 소프트웨어로부터 정보시스템을 보호하기 위한 관리 방안 및 절차를 수립하고 이행하여야 한다.

※ 소상공인의 경우 본 세부내용은 제외함.

❍ 백신 소프트웨어 등은 자동 업데이트 기능을 활용하거나, 또는 일 1회 이상 업데이트를 실시하도록 설정하여 항상 최신의 상태가 유지 될 수 있도록 한다.

❍ 개인정보처리시스템 및 개인정보취급자의 PC는 개인정보 유출을 방지하기 위해 P2P, 웹하드 등 비인가 프로그램 설치를 금지하여야 한다.

- 또한, 인터넷 홈페이지 접속, P2P, 메신저 등을 이용한 파일 전송 및 공유설정이 제한되도록 설정하여야 한다.

※ 소상공인의 경우 본 세부내용은 제외함.

8.3.3	개인정보처리시스템에 대한 보호조치 활동

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
비인가 접근 시도 등의 모니터링 및 기술적 취약점 점검을 지속적으로 수행하여야 한다.	개인정보처리시스템으로의 비인가 접근 시도에 대해 모니터링을 수행하고 있는가?
	개인정보처리시스템에 대해 기술적 취약점 점검을 주기적으로 수행하고 있는가?

❍ 비인가 접근 시도에 대해서 주기적인 모니터링을 수행하여야 한다.

- 모니터링 대상 및 검토주기, 보고 절차 등을 포함한 내부 지침을 마련하고 정해진 주기에 따라 정기적으로 점검을 실시하여야 한다.

❍ 개인정보처리시스템에 대한 기술적인 보안점검을 주기적으로 수행하여야 하며, 홈페이지 등에 개인정보 노출 방지 등을 위해서 취약점 점검, 모니터링 등의 안전성 확보에 필요한 조치를 주기적으로 수행하여야 한다.

- 기술적 취약점 점검은 라우터나 스위치 등 네트워크 취약점 분석, 방화벽 등 보안시스템 취약점 분석, 웹서비스 취약점 분석, 모의침투 테스트 등의 사항을 포함한다.

8.3.4	개인정보 표시제한

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
개인정보 처리업무를 목적으로 개인정보 조회, 출력 등의 업무 수행 시, 개인정보 마스킹을 통해 개인정보 표시제한을 수행하여야 한다.	개인정보의 조회, 출력 시 마스킹 등 개인정보 표시를 제한하는 기준을 정하고 이를 시행하고 있는가?

❍ 개인정보 업무처리를 목적으로 개인정보 조회, 출력 등의 업무를 수행하는 과정에서 개인정보 표시를 제한하기 위한 마스킹 기준을 정하고 이를 시행하여야 한다.

개인정보 표시제한(예시)
성 명 : 홍 * 동 전화번호 : 02 - *** - 1234 주 소 : 서울 종로구 ***동 12-3 생년월일 : **** 년 * 월 * 일 이동전화 : 010 - **** - 12** 접속 IP : 123.***.***.123

8.3.5	접근통제시스템 설치 및 운용

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 침입차단 및 탐지 기능을 포함한 시스템을 설치 운용하여야 한다.	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 기관의 상황에 맞는 접근통제(침입차단 및 탐지기능 등)시스템을 설치하여 운영하고 있는가?
	정보통신망을 통한 불법적인 외부 접근 및 내·외부자에 의한 정보유출 등을 모니터링하기 위해 접근통제시스템의 접근제한 정책 및 로그를 수집하고, 정기적으로 점검하고 있는가?

❍ 개인정보처리시스템은 침해사고를 방지하기 위해서는 상황에 맞는 침입차단 및 침입탐지시스템 등에 의해 보호되어야 한다.

- 침입차단시스템(Firewall), 침입탐지시스템(IDS), 침입방지시스템(IPS), 웹방화벽 또는 보안 운영체제(Secure OS) 등을 도입할 수 있다.
- 스위치 등 네트워크 장비에서 제공하는 접근제어목록(Access Control List) 등 기능을 이용하여 IP 주소 등을 제한함으로써 침입차단 기능을 구현할 수 있다.

- 공개용(무료) S/W를 사용하거나, 운영체제(OS)에서 제공하는 기능을 활용하여 해당 기능을 포함한 시스템을 설치·운영할 수 있다. 다만, 공개용(무료) S/W를 사용하는 경우에는 적절한 보안이 이루어지는지를 사전에 점검하여야 한다.

※ 개인정보처리시스템이 아닌 업무용 컴퓨터에 개인정보를 저장하는 기관의 경우 접근통제시스템이 아닌 보안프로그램이나 운영체제에서 제공하는 접근통제 기능을 사용하여 불법적인 접근을 차단할 수 있다.

❍ 정보통신망을 통한 불법적인 외부 접근 및 내·외부자에 의한 정보유출 등을 모니터링하기 위해 접근통제시스템의 로그를 수집하여 정기적으로 점검하여야 한다.

- 시스템 로그파일은 불법적인 접근시도 여부를 확인하는 유용한 정보를 제공하므로 접근통제시스템의 로그파일을 일정기간 동안 저장하고 정기적으로 점검하여야 한다.
- 정보통신망을 통해 개인정보처리시스템에 접근을 시도할 때에는 접속자의 PC 또는 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하여야 한다.
- 접근통제 시스템을 통하여 개인정보취급자 PC 또는 IP주소의 접근을 허가/제외할 때에는 적절한 승인 절차를 포함해야 하며 운영 내역을 기록관리 하여야 한다.

8.3.6	네트워크 접근통제

공공기관	대기업	중소기업	소상공인
●	●		

심사내용	세부내용
네트워크 접근통제를 강화하기 위해 기술적 보호조치를 마련하여야 한다.	네트워크 접근통제 정책을 수립하여 주기적으로 점검하고 있는가?
	개인정보 자산 중요도에 따라 네트워크를 논리적 또는 물리적으로 분리하여 운영하고 있는가?
	중요 개인정보취급자의 업무용 PC는 인터넷을 차단하는 등의 보호조치를 취하고 있는가?

- ❍ 인가된 사용자, PC 만이 네트워크에 접근하여 개인정보처리시스템 등에 접근할 수 있도록 네트워크 접근통제 정책을 수립하고 정기적인 점검을 수행하여야 한다.
- ❍ 핵심 업무영역의 네트워크는 물리적 또는 논리적으로 분리하여 인터넷 구간에서 직접 접근 할 수 없도록 통제·차단하여야 한다.
- ❍ 외부로부터의 접근이 불가피한 웹서버 등 공개용 서버는 공개서버를 경유하여 내부 망으로의 접근이 이루어지지 않도록 접근통제를 수행하여야 하며, 웹서버 자체 보호를 위해 웹 방화벽을 설치할 수 있다.
- ❍ 중요 개인정보취급자의 업무용 PC는 물리적 또는 논리적으로 인터넷을 차단하는 등의 보호조치를 취하여야 한다.

※ 중요 개인정보취급자란 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나, 개인정보처리시스템의 접근권한을 설정할 수 있는 개인정보취급자이다.

8.3.7	네트워크 운영관리

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
내부 네트워크를 통한 개인정보처리시스템 관리 시 특정 단말에서만 접근을 할 수 있도록 제한하고, 인터넷 등 외부 네트워크를 통한 개인정보처리시스템의 접속 시 보호대책을 마련하여야 한다.	내부 네트워크를 통한 개인정보처리시스템 관리 시 특정 단말에서만 접근할 수 있도록 제한하고 있는가?
	인터넷 등 외부 네트워크를 통한 개인정보처리시스템의 접속 시 VPN 또는 전용선 등의 안전한 접속수단을 사용하고 있는가?

❍ 내부 네트워크에서 개인정보처리시스템을 관리하는 경우 관리자 단말 또는 특정 IP를 통해서만 접근을 하도록 제한하여야 한다.

❍ 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하여야 한다.

- 개인정보취급자가 VPN을 이용하여 내부망의 개인정보처리시스템에 접근할 때에는 VPN 연결 시 인터넷을 차단하는 기능을 사용하여 개인정보처리시스템을 통한 업무자료나 내용이 인터넷을 통해 유출되지 않도록 인터넷망을 차단하여야 한다.

8.4 암호화 통제

8.4.1	암호화 계획 수립

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
개인정보 보호를 위한 암호화 계획을 수립해야 하고 포함된 내용은 법적 요건을 충족하여야 한다.	고유식별정보, 바이오정보, 비밀번호 등 주요 개인정보 보호를 위한 암호화 계획을 수립하고 있는가?
	암호화 계획에 포함된 암호화 대상 및 암호화 방법을 명확하게 정의하여 법적 요건을 만족하고 있는가?

❍ 개인정보를 암호화하기 위한 계획 또는 지침 등을 문서화 하고 관리하여야 한다.

- 암호화 계획은 아래 사항을 포함해야 하며, 본 계획에 따라 개인정보를 저장, 전송, 원격 접속 시에 암호화를 수행해야 한다.

암호화 계획에 포함되어야 되는 내용(예시)
1. 개인정보 현황분석 - 기관 및 서비스에서 사용 중인 개인정보 종류, 규모, 보유기간 등의 현황과 처리 과정상 유지 관리되어야 하는 관리적.기술적 보호조치 현황 분석. 2. 개인정보 위험도 분석(또는 영향평가 절차) 및 방법 - 개인정보 영향평가 실시 대상 기관의 경우 영향평가 절차 및 방법을 그 외에 기관은 위험도 분석 절차 및 방법을 작성함. 3. 암호화 추진 일정 등 - 영향평가.위험분석 시행시기 및 암호화 구축 및 관리시기 등을 포함한 세부 추진 일정

❍ 암호화 계획은 패스워드에 대한 일방향 암호화 기준, 주민등록번호 등의 고유식별번호에 대한 안전한(양방향) 암호화 알고리즘의 기술 기준 등을 포함하는 법적 요구사항을 만족해야 한다.

8.4.2	암호화 적용

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보 저장 및 전송 시, 원격접속 시 암호화를 수행하여야 한다.	인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 고유식별정보, 바이오정보, 비밀번호를 저장하는 경우 암호화를 하고 있으며, 내부 망에 저장하는 경우 위험도분석 등을 통해 암호화 또는 암호화에 상응하는 조치를 하고 있는가?
	업무용 컴퓨터에 고유식별정보를 저장하여 관리하는 경우 암호화하고 있는가?
	개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우 고유식별정보, 바이오정보, 비밀번호를 암호화하고 있는가?
	원격작업을 통해 내부시스템 접근 시, VPN 등을 통한 암호화 통신을 사용하고 있는가?
	고유식별정보, 바이오정보, 비밀번호 등의 개인정보를 암호화 할 경우 안전한 알고리즘을 사용하고 있는가?

❍ 인터넷 구간, DMZ 구간에 고유식별정보, 비밀번호 및 바이오정보 등 주요 개인정보를 저장하는 경우에는 반드시 암호화 하여 저장하여야 하며, 내부망 구간에 저장하는 경우에는 “개인정보 위험도 분석 기준”을 따르는 보호조치를 하여야 한다.

- 인터넷이 직접 연결되는 인터넷 구간과 인터넷 구간과 내부망 구간 사이에 위치하고 침입차단시스템 등으로 접근을 제한하고 있는 DMZ 구간에 있는 개인정보처리시스템은 외부에서 직접 접근이 가능하므로 주요 개인정보는 반드시 안전한 알고리즘으로 암호화 하여 저장 하여야 한다.

- 내부망 구간에 고유식별번호를 저장하는 경우는 위험도 분석기준 및 절차에 따라 암호화 여부를 정하고 암호화 또는 암호화에

상응하는 조치를 하여야 한다.

❍ 업무용 컴퓨터에 고유식별번호를 저장하는 경우에는 암호화하여 저장하여야 한다.

- 또한, 개인정보처리시스템에서 개인정보취급자의 PC에 다운로드 받아 저장할 때에도 안전한 알고리즘이 적용된 암호화 프로그램 등을 통해 암호화 후 저장하여야 한다.

❍ 개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화 하여야 한다.

- 웹 서버를 통해 전달하는 경우에는 SSL 인증서를 설치한 보안서버를 구축하여 전송하며, 보안USB등의 암호화된 보조저장매체를 사용하여야 한다.

❍ 원격작업을 통해 외부 인터넷망 등을 경유하여 내부 네트워크에 접속할 경우 적절한 식별, 인증, 접근통제, 암호화 대책(VPN 등 포함)이 수립되어야 한다.

❍ 고유식별번호, 비밀번호 등 중요 개인정보에 대해서는 안전한 알고리즘으로 암호화하여 저장하여야 한다. 비밀번호의 경우 복호화 되지 않도록 일방향 암호화 하여야 한다.

<안전한 암호화 알고리즘 예시>

구 분	알고리즘 명칭
대칭키 암호 알고리즘	ARIA-128/192/256 AES-128/192/256 Blowfish Camelia-128/192/256 MISTY1 KASUMI 등
공개키 암호 알고리즘	RSA KCDSA(전자서명용) RSAES-OAEP RSAES-PKCS1 등
일방향 암호 알고리즘	SHA-224/256/384/512 Whirlpool 등

<출처> "암호 알고리즘 및 키길이 이용 안내서(KISA)"

8.5 개발 보안

8.5.1	개인정보 영향평가

공공기관	대기업	중소기업	소상공인
●			

심사내용	세부내용
개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 수행하여야 한다.	개인정보처리시스템 개발 및 변경 시 개인정보 영향평가의 필요성 여부를 사전에 검토하는 절차를 수립하고 있는가?
	개인정보 영향평가 필요성 여부를 반영하여 영향평가를 수행하고 있는가?
	공공기관의 장은 개인정보 영향평가서를 안전행정부장관에게 제출하고 있는가?
	개인정보 영향평가 결과에 따른 개선요구사항에 대한 이행여부를 관리하고 있는가?

❍ 개인정보처리시스템의 구축 또는 변경 시 설계·분석 단계에서 개인정보 영향평가의 필요성을 사전에 검토하는 절차를 수립하여야 한다.

- 개인정보처리자는 사전 검토단계를 통해 '영향평가 필요성 검토 질문서' 또는 '사전 모의 영향평가' 등을 수행하며 영향평가 추진의 필요성 및 개인정보의 신규 수집·이용·연계 또는 처리절차상 변경 등의 발생 여부를 파악하여야 한다. 이러한 절차를 통해 나타난 결과와 내부 자원 등을 고려하여 개인정보 영향평가 수행 여부를 결정하여야 한다.

❍ 영향평가 사전검토단계를 통해 개인정보 영향평가의 필요성을 반영하여 개인정보 영향평가를 수행하여야 한다.

- 개인정보처리자는 개인정보 영향평가 수행을 위해 관련 예산을 확보하고, 영향평가 기관을 선정하여야 하며, 개인정보에 미치는 영향(Impact)에 대하여 사전에 조사·예측·검토해 개선방안을 도출한 영향평가 보고서를 작성하여야 한다.

❍ 개인정보처리자는 개인정보파일의 운용으로 인하여 정보주체의

개인정보 침해가 우려되는 개인정보처리시스템 구축 및 변경개발 등의 경우 영향평가를 수행하고, 그 결과를 안전행정부장관에게 제출하여야 한다.

❍ 개인정보처리시스템 개발 및 개선 계획 시 개인정보 영향평가를 수행하여 도출된 보완 및 개선 요구사항들이 적절하게 이행되고 있는지 점검하여야 한다.

- 개인정보처리자는 개인정보 침해요인별 조치내역을 확인·점검하고 적절하게 수행되었는지를 파악해야 하며, 조치 완료된 경우 기관장의 검토 또는 승인을 획득해야 한다. 필요시 조치내역서는 기관장의 승인을 득하여 안전행정부장관에게 제출해야 한다.

8.5.2	개발 시 보안조치

공공기관	대기업	중소기업	소상공인
●	●		

심사내용	세부내용
개인정보처리시스템 개발 시 보안 요구사항에 따라 구현 및 시험 등에 적절한 보호조치를 마련하여야 한다.	개인정보처리시스템 개발 및 변경 시 보안 요구사항을 정의하고 있는가?
	개인정보처리시스템 개발 및 변경 시 안전한 코딩방법에 따라 구현하고 있는가?
	운영데이터를 테스트데이터로 사용하는 경우 개인정보를 익명화하고 있는가?
	개발환경과 운영환경을 분리하여 운영하고 있는가?
	외부용역을 통한 개인정보처리시스템 개발 시 보안규정에 따라 관리감독하고 있는가?
	개인정보처리시스템 개발 및 변경에 대한 보안 요구사항 이행여부를 점검하고 있는가?

❍ 개인정보처리시스템 개발 및 변경 시 적절한 보호조치를 위한 개발 보안 요구사항을 정의하여야 한다.

- 보안 요구사항에는 개인정보 보호를 위한 법적 요구사항 등이 포함되어야 하고 분석 및 설계 단계에서 정의된 보안 요구사항에 따라 검토되어야 한다.

❍ 개인정보처리시스템 개발 및 변경시 안전한 소프트웨어 개발을 위해 소스코드 등에 존재할 수 있는 잠재적인 보안취약점을 제거하고, 보안을 고려하여 기능을 설계·구현하여야 한다. 안전한 소프트웨어 개발을 위해 다음과 같은 활동을 포함할 수 있다.

- 안전한 코딩 표준 정의
- 소프트웨어 개발보안 가이드
- 소스코드 보안약점 진단
- 실행코드 보안취약점 진단 등

❍ 개인정보가 포함된 운영 데이터를 테스트 데이터로 사용하지 않도록 하여야 한다.

- 단, 불가피하게 운영 데이터를 테스트 데이터로 사용하는 경우에는 변환처리를 통한 익명화, 운영 시스템과 동일한 접근통제 정책 수립 등의 보호대책을 강구하여야 한다.

❍ 원칙적으로 개발과 운영 환경을 분리하여야 한다.

- 운영환경에서의 개발 시 운영시스템의 성능 및 용량에 영향을 줄 수 있으며, 승인받지 않은 개발자가 운영시스템에 접근하는 등 보안사고 위험을 줄이기 위하여 개발, 테스트 및 운영환경을 분리하여 한다.

❍ 외부 용역을 통한 개인정보처리시스템 개발 및 변경 시 신청기관의 내부 보안요구사항을 준수하도록 관리 감독 하여야 한다.

❍ 개인정보처리시스템 개발, 변경 후 개발 보안요구사항을 이행하였는지 점검하여야 한다. 또한 아래 사항을 포함하여 점검하고 발견한 취약점을 조치하고 있는지 확인하여야 한다.

- 개발자 계정 및 권한 삭제여부

- 테스트 데이터 익명화 및 삭제 여부
- 소프트웨어 보안취약점 제거여부
- 소프트웨어 보안취약점 발견사항 조치여부 등

제9절 물리적 안전성 확보조치

❍ 개인정보 보호대책 구현을 위한 물리적 안전성 확보조치 심사영역은 CCTV의 설치 및 운영에 대한 보호조치 및 물리적 출입통제 등에 대한 보호조치 사항을 정하고 있다.

9.1 영상정보처리기기 관리

9.1.1	영상정보처리기기의 설치·운영 제한

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
영상정보처리기기 설치·운영 시, 적절한 보호조치를 마련하여야 한다.	공공기관의 장은 영상정보처리기기를 설치하는 경우 관련 전문가 및 이해관계인의 의견을 수렴하고 있는가?
	공개된 장소에 영상정보처리기기를 설치·운영할 때 적법한 이유로 설치하고 있는가?
	영상정보처리기기 운영자는 영상정보관리책임자를 지정하고 있으며, 영상정보처리기기 운영·관리 방침을 마련하여 점검하고 있는가?
	설치 운영 중인 영상정보처리기기를 설치 목적에 맞게 사용·관리하고 있는가?
	영상정보처리기기를 설치·운영 할 경우 정보주체가 쉽게 인식할 수 있도록 안내판을 설치하고 있는가?

❍ 공공기관은 공개된 장소에 영상정보처리기기를 설치·운영하려는 경우 다음에 해당하는 절차를 거쳐 전문가 및 이해관계인의 의견을 수렴하여야 한다.

- 「행정절차법」에 따른 행정예고의 실시 또는 의견 청취
- 해당 영상정보처리기기의 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회·설문조사 또는 여론조사

※ 개인 사생활 침해우려 장소에 영상정보처리기기를 설치·운영하려는 경우 다음의 사람으로부터 의견을 수렴하여야 한다.

. 관계 전문가

. 해당 시설에 종사하는 사람, 해당 시설에 구금되어 있거나 보호받고 있는 사람 또는 그 사람의 보호자 등 이해관계인 등

❍ 공개된 장소에 영상정보처리기기를 설치·운영하지 않아야 한다. 단, 다음과 같이 법률에서 정하는 경우에는 예외로 한다.

- 법령에서 구체적으로 허용하고 있는 경우
- 범죄의 예방 및 수사를 위하여 필요한 경우
- 시설안전 및 화재 예방을 위하여 필요한 경우
- 교통단속을 위하여 필요한 경우
- 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

❍ 영상정보처리기기 운영자는 설치근거 및 목적, 대수 및 촬영범위 등 영상정보처리기기 운영·관리 방침을 마련하여야 한다.

- 영상정보처리기기 운영·관리 방침은 원칙적으로 영상정보처리기기 운영자의 인터넷 홈페이지에 지속적으로 게재해야 하며, 인터넷 홈페이지에 게재할 수 없는 경우에는 정보주체가 쉽게 확인할 수 있는 방법으로 영상정보처리기기 운영·관리 방침을 공개해야 한다.

❍ 영상정보처리기기 운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비출 수 없도록 하고, 녹음기능은 사용해서는 안 된다.

❍ 영상정보처리기기 운영자는 정보주체가 쉽게 인식할 수 있도록 다음 사항을 기재한 안내판을 설치하여야 한다.

- 설치목적 및 장소
- 촬영범위 및 시간
- 관리책임자의 성명 또는 직책 및 연락처
- 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 수탁자의 명칭 및 연락처

9.1.2	영상정보처리기기의 설치·운영 사무의 위탁 관리

공공기관	대기업	중소기업	소상공인
●	●		

심사내용	세부내용
영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 적절한 위탁절차를 마련하여야 한다.	영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 위탁하는 절차 및 요건에 맞게 계약서 및 관련서류를 점검하고 있는가?
	영상정보처리기기의 설치 및 관리에 관한 사무를 위탁한 경우, 안내판에 수탁기관의 명칭 등을 포함하고 있는가?

❍ 공공기관이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 다음의 내용이 포함된 문서로 하여야 하며, 안내판에 수탁자의 명칭 및 연락처를 게재하여야 한다. 대기업의 경우에는 이에 준하는 위탁 절차를 마련하여야 한다.

1. 위탁하는 사무의 목적 및 범위
2. 재위탁 제한에 관한 사항
3. 영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
4. 영상정보의 관리 현황 점검에 관한 사항
5. 위탁받는 자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

9.2 물리적 보안관리

9.2.1	출입통제 및 사무실 보안

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보를 취급하는 공간에 대해 출입통제 등 물리적 보호조치를 취하고 접근 가능한 인원은 허가받은 인력에 한해 최소화하여야 한다.	전산실, 자료보관실 등 개인정보를 보관하고 있는 시설 및 장비를 보호하기 위한 출입통제 절차를 수립하고 있는가?
	전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 장소의 출입통제는 허가받은 인력에 한하며, 관련 출입기록을 보관하고 있는가?
	개인정보를 포함하고 있는 중요 문서, 출력물, 저장매체가 책상 등에 노출되지 않도록 보호하고 있는가?

❍ 개인정보처리 및 저장시설, 장비, 사무실, 보관소 등을 보호하기 위한 보호 구역을 정의하고 보호구역에 대한 물리적 접근을 통제하기 위한 대책을 마련하여야 한다.

- 보호구역이 필요한 보안등급에 따라 정의되고 각각 등급에 맞는 보안조치와 절차를 수립하여야 한다.

예) 접견구역 : 외부인 출입 허용구역
제한구역 : 내부직원 및 허가된 외부직원 출입 구역
통제구역 : 개인정보처리시스템 집적장소(서버실, 문서 등)

❍ 개인정보를 보관하는 전산실, 자료보관실 등 보호구역에 대한 출입통제기록을 남겨 허가받은 인력에 한해 출입이 통제되도록 해야 하며, 접근기록을 보관하고, 주기적으로 타당성을 검토해야 한다.

- 비인가자의 보호구역 출입 시에는 출입목적, 출입시간, 출입자 연락처 등을 포함해 기록하여야 하며, 주기적으로 출입내역을 검토하여야 한다.

❍ 중요문서 등이 책상이나 사무 공간 등에 방치되지 않도록 클린데스크를 통해 개인정보 노출을 최소화 하여야 한다.

- 업무용 PC의 화면보호기능(동작시간, 암호 등)을 설정하고 이석 시 중요 개인정보 문서 및 보조저장매체는 책상위에 방치하지 않아야 하고, 퇴근 시 주요 개인정보 등은 잠금장치가 있는 안전한 곳에 보관하는 등의 지침을 마련하고 이행하여야 한다.

9.2.2	이동컴퓨팅 보안관리

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
이동컴퓨팅 기기 사용 시에 개인정보를 보호하기 위한 보호정책을 수립하고, 내부 네트워크로의 연결 및 공공장소에서의 사용에 대한 정책을 마련하여야 한다.	이동컴퓨팅 기기 사용 시 개인정보 보호를 위한 보호정책을 수립하고 있는가?
	이동컴퓨팅 기기의 분실 시 개인정보의 유출 방지를 위한 암호화, 장비보호를 위한 물리적 보호조치 등 보호대책을 마련하고 있는가?
	이동컴퓨팅 기기를 내부 네트워크 연결 및 공공장소에서 사용 시 개인정보 보호대책을 마련하고 있는가?

❍ 이동 컴퓨팅 기기의 사용 시에 개인정보를 보호하기 위한 정책을 마련하여야 한다.

- 보호정책은 이동 컴퓨터 기기의 물리적 보호, 접근제어, 데이터의 암호화, 백업, 바이러스 정책, 내부네트워크와의 연결, 분실 시 정보 유출 방지를 위한 암호화, 장비보호를 위한 물리적 로깅장치, 분실 컴퓨터의 추적 등을 포함할 수 있다.

❍ 이동 컴퓨팅 기기의 분실 시 정보의 유출 방지를 위한 암호화, 장비보호를 위한 물리적 로깅장치, 분실 컴퓨터의 추적 등의 보호대책을 수립하여야 한다.

- 보호대책은 개인정보가 포함된 문서의 암호 설정, 이동 컴퓨팅

기기의 부팅 시 패스워드 설정, 필요시 물리적 잠금장치 사용 등을 포함하여야 한다.

❍ 이동 컴퓨팅 기기를 공공장소에서 사용하거나 이동 컴퓨터 기기를 통해 내부 네트워크 연결 시 개인정보 보호를 위해 다음을 포함한 절차가 마련되어 있어야 한다.

- 이동 컴퓨팅 기기 사용에 대한 절차
- 물리적 보호, 접근제어, 암호화, 백업, 바이러스 보호에 대한 절차
- 내부 네트워크로의 연결 절차

9.2.3	개인정보처리시스템 저장매체 폐기

공공기관	대기업	중소기업	소상공인
●	●	●	

심사내용	세부내용
개인정보처리시스템 폐기 또는 재사용 시 개인정보를 담고 있는 하드디스크, 스토리지, 테이프 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 개인정보는 복구 불가능하도록 완전히 삭제하여야 한다.	개인정보처리시스템의 저장매체에 대한 유출, 오용을 방지하기 위한 매체의 폐기 및 재사용에 대한 절차를 수립하였는가?
	저장매체의 폐기 또는 재사용 시 개인정보는 복구 불가능하게 삭제하고 그 이력을 남기고 있는가?

❍ 허가되지 않은 유출이나 오용으로부터 개인정보를 보호하기 위해, USB, 이동식 하드 디스크 등 이동식 저장매체의 폐기 및 재사용을 포함한 사용 절차를 수립하고 운영하여야 한다.

- 개인정보 저장 매체의 폐기 시에 감사증적을 위해 폐기일, 폐기내용, 폐기자 등을 포함한 관련정보를 기록 절차
- 외부계약자가 매체를 폐기할 경우에는 사진 확인 또는 실사과정을 포함한 명확한 폐기 확인 절차
- 즉시 폐기가 이행되지 않을 때에는, 폐기 시까지 노출을 차단하도록 안전한 매체보관 절차

9.2.4	휴대용 저장매체 관리

공공기관	대기업	중소기업	소상공인
●	●		

심사내용	세부내용
개인정보 유출을 예방하기 위해 외장하드, USB, CD 등 휴대용 저장매체 취급, 보관, 폐기 및 재사용에 대한 절차를 수립하여야 한다. 또한 매체를 통한 악성코드 감염 방지대책을 마련하여야 한다.	외장하드, USB, CD 등 휴대용 저장매체 취급, 보관, 폐기, 재사용에 관한 관리절차를 수립하고 있는가?
	휴대용 저장매체를 통한 악성코드 감염 및 개인정보의 유출 방지 대책을 수립하고 있는가?

❍ 개인정보를 담고 있는 휴대용 저장매체 관리를 위한 공식적인 절차를 수립하여 개인정보 유출을 효과적으로 예방하여야 한다.

- 휴대용 저장매체 사용범위: 통제구역, 제한구역 등 보호구역별 저장매체 사용 절차
- 휴대용 저장매체 등록절차
- 휴대용 저장매체 반입·출 절차
- 휴대용 저장매체 재사용 및 폐기 절차
- 휴대용 저장매체 보호대책 등

※ 관리적인 보호대책(사전 승인 및 사후 모니터링)만으로는 휴대용 저장매체를 통한 개인정보유출을 차단하기 어려우므로 기술적인 대책(DLP, DRM 등)을 마련할 수 있다.

❍ 휴대용 저장매체를 통한 악성코드 감염 및 개인정보 유출을 방지하기 위해 허가되지 않거나 불분명한 소스, 네트워크 등으로 부터 다운로드를 금지하기 위한 대책을 수립하여야 한다.

- 부득이 하게 다운로드를 받을 경우 해당 소프트웨어는 바이러스 검사를 필수적으로 받게 하는 등의 대책을 적용하여야 한다.

9.2.5	저장매체의 보관

공공기관	대기업	중소기업	소상공인
●	●	●	●

심사내용	세부내용
개인정보가 포함된 저장매체를 안전한 장소에 보관하여야 한다.	개인정보가 포함된 저장매체를 잠금장치가 있는 안전한 장소에 보관하고 있는가?

❍ 개인정보가 포함된 문서나 보조기억매체들은 잠금장치가 부착되어 있는 안전한 장소에 보관되어야 한다.

- 보조기억매체는 이동형 하드디스크, USB메모리, Flash메모리, CD, DVD 등을 포함한 저장매체로 금고 또는 잠금장치가 있는 캐비닛 등에 안전하게 보관하여야 한다.

[부록 1] 관련 서식

[별지 제1호 서식] 개인정보 보호 인증신청서
[별지 제2호 서식] 개인정보 보호 인증신청 내역서
[별지 제3호 서식] 개인정보 보호 인증신청 접수증
[별지 제4호 서식] 개인정보 보호 인증심사 계약서
[별지 제5호 서식] 인증심사 실시계획서
[별지 제6호 서식] 인증심사 부적합 보고서
[별지 제7호 서식] 인증심사 보완요청서
[별지 제8호 서식] 인증심사 보완조치 내역서
[별지 제9호 서식] 인증심사 보완조치 내역확인서
[별지 제10호 서식] 개인정보 보호 인증서
[별지 제11호 서식] 이의신청서
[별지 제12호 서식] 인증서 재발급 신청서

[별지 제1호 서식] 개인정보 보호 인증신청서

개인정보 보호 인증신청서

신청인	기관명		기관장(성명)	
	전화번호		담당자	
	주소(소재지)			
인증신청의 구분		☐ 최초심사 ☐ 갱신심사 ☐ 변경심사 ☐ 유지관리심사		
기관신청	유형	☐ 공공기관 ☐ 대기업 ☐ 중소기업 ☐ 소상공인		
	영역	☐ 전체(기관/기업) ☐ 일부(독립된 특정서비스·업무)		
개인정보 보호 인증범위 내용				
개인정보취급자 수				
개인정보파일 수				
개인정보처리시스템 수				
정보주체 수				
위탁기관 수				
기타사항				

「개인정보 보호 인증제 운영에 관한 규정」 제8조에 따라 위와 같이 개인정보 보호 인증을 신청합니다.

년 월 일

신청인 (서명 또는 인)

한국정보화진흥원장 귀하

1. 개인정보 보호의 신청 내역서 1부. (추가 제출)

[별지 제2호 서식] 개인정보 보호 인증신청 내역서

<table>
<tr><th colspan="4">개인정보 보호 인증신청 내역서</th></tr>
<tr><td>접수번호</td><td colspan="3">20XX - XXX * 인증기관이 작성</td></tr>
<tr><td>신청기관명</td><td></td><td>설립일</td><td></td></tr>
<tr><td>주요사업 및
업무내용</td><td colspan="3"></td></tr>
<tr><td rowspan="2">개인정보 보호
담당 조직 및
예산</td><td>부서명</td><td>담당인원</td><td>관련 예산</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>인증대상 서비스
및
업무 내용</td><td colspan="3">□ 개인정보 보호 인증 범위
○ 인증범위 : “00 기관 대민 서비스 ”
- 인증범위에 대한 설명

□ 개인정보 보호체계 구축 및 운영기간
- 년 월 ~ 년 월 (개월)

□ 주요 개인정보처리시스템 현황
- 주요 개인정보처리시스템별 용도, 특성, 개인정보 보유 수 등을 간략히 기록</td></tr>
<tr><td>별도 제출 문서</td><td colspan="3">1. 개인정보 보호 인증범위서
2. 개인정보 보호 운영현황 보고서</td></tr>
</table>

[별지 제3호 서식] 개인정보 보호 인증신청 접수증

<table>
<tr><th colspan="5">개인정보 보호 인증신청 접수증</th></tr>
<tr><td colspan="2">접수번호</td><td colspan="3">20XX - XXX</td></tr>
<tr><td rowspan="3">신청
기관</td><td>신청기관명</td><td></td><td>대표자명</td><td></td></tr>
<tr><td>담당자명</td><td></td><td>전화번호
(담당자)</td><td></td></tr>
<tr><td>주소</td><td colspan="3"></td></tr>
<tr><td colspan="2">인증신청 구분</td><td colspan="3">☐ 최초심사 ☐ 유지관리심사 ☐ 변경심사 ☐ 갱신심사</td></tr>
<tr><td colspan="2">인증신청 유형</td><td colspan="3">☐ 공공기관 ☐ 대기업 ☐ 중소기업 ☐ 소상공인</td></tr>
<tr><td colspan="2">인증신청 대상범위</td><td colspan="3"></td></tr>
<tr><td colspan="5">「개인정보 보호 인증제 운영에 관한 규정」 제8조에 따라 개인정보 보호 인증신청을 접수하였음을 확인합니다.

년 월 일

개인정보 보호 인증기관
한국정보화진흥원장 (인)</td></tr>
</table>

[별지 제4호 서식] 개인정보 보호 인증심사 계약서

<table>
<tr><td colspan="3" rowspan="2">개인정보 보호 인증심사 계약서</td><td>계 약 번 호</td></tr>
<tr><td>제 - 호
관 리 번 호
20XX - X - XXXXX</td></tr>
<tr><td rowspan="2">계약자</td><td>인증기관</td><td colspan="2"></td></tr>
<tr><td>신청기관</td><td colspan="2"></td></tr>
<tr><td rowspan="5">계약내용</td><td>인증심사 구분</td><td colspan="2">☐ 최초심사 ☐ 유지관리심사 ☐ 변경심사 ☐ 갱신심사</td></tr>
<tr><td>인증심사 유형</td><td colspan="2">☐ 공공기관 ☐ 대기업 ☐ 중소기업 ☐ 소상공인</td></tr>
<tr><td>인증심사
대상범위</td><td colspan="2"></td></tr>
<tr><td>인증심사수수료</td><td colspan="2">금_____원 (₩_____)</td></tr>
<tr><td>계약기간 및
인증심사
실시기간</td><td colspan="2">계약기간 : 20 년 월 일 ~ 20 년 월 일
(인증심사 실시기간 : 20 . . ~ 20 . .)</td></tr>
</table>

인증기관과 신청기관은 상호 대등한 입장에서 붙임의 계약문서에 의하여 인증심사에 대한 계약을 체결하고 신의에 따라 성실히 계약상의 의무를 이행할 것을 확약합니다.

붙임 : 1. 인증심사 계약조건 1부
2. 인증범위서 1부
3. 인증심사항목 목록 1부
4. 인증심사수수료 산출내역서 1부. 끝.

20 . . .

인증기관 : 한국정보화진흥원장 (인)
서울특별시 중구 청계천로 14(무교동 77번지)

신청기관 : (인)
○○○○○ ○○○ ○○○ ○○○

[별지 제5호 서식] 개인정보 보호 인증심사 실시계획서

개인정보 보호 인증심사 실시계획서	
관리번호	*20XX - X - XXXXX*
신청기관명	
인증심사 구분	□ 최초심사 □ 유지관리심사 □ 변경심사 □ 갱신심사
인증심사 유형	□ 공공기관 □ 대기업 □ 중소기업 □ 소상공인
인증심사 대상범위	
인증심사 실시기간	20 년 월 일 ~ 20 년 월 일
착수회의일(예정)	
종료회의일(예정)	
인증심사팀 구성	심사팀장 : 심사원 : 심사원 : 심사원 :
요청·통보사항	

위와 같이 귀 기관에 대한 개인정보 보호 인증심사 실시계획을 통보합니다.

20 년 월 일

개인정보 보호 인증기관

한국정보화진흥원장 (인)

[별지 제6호 서식] 인증심사 부적합 보고서

<table>
<tr><td colspan="4">인증심사 부적합 보고서</td></tr>
<tr><td>관리번호</td><td colspan="3">20XX - X - XXXXX</td></tr>
<tr><td>작성일자</td><td colspan="2"></td><td>심사원 (인)</td></tr>
<tr><td rowspan="4">인증심사
신청내역</td><td>신청기관명</td><td colspan="2"></td></tr>
<tr><td>심사구분</td><td colspan="2">□최초심사 □유지관리심사 □변경심사 □갱신심사</td></tr>
<tr><td>심사유형</td><td colspan="2">□공공기관 □대기업 □중소기업 □소상공인</td></tr>
<tr><td>심사대상범위</td><td colspan="2"></td></tr>
<tr><td>해당
심사항목</td><td colspan="3"></td></tr>
<tr><td>부적합
내용</td><td colspan="3">① 위반 내용 요약

② 준수 사항(PIPL, 내부 정책, 법률)

③ 운영 내용

④ 위반 내용

⑤ 수정·보완 권고 사항</td></tr>
<tr><td>근거자료</td><td colspan="3">- 문서명 (작성일자)
- 관련 법률 (조, 항)</td></tr>
</table>

[별지 제7호 서식] 인증심사 보완요청서

인증심사 보완요청서

관리번호	*20XX - X - XXXXX*
신청기관명	
보완요청 사항	□ 심사항목 총 _____ 건 □ 보완요청사항 o 부적합 심사항목 _____ 건 (부적합 세부 점검항목 _____ 건) ※ 보완 요청사항 세부내용은 붙임자료 첨부
보완조치내역서 제출기한	20 년 월 일까지

위와 같이 개인정보 보호 인증심사 실시결과 인증심사기준 부적합 사항에 대하여 보완을 요청하오니 기한내에 보완조치 결과 및 증빙자료를 제출하여 주시기 바랍니다.

20 년 월 일

개인정보 보호 인증기관
한국정보화진흥원장 (인)

붙임 1. 보완 요청사항 세부내용

1. 이 심사는 샘플링 심사기법에 의하여 수행된 것으로 발견되지 않은 부적합 사항이 존재할 수 있습니다.
2. 이 보고서의 내용은 비밀로 취급되며 신청기관의 사전 동의 없이는 공개되지 않습니다. 다만 법원의 요구가 있거나 법령에 의한 경우 예외로 합니다.

[별지 제8호 서식] 인증심사 보완조치 내역서

<table>
<tr><td colspan="5">인증심사 보완조치 내역서</td></tr>
<tr><td>관리번호</td><td colspan="4">20XX - X - XXXXX * 인증기관이 작성</td></tr>
<tr><td rowspan="2">신청기관</td><td>신청기관명</td><td></td><td>대표자명</td><td></td></tr>
<tr><td>담당자명</td><td></td><td>전화번호
(담당자)</td><td></td></tr>
<tr><td>보완조치
결과 내용</td><td colspan="4">☐ 부적합 심사항목 _____ 건

(부적합 세부 점검항목 _____ 건)을 보완조치 완료함

※ 보완 조치결과 세부내용 및 증빙자료는 붙임자료 첨부</td></tr>
<tr><td colspan="5">위와 같이 개인정보 보호 보완조치 결과를 제출합니다.

20 년 월 일

신청기관명 (인)</td></tr>
<tr><td colspan="5">붙임 1. 보완 요청 조치결과 세부내용 및 증빙자료</td></tr>
</table>

[별지 제9호 서식] 인증심사 보완조치 내역확인서

<table>
<tr><th colspan="4">인증심사 보완조치 내역확인서</th></tr>
<tr><td>관리번호</td><td>20XX - X - XXXXX</td><td>작성일자</td><td></td></tr>
<tr><td>부적합
심사항목
및 내용</td><td colspan="3"></td></tr>
<tr><td>보완조치
내역
확인결과</td><td colspan="3">※ 보완조치의 적합·부적합 내역을 분류하여 기재하고 필요시
증적자료(시행화면, 문서 사진 등)를 별지에 첨부</td></tr>
<tr><td rowspan="3">신청기관
담당자</td><td>소속부서</td><td colspan="2"></td></tr>
<tr><td>직책</td><td colspan="2"></td></tr>
<tr><td>담당자명</td><td colspan="2">성명 (인)</td></tr>
<tr><td colspan="2">인증심사팀장</td><td colspan="2">성명 (인)</td></tr>
</table>

[별지 제10호 서식] 개인정보 보호 인증서

인증번호 :

개인정보 보호(PIPL) 인증서

기 관 명 :

대 표 자 :

소 재 지 :

인증유형 :

인증범위 :

유효기간 :

귀 기관(기업)의 개인정보 보호수준이 「개인정보 보호 인증제 운영에 관한 규정」에 따른 인증심사기준에 부합함을 인증합니다.

년 월 일

한국정보화진흥원장 (인)

[별지 제11호 서식] 이의신청서

이의신청서

관리번호		*20XX - X - XXXXX * 인증기관이 작성*		
신청인	신청기관명		대표자명	
	담당자명		전화번호(담당자)	
	주 소			
이의신청 내용		※ 세부내용은 별지 사용 가능		

위와 같이 인증심사 결과 또는 인증취소 처분에 대하여 이의를 신청합니다.

20 년 월 일

신청인(대표자명) (서명 또는 인)

[별지 제12호 서식] 인증서 재발급 신청서

<table>
<tr><td colspan="4">인증서 재발급 신청서</td></tr>
<tr><td colspan="2">인증번호</td><td>－</td><td>관리번호</td><td>* 인증기관이 작성</td></tr>
<tr><td rowspan="3">신청
기관</td><td>신청기관명</td><td></td><td>사업자등록번호</td><td></td></tr>
<tr><td>대표자명</td><td></td><td>담당자명
(연락처)</td><td>(　　)　　－</td></tr>
<tr><td>주　소</td><td colspan="3"></td></tr>
<tr><td rowspan="3">재발급
사유
및
내용</td><td>사유</td><td colspan="3"></td></tr>
<tr><td>변경전</td><td colspan="3"></td></tr>
<tr><td>변경후</td><td colspan="3"></td></tr>
<tr><td colspan="4">위와 같이 개인정보 보호 인증서 재발급을 신청합니다.

20　년　　월　　일

신청기관명 (인)</td></tr>
</table>

[부록 2] 인증심사 신청서 첨부서류

[붙임 1] 개인정보 보호 인증범위서
[붙임 2] 개인정보 보호 운영현황 보고서

[붙임 1] 개인정보 보호 인증범위서

□ 개인정보 보호 인증범위서

<table>
<tr><td colspan="2">인증범위</td><td colspan="3">000 기관 000 대국민 서비스 등</td><td>유 형</td><td>공공기관</td></tr>
<tr><td colspan="2">개인정보 보호책임자</td><td colspan="5">소속 및 직책, 성명</td></tr>
<tr><td rowspan="3">주요 사업장 위치</td><td>본 사</td><td colspan="5"></td></tr>
<tr><td>지 사</td><td colspan="5"></td></tr>
<tr><td>데이터센터</td><td colspan="5"></td></tr>
<tr><td colspan="2">인증범위 설명</td><td colspan="5"></td></tr>
<tr><td colspan="2" rowspan="2">정보주체 수</td><td rowspan="2">명</td><td>온라인 회원</td><td colspan="3">명</td></tr>
<tr><td>오프라인 회원</td><td colspan="3">명</td></tr>
<tr><td colspan="2">개인정보 파일 수</td><td colspan="5"></td></tr>
<tr><td colspan="2">개인정보처리시스템 수</td><td colspan="5"></td></tr>
<tr><td colspan="2" rowspan="2">개인정보취급자 수</td><td rowspan="2">명</td><td colspan="2">개인정보처리자 취급자 수</td><td colspan="2">명</td></tr>
<tr><td colspan="2">위탁업체 취급자 수</td><td colspan="2">명</td></tr>
<tr><td colspan="2" rowspan="5">주요 위탁기관 현황</td><td colspan="2">위탁기관 명</td><td colspan="2">개인정보처리 업무</td><td>개인정보 취급자 수</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">(개인)정보보호 인증취득 현황</td><td colspan="5">ISO 27001, ISMS, PIMS 등 (개인)정보보호 인증서를 취득하고 있는 경우 표기</td></tr>
</table>

1. 조직구성 현황

전체 조직도

※ 개인정보 보호 인증제 인증범위에 해당하는 조직 별도 표시

개인정보 보호 조직도

2. 개인정보 자산 현황

2.1 개인정보처리시스템 네트워크 구성도

대외 서비스 네트워크 구성도

※ 대외 서비스를 위해 구성된 네트워크 구성도 표시 (예 : 데이터센터 네트워크 등)
– 개인정보처리시스템을 기준으로 서버, 네트워크, 보안시스템 표기
– 타기관 연계서비스가 있는 경우 표기

내부 네트워크 구성도

※ 개인정보취급자가 위치하는 내부 네트워크 구성도 (예 : 사내 네트워크 구성도 등)

2.2 개인정보처리 관련 주요 자산목록

구 분	자산명	수량	용도	자산위치
서버				
네트워크				
정보보호시스템				
응용프로그램				
데이터베이스				
PC				
문서				
CCTV				

※ 개인정보 보호인증 범위에 해당하는 정보시스템, 문서 자산을 기록
– 신청기관의 정보시스템 분류 기준에 따라 변경할 수 있음

3. 개인정보 보호체계 운영현황

3.1 개인정보 보호 관리체계

심사영역	심사목적	심사항목	선택 여부	미선택 시 사유
1. 보호 관리체계의 수립	1.1 관리계획	1.1.1 관리계획 수립		
		1.1.2 범위 설정		
	1.2 조직	1.2.1 조직과 책임		
	1.3 경영진의 책임	1.3.1 경영진의 참여		
		1.3.2 자원의 확보		
2. 실행 및 운영	2.1 문서화	2.1.1 문서화		
	2.2 개인정보 식별	2.2.1 개인정보 식별		
	2.3 위험관리	2.3.1 위험관리계획		
		2.3.2 위험평가 수행		
		2.3.3 위험평가 이행계획		
		2.3.4 이행계획에 따른 보호대책 구현		
3. 검토 및 모니터링	3.1 개인정보 보호 관리체계의 검토 및 모니터링	3.1.1 보호 관리체계 검토		
		3.1.2 내부 모니터링		
4. 교정 및 개선	4.1 교정 및 개선활동 실적관리	4.1.1 개인정보 보호 개선 활동		
	4.2 내부 공유 및 인식제고	4.2.1 내부 공유 및 인식제고		

3.2 개인정보 보호 대책구현

심사영역	심사목적	심사항목	선택 여부	미선택 시 사유
5. 개인정보 처리제한	5.1 개인정보 수집 시 보호조치	5.1.1 개인정보 수집제한		
		5.1.2 정보주체의 동의		
		5.1.3 법정대리인 동의 및 고지		
		5.1.4 민감정보 및 고유식별정보의 수집제한		
		5.1.5 간접수집 보호조치		
		5.1.6 대체가입수단의 제공		
		5.1.7 개인정보처리방침의 수립 및 공개		

심사영역	심사목적	심사항목	선택 여부	미선택 시 사유
	5.2 개인정보 이용 및 제공 시 보호조치	5.2.1 개인정보 제3자 제공		
		5.2.2 개인정보의 목적 외 이용 및 제공		
		5.2.3 개인정보의 이전		
	5.3 개인정보의 보유 시 보호조치	5.3.1 개인정보 품질 보장		
		5.3.2 개인정보 파일관리		
	5.4 개인정보 파기 시 보호조치	5.4.1 개인정보 파기절차		
		5.4.2 개인정보 파기		
6. 정보주체 권리보장	6.1 권리보장	6.1.1 개인정보의 열람·정정·삭제		
		6.1.2 개인정보의 처리정지		
		6.1.3 권리행사의 방법 및 절차		
7. 관리적 안전성 확보조치	7.1 개인정보 보호책임자의 지정	7.1.1 개인정보 보호책임자의 지정		
	7.2 교육 및 훈련	7.2.1 교육 및 훈련 시행		
		7.2.2 교육 및 훈련 평가		
	7.3 개인정보취급자 관리	7.3.1 개인정보취급자 감독		
		7.3.2 보안서약서		
	7.4 위탁업무 관리	7.4.1 외부위탁계약		
		7.4.2 정보주체 고지		
		7.4.3 위탁자 관리·감독		
	7.5 개인정보 유출사고 대응	7.5.1 개인정보 유출사고 대응계획 수립 및 운영		
		7.5.2 개인정보 유출사고 대응		
8. 기술적 안전성 확보조치	8.1 접근권한 관리	8.1.1 개인정보취급자 등록		
		8.1.2 개인정보취급자 권한관리		
		8.1.3 접근권한 검토		
	8.2 접속기록 관리	8.2.1 개인정보처리시스템 접속기록 관리		
		8.2.2 접속기록 검토		

심사영역	심사목적	심사항목	선택 여부	미선택 시 사유
	8.3 운영보안	8.3.1 비밀번호 관리		
		8.3.2 악성소프트웨어 통제		
		8.3.3 개인정보처리시스템에 대한 보호조치 활동		
		8.3.4 개인정보 표시제한		
		8.3.5 접근통제시스템 설치 및 운용		
		8.3.6 네트워크 접근통제		
		8.3.7 네트워크 운영관리		
	8.4 암호화 통제	8.4.1 암호화 계획 수립		
		8.4.2 암호화 적용		
	8.5 개발보안	8.5.1 개인정보 영향평가		
		8.5.2 개발 시 보안조치		
9. 물리적 안전성 확보조치	9.1 영상정보처리기기 관리	9.1.1 영상정보처리기기의 설치·운영 제한		
		9.1.2 영상정보처리기기의 설치·운영 사무의 위탁 관리		
	9.2 물리적 보안관리	9.2.1 출입통제 및 사무실 보안		
		9.2.2 이동컴퓨팅 보안관리		
		9.2.3 개인정보처리시스템 저장매체 폐기		
		9.2.4 휴대용 저장매체 관리		
		9.2.5 저장매체의 보관		

[붙임 2] 개인정보 보호 운영현황 보고서

□ 개인정보 보호 운영현황 보고서

□ 개인정보 보호 운영현황 보고서는 개인정보 보호 인증(PIPL)에서 요구하는 개인정보 보호 관리체계 구축 및 보호대책 이행에 대해 신청기관의 실제 운영현황을 파악하기 위하여 작성합니다.
- 개인정보 보호인증 인증심사 시 근거자료로 활용되므로 성실히 작성하여야 합니다.

□ 작성방법

1. 운영여부
- 인증기준 세부내용에 대해 신청기관의 운영여부를 Y(Yes), N(No)로 구분하여 표시합니다.
- Y(Yes) : 해당 인증기준에서 요구하는 사항에 대해 신청기관이 보호대책을 운영 및 이행하고 있는 경우
- N(No) : 해당 인증기준에서 요구하는 사항이 신청기관에 해당되지 않는 경우
  ※ 신청기관의 유형 및 현황에 따라 결정 (예 : 8.5.1 개인정보 영향평가 : 공공기관을 제외한 대기업, 중소기업, 소상공인은 "N")

2. 운영현황
- 인증기준 세부내용에 대해 신청기관이 실제 운영 및 이행하는 현황에 대해 상세하게 작성

3. 관련문서
- 인증기준 세부내용에 대해 신청기관의 개인정보 보호정책서(관리계획, 지침, 절차 등) 및 운영관련 이행증적 문서(예:계정신청서 등)
  ※ 신청기관 내부 개인정보 보호정책서의 경우 세부 조, 항까지 작성

4. 관련시스템
- 인증기준 세부내용에 대해 신청기관에서 실제 적용되거나 관련된 정보시스템명 작성

5. 관련 담당자
- 해당 인증기준 세부내용에 대한 신청기관이 운영 및 이행 담당자
  ※ 인증심사 시 인증심사원의 인터뷰 요청 시 실제 인터뷰 대상자를 작성

1. 개인정보 보호 관리체계 영역

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
1. 보호 관리 체계 의 수립	1.1 관리계획	1.1.1 관리계획 수립	개인정보 보호 관리계획 수립을 통해 명확한 방침 및 방향 제시를 보증하여야 하며, 이에 대해 개인정보 보호책임자의 검토와 승인을 거쳐야 한다.	개인정보 보호 관리체계를 고려한 개인정보 보호 관리계획을 수립하고 있는가?					
		1.1.2 범위 설정	개인정보처리자의 서비스에 중대한 영향을 미치는 요소를 고려하여 개인정보 보호 관리체계의 범위를 설정하여야 한다.	개인정보 처리조직 및 업무를 고려하여 개인정보 보호 관리체계의 범위를 명확하게 정의하고 있는가? 만일 정의된 범위 내에서 예외사항이 있을 경우 그 이유를 명확히 설명하고 있는가?					
	1.2 조직	1.2.1 조직과 책임	개인정보 보호 활동을 수행하고 관리하는 구성원들에 대한 책임, 역할 및 권한을 정의하여야 한다.	개인정보 보호 조직과 관련한 구성원의 책임, 역할 및 권한을 명확히 정의하고 있는가?					
	1.3 경영진의 책임	1.3.1 경영진의 참여	개인정보 보호책임자는 개인정보 보호 관리체계 수립 및 운영 등 조직이 수행하는 개인정보 보호 활동 전반에 경영진의 참여가 이루어질 수 있도록 보고, 검토 및 승인 절차를 수립하여야 한다.	개인정보 보호활동을 원활히 수행하기 위해 개인정보 보호책임자를 포함한 경영진이 개인정보 보호활동에 관한 의사결정에 적극적으로 참여할 수 있는 보고, 검토 및 승인 절차를 수립하고 있는가?					
		1.3.2 자원의 확	개인정보 보호를 위해	개인정보 보호 관리체계를					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
		보	필요한 자원(예산, 인력)을 반영하고, 검토하여야 한다.	효율적으로 운영·관리하기 위한 개인정보 보호 투자 계획(예산) 및 인적자원 확보계획을 기관의 규모 및 실현 가능성 등을 고려하여 수립하고 있는가?					
2. 실행 및 운영	2.1 문서화	2.1.1 문서화	효율적인 보호 관리체계 수립 및 운영을 위해 문서화 과정이 필요하고, 이러한 문서들과 기록을 관리하여야 한다.	개인정보 보호 관리체계의 운영을 확인할 수 있는 문서 또는 전산자료를 기록하고 있는가?					
				개인정보 보호 관리체계 요구사항에 맞도록 관련 문서에 대한 이력 및 변경사항 등을 기록하여 관리하고 있는가?					
	2.2 개인정보 식별	2.2.1 개인정보 식별	개인정보처리자가 처리하는 서비스와 관련한 개인정보처리시스템/개인정보DB/개인정보파일 등 각각에 따른 개인정보 자산현황(자산명, 용도, 도입일자, 관리자 등)을 작성하여 관리하여야 한다.	조직의 업무 수행과 관련된 개인정보 자산을 식별하여 목록을 관리하고 있는가?					
				개인정보 자산 항목별 형태, 소유자, 관리자, 사용자 특성 등을 포함한 목록을 지속적으로 관리·통제하고 있으며 책임소재가 명확한가?					
				식별된 개인정보 및 관련 자산을 조직과 업무에 미치는 보안 특성과 영향, 법적 준수사항 등을 고려하여 중요도를 결정하였는가?					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
	2.3 위험관리	2.3.1 위험관리계획	개인정보처리자는 개인정보를 취급하는 업무(서비스)에 대하여 적합한 위험관리 계획을 수립하고, 위험관리 계획에 따라 보호대책을 수립하여야 한다.	위험관리절차(방법론)가 존재하며 관리적·기술적·법적 요구사항을 포함하는 위험관리계획을 수립하는가?					
		2.3.2 위험평가 수행	식별된 개인정보 자산에 영향을 줄 수 있는 모든 위협과 취약성, 위험을 개인정보의 흐름에 따라 식별하고 분류하여야 하며, 이 개인정보 자산의 가치와 위험을 고려하여 잠재적 손실에 대한 영향을 식별·분석하여야 한다.	개인정보의 흐름에 따라 개인정보 흐름도(흐름표)를 작성하여 위험을 식별하고 있는가?					
				수립된 위험관리계획에 따라 위험평가를 수행하고 보고하였는가?					
				개인정보 유출·침해사고 방지가 가능한 합리적인 목표 위험수준을 설정 하였는가?					
				개인정보 흐름도는 주기적 또는 필요 시 재검토되어 최신성을 유지하는가?					
		2.3.3 위험평가 이행계획	위험평가 이행계획에 따라 보호대책을 구현하고, 보호대책의 효과성에 대하여 주기적인 검토를 하여야 한다.	위험평가 이행계획 수립 시 보호대책의 효과성을 검토하였는가?					
				위험평가 이행계획을 적절하게 수립하여 승인받고 있는가?					
		2.3.4 이행계획에 따른 보호대책 구현	개인정보 보호 우선순위, 일정계획, 예산, 책임, 운영계획 등을 포함한 위	위험평가 이행계획에 따라 보호대책을 적절히 구현하였는가?					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
			험평가 이행계획에 의해 적절히 구현되어야 한다.						
3. 검토 및 모니터링	3.1 개인정보 보호체계의 검토 및 모니터링	3.1.1 보호 관리체계 검토	개인정보 보호 관련 법령에서 요구하는 사항을 내부규정 및 관리계획에 포함하여야 하며, 이를 주기적으로 검토하여야 한다.	개인정보 보호 관리체계의 주기적인 검토를 위한 절차가 존재하는가?					
				법, 규제, 계약상의 요구사항들이 내부규정 및 관리계획에 반영되었는지 주기적으로 검토하였는가?					
		3.1.2 내부 모니터링	개인정보처리자의 개인정보 보호 관리체계가 계획된 절차에 따라 효과적으로 실행되는지를 점검하기 위하여 감사의 기준, 범위, 주기 및 방법을 규정하고, 계획된 주기로 내부감사를 수행하여야 한다.	개인정보 보호 관리체계 감사 계획(기준, 범위, 주기, 방법 등)을 수립하고 있는가?					
				개인정보 보호 감사는 계획에 따라 주기적으로 수행되고 감사결과에 따른 개선활동이 이루어지고 있는가?					
4. 교정 및 개선	4.1 교정 및 개선활동 실적관리	4.1.1 개인정보 보호 개선 활동	개인정보 보호활동을 지속적으로 점검·개선하고, 그 실적이 주기적으로 관리되어야 한다.	조직 내외부에 개인정보 수집, 이용, 제공시 필요 이상의 정보를 처리한 실적 등을 주기적으로 점검하고 개선하고 있는가?					
				개인정보 보호를 위한 관리적·기술적·물리적인 보호조치를 강구하고 이에 대해 주기적으로 점검하고 개선하고 있는가?					
	4.2 내부 공유 및 인식제고	4.2.1 내부 공유 및 인식제고	개인정보 보호 관리계획	개인정보 보호 관리계획은					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
			은 조직 내 모든 임직원 및 관련자에게 배포되고, 모든 임직원 및 개인정보취급자 등은 해당 내용을 이해하여야 한다.	조직 내 모든 임직원 및 관련자에게 배포되고, 모든 임직원 및 개인정보취급자 등은 해당 내용을 이해하고 있는가?					

2. 개인정보 보호 대책구현 영역

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
개인정보 처리	5.1 개인정보 수집 시 보호조치	5.1.1 개인정보 수집제한	개인정보처리자는 서비스 제공을 위해 필요한 최소한의 정보만을 수집하고, 목적 내에서만 개인정보를 수집하여야 한다.	개인정보 수집 목적 및 수집항목을 명확히 하여 수집하고, 정보주체 및 법정대리인으로부터 법령에 근거한 범위 내에서 수집하고 있는가?					
				서비스 제공을 위해 필요한 최소한의 정보만을 수집하는가?					
		5.1.2 정보주체의 동의	개인정보는 법령에 특별한 규정이 있는 경우를 제외하고는 정보주체의 동의를 얻은 후에 수집하여야 한다.	개인정보 수집 시 주요 고지내용을 정보주체에게 알리고 동의를 받는가?					
				개인정보 수집 동의를 득할 때 이용자에게 고지한 사항 중 변경이 발생한 경우 정보주체에게 고지내용을 알리고 동의를 얻는가?					
				개인정보 수집에 대해 동의 받는 방법은 적절한가?					
				정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 수집하는가?					
				법정대리인 또는 정보주체의 동의를 받을 때에는 각					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
				각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받는가?					
				정보주체의 개인정보를 이용하여 재화나 서비스를 홍보하거나 판매를 권유하는 경우 정보주체가 이를 명확하게 인지할 수 있도록 알려 주었는가?					
		5.1.3 법정대리인 동의 및 고지	만14세 미만의 아동의 개인정보를 수집 할 경우 법정대리인에게 필요한 사항을 고지하고 동의를 받아야 한다.	만14세 미만 아동의 개인정보를 수집하는 경우 법정 대리인에게 필요한 사항을 고지하고 동의를 받고 있는가?					
		5.1.4 민감정보 및 고유식별정보의 수집제한	정보주체의 권리 이익이나 사생활을 뚜렷하게 침해할 우려가 있거나, 그 자체로 개인을 식별할 수 있는 고유식별정보는 수집하지 않아야 하며, 필요한 경우 정보주체로부터 별도의 동의를 받아야 한다.	사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 민감정보를 수집하는 경우 정보주체로부터 별도의 동의를 받거나 관련 법령에 근거하여 수집하고 있는가?					
				주민등록번호를 제외한 고유식별정보를 수집하는 경우 정보주체로부터 별도의 동의를 받거나 관련 법령에 근거하여서만 수집하고					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
				있는가?					
				개인정보처리자가 주민등록번호를 처리하는 경우 관련 법령에 따라 처리하고 있는가 ?					
		5.1.5 간접수집 보호조치	시스템에 의한 수집 또는 개인정보 처리를 통해 생성한 간접 수집 개인정보에 대하여 요구 시 정보주체에게 고지하여야 한다.	간접 수집하는 개인정보에 대해 정보주체의 요구가 있는 경우 즉시 정보주체에게 이를 고지하고 있는가?					
		5.1.6 대체가입수단의 제공	인터넷 홈페이지 회원가입 시 주민등록번호에 대한 대체가입 수단을 제공하여야 한다.	인터넷 홈페이지를 통해 회원으로 가입할 경우 주민등록번호를 대체하는 가입 수단을 제공 하는가?					
		5.1.7 개인정보처리방침의 수립 및 공개	개인정보처리자는 개인정보 처리방침을 수립하여 정보주체가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하여야 한다.	개인정보 처리방침을 수립하거나 변경하는 경우에 정보주체가 언제든지 쉽게 확인할 수 있도록 적절한 방법으로 공개하였는가?					
				개인정보의 처리방침이 법적 요구사항 및 운영에 필요한 사항을 포함하여 작성되었는가?					
				개인정보 처리방침을 변경하는 경우 그 변경사항 및 이력을 정보주체가 확인할 수 있도록 하는가?					
	5.2 개인정보	5.2.1 개인정보	개인정보를 제3자에게	개인정보를 제3자에게 제					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
	이용 및 제공 시 보호조치	제3자 제공	제공 시 정보주체로부터 동의를 받은 후에 개인정보에 대한 적절한 보호조치 및 3자 제공을 하여야 한다.	공 또는 공유할 경우 법령에 근거하거나 주요 고지사항을 정보주체에게 알리고 동의를 받고 있는가?					
				이미 고지한 제3자 제공 동의 사항 중 변경이 발생한 경우에도 정보주체에게 이를 알리고 동의를 받고 있는가?					
				개인정보를 제공받은 경우, 제공받은 목적 외의 용도로 이용하지 않는가?					
		5.2.2 개인정보의 목적 외 이용 및 제공	개인정보는 정보주체에게 고지하고 동의 받은 범위를 벗어나 이용하지 않아야 하고, 만약 동의 범위를 벗어나 이용할 경우 정보주체로부터 추가적으로 동의를 획득하고, 개인정보에 대한 적절한 보호조치를 취해야 한다.	개인정보를 목적 외의 용도로 이용하는 경우, 법령에 근거하거나 정보주체의 동의 획득 등 사실이 명확한가?					
				개인정보를 목적 외의 용도로 이용하는 경우, 주요 고지사항을 정보주체에게 알리고 별도 동의를 받는가?					
				개인정보를 목적 외의 용도로 제3자에게 제공하는 경우, 제공받는 자가 보호조치를 취하도록 하거나, 이용목적·방법 등을 제한하도록 요청하고 있는가?					
				공공기관이 개인정보를 목적 외의 용도로 이용하거					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
				나 이를 제3자에게 제공하는 경우, 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 관보 또는 인터넷 홈페이지 등에 게재하고 있는가?					
				공공기관이 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우, 대장관리(이력관리)를 하고 있는가?					
		5.2.3 개인정보의 이전	개인정보처리자가 양도·합병으로 인해 개인정보를 이전 하거나 받는 경우 또는 개인정보를 국외의 제3자에게 제공 또는 공유하는 경우 적절한 보호조치를 하여야 한다.	영업의 양도, 합병 등으로 개인정보를 이전받은 경우 양도자가 정보주체의 개인정보를 이용하거나 제공할 수 있는 당초의 목적 범위 안에서만 개인정보를 이용하거나 제공하는가?					
				영업의 양도, 합병 등으로 개인정보를 이전하려는(또는 이전 받는) 경우 미리 주요 사항을 해당 정보주체에게 알렸는가?					
				개인정보처리자가 개인정보를 국외의 제3자에게 제공 또는 공유하는 경우 주요 고지 사항을 정보주체에게 알리고, 동의를 요구하고 있는가?					
	5.3 개인정보	5.3.1 개인정보	개인정보처리자가 처리	개인정보처리자가 처리하					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
	보유 시 보호 조치	품질 보장	하고 있는 개인정보는 정확성, 완전성, 최신성을 유지하여야 한다.	고 있는 개인정보가 정확하고 최신의 상태로 유지되는가?					
		5.3.2 개인정보 파일관리	개인정보파일을 운용하는 공공기관은 그 현황을 안전행정부에 등록하여야 하고, 변경사항 발생 시 이를 고지하여야 한다.	공공기관의 장이 개인정보파일을 운용하는 경우, 안전행정부장관에게 등록 또는 변경사항을 고지하였는가?					
	5.4 개인정보 파기 시 보호 조치	5.4.1 개인정보 파기 절차	개인정보처리자는 개인정보의 파기에 관한 사항을 기록 관리하여야 하며, 파기 시행 후 파기결과를 확인하여야 한다.	개인정보를 파기하는 경우 파기에 관한 사항을 기록 관리하고 있으며, 개인정보 보호책임자가 파기결과를 확인하고 있는가?					
		5.4.2 개인정보 파기	개인정보처리자는 개인정보 파기에 관한 관리계획을 수립하고, 관리계획에 따라 개인정보의 수집 목적이 달성된 경우, 개인정보를 안전한 방법으로 지체 없이 파기하여야 한다.	개인정보의 보유기간 경과, 수집 및 이용목적이 달성된 경우 지체 없이 개인정보를 파기하는가?					
				개인정보의 파기 방법은 복구 불가능한 수준의 안전한 방법으로 파기하고 있는가?					
				개인정보의 수집목적이 달성된 경우에도 타 법령에 근거하여 개인정보를 전부 또는 일부 보유한다면 보유 근거법령 및 보유기간 등을 정보주체에게 명확히 공개하고 해당 개인정보를 별도로 분리·보관하도록 하					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
				고 있는가?					
정보주체 권리보장	6.1 권리보장	6.1.1 개인정보 열람·정정·삭제	개인정보의 열람·정정·삭제 개인정보처리자는 정보주체의 개인정보에 대한 열람·정정·삭제 방법 및 절차를 제공하고, 정정·삭제 요구 시 지체 없이 처리하고 기록을 남겨야 한다.	정보주체 또는 정보주체의 법정 대리인이 정보주체 자신의 개인정보에 대한 열람 또는 이용 및 제공내역을 요구할 수 있는 방법 또는 절차를 제공하는가?					
				개인정보처리자가 개인정보에 대한 열람 또는 이용 및 제공내역을 요구받을 경우 기간 내에 열람 가능하도록 처리하고, 열람할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리는가?					
				정보주체 또는 정보주체의 법정 대리인으로부터 정보주체의 개인정보 정정 또는 삭제에 대한 요구가 있는 경우 일정 기한 내에 필요한 조치를 취하고, 정보주체에게 알리는가?					
				정보주체에 의해 정정 또는 삭제 요구된 개인정보가 법령에서 정한 수집대상으로 명시되어 있어 삭제할 수 없는 경우 그 내용을 정보주체에게 알리는가?					
				개인정보를 정정·삭제하여					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
				야 하는 경우, 위탁사에게 제공한 개인정보도 함께 지체 없이 처리하는가?					
		6.1.2 개인정보의 처리정지	개인정보처리자는 정보주체의 개인정보에 대한 처리정지 방법 및 절차를 제공하고, 처리정지 요구 사항을 처리하고 기록을 남겨야 한다.	개인정보에 대한 처리정지의 요구, 처리정지의 거절, 통지 등의 방법 및 절차를 제공하는가?					
				정보주체로부터 개인정보 처리 정지요구를 받았을 때 이를 처리하는가?					
				정보주체에 의한 처리정지 요구를 거절하는 정당한 사유가 있을 때, 그 내용을 정보주체에게 알리는가?					
		6.1.3 권리행사의 방법 및 절차	정보주체가 열람등 요구에 대한 거절 등 조치에 이의를 제기할 수 있도록 필요한 절차를 마련하여야 한다.	정보주체가 열람등(열람 및 존재확인) 요구에 대한 거절 등 조치에 대하여 이의사항이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하는가?					
				정보주체의 열람, 정정·삭제, 처리정지 등의 요구를 받은 경우 적절한 방법으로 본인여부를 확인하는가?					
관리적 안전성 확보조치	7.1 개인정보 보호책임자의 지정	7.1.1 개인정보 보호 책임자의 지정	개인정보 보호책임자를 지정하고, 적절한 책임, 권한 및 역할을 정의하여야 한다.	개인정보 보호책임자의 자격 요건은 법령에 따른 자격요건을 충족하는 자를 정하고 이에 적합한 자를					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
				지정하고 있는가?					
				개인정보 보호책임자의 개인정보 보호에 관한 역할 및 책임이 정의되었는가?					
				개인정보 보호책임자는 개인정보 보호 역량을 강화하기 위해 노력하고 있는가?					
				개인정보 보호책임자는 개인정보 보호와 관련한 법령의 위반사실을 알게 된 경우 개선조치 하였는가?					
	7.2 교육 및 훈련	7.2.1 교육 및 훈련 시행	개인정보 보호 인식제고 및 실제 운영에 필요한 교육·훈련 계획을 수립하여 이행하여야 하고, 교육의 대상 및 내용이 적절하여야 한다.	교육내용은 개인정보 보호 관련 법률 및 제도, 사내 규정, 관리적·기술적 조치 사항 및 이를 수행하기 위한 방법 등 개인정보취급자가 필수적으로 알아야 하는 사항을 포함하는가?					
				개인정보 보호 교육 대상은 개인정보 보호책임자 및 개인정보취급자(수탁직원 포함)를 포함하는가?					
				개인정보 보호정책의 중대한 변경, 신규입사자, 조직 내·외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생할 경우 추가 교육을 수행하는가?					
		7.2.2 교육 및 훈	개인정보 보호 교육 및	개인정보 보호 교육 및 훈					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
		련 평가	훈련 시행에 대한 기록을 남기고 그 결과를 평가하여 다음 교육 및 훈련에 반영하여야 한다.	련이 계획에 따라 주기적으로 시행되고, 이에 대한 기록을 유지하는가?					
				개인정보 보호 교육 및 훈련의 효과를 측정, 분석한 결과를 차기 교육계획에 반영하고 있는가?					
	7.3 개인정보 취급자 관리	7.3.1 개인정보취급자 감독	개인정보취급자를 최소한으로 제한하고, 목록화하여 관리하여야 한다.	업무상 개인정보를 취급해야 하는 개인정보취급자는 최소한으로 제한하고 있는가?					
				개인정보취급자 명단 관리 등 관리방안을 마련하고 있는가?					
		7.3.2 보안서약서	조직에서 임직원들의 기밀정보 유출 위험을 최소화하고, 임직원에게 개인정보 보호에 대한 책임을 명확히 주지시키기 위해 보안서약서에 서명토록 해야 한다.	내부직원(정규직/계약직/임시직)의 개인정보 처리업무 시작 시 개인정보 보호에 관한 책임 및 의무를 고지한 개인정보 보호 서약서를 제출하도록 관리하고 있는가?					
				개인정보를 처리하는 외부직원(위탁직원 포함) 등에 대하여 위탁계약서에 책임과 의무를 명시하고 개인정보 보호 서약서를 제출하도록 관리하고 있는가?					
	7.4 위탁업무 관리	7.4.1 외부위탁계약	신청기관의 개인정보 처리업무를 외부 위탁하는 경우에는 개인정보 보호	개인정보 처리업무를 위탁하는 경우 문서화된 계약서 등에 의하여 이루어지					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
			에 관한 요구사항 및 관리감독에 관한 사항을 계약서 등에 문서화하여야 한다.	고 있는가?					
				위탁계약서에 위탁업무 목적 외 처리금지, 개인정보의 안전성 확보조치 등 법률에서 정한 사항들을 포함하고 있는가?					
		7.4.2 정보주체 고지	개인정보 처리업무 위탁 시 관련사항을 정보주체에게 알리고 필요한 경우 동의를 받아야 한다.	개인정보처리자(위탁자)는 정보주체가 언제든지 수탁자의 정보를 확인할 수 있도록 관보 또는 인터넷 홈페이지에 게재하는 등의 방법으로 공개하고 있는가?					
				개인정보처리자(위탁자)가 재화 또는 서비스를 홍보하는 등 그 업무범위에서 제3자에게 업무를 위탁하는 경우, 위탁업무의 내용과 수탁자의 정보 등을 정보주체에게 서면, 전자우편 등의 방법으로 알리고 있는가?					
		7.4.3 위탁자 관리·감독	외부위탁 업체가 계약서 등에 명시된 사항을 충분히 이행하는지 주기적으로 관리 감독하여야 한다.	개인정보처리자(위탁자)는 수탁자가 개인정보를 안전하게 처리하는지를 주기적으로 감독하는가?					
				개인정보처리자(위탁자)는 개인정보 처리목적을 미리 정하고, 수탁자가 처리목적을 벗어나서 정보주체의 개인정보를 처리하지 않도					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
				록 관리하는가?					
	7.5 개인정보 유출사고 대응	7.5.1 개인정보 유출사고 대응계획 수립 및 운영	개인정보의 유출사고에 대응하기 위한 긴급 연락체계, 개인정보 보호 사고 발생 시 보고 및 대응 절차, 사고 대응 조직의 구성 등을 포함한 개인정보 사고 대응 계획을 수립하고, 계획에 따라 대응체계를 운영하여야 한다.	개인정보 유출사고 대응계획이 수립되어 있고, 대응계획에 역할 및 책임이 명확히 기술되어 있는 등 필요한 내용이 충분히 반영되어 있는가?					
				개인정보 유출사고를 대응할 수 있는 체계를 구축하고 있으며, 모니터링 및 대응방법, 절차, 보고 및 승인 방법 등을 포함하고 있고 실제로 운영하고 있는가?					
		7.5.2 개인정보 유출사고 대응	피해를 최소화하기 위한 적절한 보호조치를 마련하고, 개인정보 유출사고 대응 및 통지, 신고 절차 및 방법에 따라 신속히 수행하여야 한다.	개인정보가 유출되었음을 알게 되었을 때, 지체 없이 해당 정보주체에게 유출사실을 알릴수 있는 체계를 마련하고 있는가?					
				개인정보가 유출되었음을 알게 되었을 때, 정보주체에 대한 유출사실의 통지 시기, 방법 및 절차 등을 적절하게 수립하고 있는가?					
				1만 명 이상 정보주체의 개인정보가 유출된 경우, 개인정보처리자는 관계기관에 신고하기 위한 절차가 있는가?					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
				개인정보가 유출된 경우, 그 피해를 최소화하기 위한 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등의 보호조치를 마련하고 있는가?					
기술적 안전성 확보조치	8.1 접근권한 관리	8.1.1 개인정보취급자 등록	개인정보 처리시스템과 서비스에 접근을 허용하거나 취소하기 위한 공식적인 사용자 등록 및 해지절차를 마련하여야 한다.	개인정보처리시스템과 서비스에 접근을 허용하거나 취소하기 위한 공식적인 사용자 등록 및 해지 절차가 있는가?					
		8.1.2 개인정보취급자 권한관리	개인정보 처리시스템에 대한 접근 권한이 서비스 제공을 위하여 필요한 최소한의 인원에게만 부여하여야 하고, 기록을 보관하여야 한다.	개인정보 처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무담당자에 따라 차등 부여하고 있는가?					
				개인정보취급자의 퇴직, 계약 종결 또는 직무 변경 시 접근권한을 제거 또는 변경하고 있는가?					
				권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하고 있는가?					
				하나의 계정으로 다수가 동일 시스템에 접속하거나 동시 접속할 수 없도록 조치하고 있는가?					
		8.1.3 접근권한 검토	개인정보취급자에게 부	개인정보취급자의 접근권					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
			여된 접근권한 현황에 대해 정기적으로 점검을 하여야 한다.	한을 주기적으로 검토하고 있는가?					
				특수 접근권한의 할당이나 사용을 제한하고 주기적으로 점검하고 있는가?					
				접근권한 검토 결과 적정성이 의심될 경우 그에 따른 조치가 이루어지고 있는가?					
	8.2 접속기록 관리	8.2.1 개인정보처리시스템 접속기록 관리	개인정보처리시스템의 접속기록은 보관되고, 보호조치에 의해 관리되어야 한다.	개인정보처리시스템의 접속기록이 위·변조되지 않도록 별도 저장장치에 백업 보관하고 있는가?					
				개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관·관리하고 있는가?					
		8.2.2 접속기록 검토	개인정보 열람기록 및 처리기록을 주기적으로 분석하고 검토하여야 한다.	개인정보취급자의 열람 기록 및 접속기록을 분석하고 주기적으로 검토하고 있는가?					
	8.3 운영보안	8.3.1 비밀번호 관리	개인정보처리시스템 접속 시 안전한 비밀번호를 사용하여야 한다.	개인정보취급자가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 관리 절차를 수립하고 있는가?					
				개인정보취급자가 비밀번호관리 절차를 이행하고 있는가?					
		8.3.2 악성소프트	바이러스 등의 악성 소	악성 소프트웨어를 차단하					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
		웨어 통제	프트웨어로부터 개인정보처리시스템을 보호하기 위해 악성 소프트웨어들을 예방하고 탐지, 대응하는 대책을 이행하여야 한다.	기 위한 관리방안을 수립하고 이행하고 있는가?					
				백신 소프트웨어 등 보안 프로그램은 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하도록 설정하고 있는가?					
				개인정보처리시스템, 개인정보취급자의 PC에 P2P, 웹 하드 등과 같은 비인가 프로그램 설치를 금지하고 있는가?					
		8.3.3 개인정보처리시스템에 대한 보호조치 활동	비인가 접근 시도 등의 모니터링 및 기술적 취약점 점검을 지속적으로 수행하여야 한다.	개인정보처리시스템으로의 비인가 접근 시도에 대해 모니터링을 수행하고 있는가?					
				개인정보처리시스템에 대해 기술적 취약점 점검을 주기적으로 수행하고 있는가?					
		8.3.4 개인정보 표시제한	개인정보 처리업무를 목적으로 개인정보 조회, 출력 등의 업무 수행 시, 개인정보 마스킹을 통해 개인정보 표시제한을 수행하여야 한다.	개인정보의 조회, 출력 시 마스킹 등 개인정보 표시를 제한하는 기준을 정하고 이를 시행하고 있는가?					
		8.3.5 접근통제시스템 설치 및 운용	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 침입차단	정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 기관의 상황에 맞					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
			및 탐지 기능을 포함한 시스템을 설치 운용하여야 한다.	는 접근통제(침입차단 및 탐지기능 등)시스템을 설치하여 운영하고 있는가?					
				정보통신망을 통한 불법적인 외부 접근 및 내·외부자에 의한 정보유출 등을 모니터링하기 위해 접근통제 시스템의 접근제한 정책 및 로그를 수집하고, 정기적으로 점검하고 있는가?					
		8.3.6 네트워크 접근통제	네트워크 접근통제를 강화하기 위해 기술적 보호조치를 마련하여야 한다.	네트워크 접근통제 정책을 수립하여 주기적으로 점검하고 있는가?					
				개인정보 자산 중요도에 따라 네트워크를 논리적 또는 물리적으로 분리하여 운영하고 있는가?					
				중요 개인정보취급자의 업무용 PC는 인터넷을 차단하는 등의 보호조치를 취하고 있는가?					
		8.3.7 네트워크 운영관리	내부 네트워크를 통한 개인정보처리시스템 관리 시 특정 단말에서만 접근을 할 수 있도록 제한하고, 인터넷 등 외부 네트워크를 통한 개인정보처리시스템의 접속 시 보호대책을 마련하여야 한다.	내부 네트워크를 통한 개인정보처리시스템 관리 시 특정 단말에서만 접근할 수 있도록 제한하고 있는가?					
				인터넷 등 외부 네트워크를 통한 개인정보처리시스템의 접속 시 VPN 또는 전용선 등의 안전한 접속					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
				수단을 사용하고 있는가?					
	8.4 암호화 통제	8.4.1 암호화 계획 수립	개인정보 보호를 위한 암호화 계획을 수립해야 하고 포함된 내용은 법적 요건을 충족하여야 한다.	고유식별정보, 바이오정보, 비밀번호 등 주요 개인정보 보호를 위한 암호화 계획을 수립하고 있는가?					
				암호화 계획에 포함된 암호화 대상 및 암호화 방법을 명확하게 정의하여 법적 요건을 만족하고 있는가?					
		8.4.2 암호화 적용	개인정보 저장 및 전송 시, 원격접속 시 암호화를 수행하여야 한다.	인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 고유식별정보, 바이오정보, 비밀번호를 저장하는 경우 암호화를 하고 있으며, 내부 망에 저장하는 경우 위험도분석 등을 통해 암호화 또는 암호화에 상응하는 조치를 하고 있는가?					
				업무용 컴퓨터에 고유식별정보를 저장하여 관리하는 경우 암호화하고 있는가?					
				개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우 고유식별정보, 바이오정보, 비밀번호를 암호화하고 있는가?					
				원격작업을 통해 내부시스					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
				템 접근 시, VPN 등을 통한 암호화 통신을 사용하고 있는가?					
				고유식별정보, 바이오정보, 비밀번호 등의 개인정보를 암호화 할 경우 안전한 알고리즘을 사용하고 있는가?					
	8.5 개발보안	8.5.1 개인정보 영향평가	개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 수행하여야 한다.	개인정보처리시스템 개발 및 변경 시 개인정보 영향평가의 필요성 여부를 사전에 검토하는 절차를 수립하고 있는가?					
				개인정보 영향평가 필요성 여부를 반영하여 영향평가를 수행하고 있는가?					
				공공기관의 장은 개인정보 영향평가서를 안전행정부 장관에게 제출하고 있는가?					
				개인정보 영향평가 결과에 따른 개선요구사항에 대한 이행여부를 관리하고 있는가?					
		8.5.2 개발 시 보안조치	개인정보처리시스템 개발 시 보안 요구사항에 따라 구현 및 시험 등에 적절한 보호조치를 마련하여야 한다.	개인정보처리시스템 개발 및 변경 시 보안 요구사항을 정의하고 있는가?					
				개인정보처리시스템 개발 및 변경 시 안전한 코딩방법에 따라 구현하고 있는					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
				가?					
				운영데이터를 테스트데이터로 사용하는 경우 개인정보를 익명화하고 있는가?					
				개발환경과 운영환경을 분리하여 운영하고 있는가?					
				외부용역을 통한 개인정보처리시스템 개발 시 보안규정에 따라 관리감독하고 있는가?					
				개인정보처리시스템 개발 및 변경에 대한보안 요구사항 이행여부를 점검하고 있는가?					
물리적 안전성 확보조치	9.1 영상정보처리기기 관리	9.1.1 영상정보처리기기의 설치·운영 제한	영상정보처리기기 설치·운영 시, 적절한 보호조치를 마련하여야 한다.	공공기관의 장은 영상정보처리기기를 설치하는 경우 관련 전문가 및 이해관계인의 의견을 수렴하고 있는가?					
				공개된 장소에 영상정보처리기기를 설치·운영할 때 적법한 이유로 설치하고 있는가?					
				영상정보처리기기 운영자는 영상정보관리책임자를 지정하고 있으며, 영상정보처리기기 운영·관리 방침을 마련하여 점검하고 있는가?					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
				설치 운영 중인 영상정보처리기기를 설치목적에 맞게 사용·관리하고 있는가?					
				영상정보처리기기를 설치·운영 할 경우 정보주체가 쉽게 인식할 수 있도록 안내판을 설치하고 있는가?					
		9.1.2 영상정보처리기기의 설치·운영 사무의 위탁 관리	영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 적절한 위탁절차를 마련하여야 한다.	영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 위탁하는 절차 및 요건에 맞게 계약서 및 관련서류를 점검하고 있는가?					
				영상정보처리기기의 설치 및 관리에 관한 사무를 위탁한 경우, 안내판에 수탁기관의 명칭 등을 포함하고 있는가?					
	9.2 물리적 보안관리	9.2.1 출입통제 및 사무실 보안	개인정보를 취급하는 공간에 대해 출입통제 등 물리적 보호조치를 취하고 접근 가능한 인원은 허가받은 인력에 한해 최소화하여야 한다.	전산실, 자료보관실 등 개인정보를 보관하고 있는 시설 및 장비를 보호하기 위한 출입통제 절차를 수립하고 있는가?					
				전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 장소의 출입통제는 허가받은 인력에 한하며, 관련 출입기록을 보관하고 있는가?					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
				개인정보를 포함하고 있는 중요 문서, 출력물, 저장매체가 책상 등에 노출되지 않도록 보호하고 있는가?					
		9.2.2 이동컴퓨팅 보안관리	이동컴퓨팅 기기 사용 시에 개인정보를 보호하기 위한 보호정책을 수립하고, 내부 네트워크로의 연결 및 공공장소에서의 사용에 대한 정책을 마련하여야 한다.	이동컴퓨팅 기기 사용 시 개인정보 보호를 위한 보호정책을 수립하고 있는가?					
				이동컴퓨팅 기기의 분실 시 개인정보의 유출 방지를 위한 암호화, 장비보호를 위한 물리적 보호조치 등 보호대책을 마련하고 있는가?					
				이동컴퓨팅 기기를 내부 네트워크 연결 및 공공장소에서 사용 시 개인정보 보호대책을 마련하고 있는가?					
		9.2.3 개인정보처리시스템 저장매체 폐기	개인정보처리시스템 폐기 또는 재사용 시 개인정보를 담고 있는 하드디스크, 스토리지, 테이프 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 개인정보는 복구 불가능하도록 완전히 삭제하여야 한다.	개인정보처리시스템의 저장매체에 대한 유출, 오용을 방지하기 위한 매체의 폐기 및 재사용에 대한 절차를 수립하였는가?					
				저장매체의 폐기 또는 재사용 시 개인정보는 복구 불가능하게 삭제하고 그 이력을 남기고 있는가?					
		9.2.4 휴대용 저장매체 관리	개인정보 유출을 예방하기 위해 외장하드, USB,	외장하드, USB, CD 등 휴대용 저장매체 취급, 보관,					

심사 영역	심사목적	심사항목	심사내용	세부내용	이행 여부	운영현황	관련문서	관련 시스템	담당자
			CD 등 휴대용 저장매체 취급, 보관, 폐기 및 재사용에 대한 절차를 수립하여야 한다. 또한 매체를 통한 악성코드 감염 방지대책을 마련하여야 한다.	폐기, 재사용에 관한 관리 절차를 수립하고 있는가?					
				휴대용 저장매체를 통한 악성코드 감염 및 개인정보의 유출 방지 대책을 수립하고 있는가?					
		9.2.5 저장매체의 보관	개인정보가 포함된 저장매체를 안전한 장소에 보관하여야 한다.	개인정보가 포함된 저장매체를 잠금장치가 있는 안전한 장소에 보관하고 있는가?					

[별표 1] 인증심사 수수료 산정기준

[별표 1] 인증심사 수수료 산정기준

1. 인증심사 수수료는 직접인건비, 제경비, 기술료, 직접경비로 구성된다.

인증심사 수수료 = 직접인건비 + 직접경비 + 기술료 + 제경비

2. 직접인건비 산정은 인증심사에 투입되는 인증심사원의 인건비로 산정한다.

직접인건비 = 심사원 등급 단가 × 투입공수

가. 인건비는 S/W사업 대가산정 가이드의 정보보안 컨설팅비를 준용한다.

인증심사원 등급	컨설턴트 등급
책임심사원	수석 컨설턴트
선임심사원	책임 컨설턴트
심사원	전임 컨설턴트

나. 투입공수 산정은 다음과 같다.

투입공수 = (개인정보처리시스템 수에 따른 투입공수 + 개인정보취급자 수에 따른 투입공수 + 위탁기관 수에 따른 투입공수 + 정보주체 수에 따른 투입공수) × (1 + 가중치)

① 개인정보처리시스템 수 = 인증범위 내 개인정보처리시스템 수

○ 개인정보처리시스템 수는 개인정보 DB서버를 포함하며 개인정보 DB와 연결하여 개인정보의 수집, 기록, 검색, 저장, 정정, 파기 등의 처리가 가능한 어플리케이션 서버, WAS서버 등을 포함하여 산정

※ 단순 단말PC 및 웹서버는 제외. 단, 웹서버가 WAS서버나 DB서버와 동일한 경우는 포함

<개인정보처리시스템 수에 따른 투입공수>

개인정보처리시스템 수	투입공수(단위 : MAN/DAY)
3대 미만	2
5대 미만	5
10대 미만	10
20대 미만	15
30대 미만	20
40대 미만	25
50대 미만	30
70대 미만	35
100대 미만	40
150대 미만	45
200대 미만	50
300대 미만	55
500대 미만	60
700대 미만	65
1,000대 미만	70
1,500대 미만	75
2,000대 미만	80
3,000대 미만	85
5,000대 미만	90
7,000대 미만	95
10,000대 미만	100
10,000대 이상	100일 + (협의조정)

② 개인정보취급자 수 = 인증범위 내 개인정보취급자 수

○ 개인정보취급자 수는 임직원, 파견근로자, 시간제근로자 등 신청기관의 지휘·감독을 받아 인증범위 내 개인정보를 처리하는 자뿐만 아니라 외부 위탁기관의 직원도 포함하여 산정

<개인정보취급자 수에 따른 투입공수>

개인정보취급자 수	투입공수(MAN/DAY)
5명 미만	1
10명 미만	2
20명 미만	4
30명 미만	6
50명 미만	8
70명 미만	10
100명 미만	12
150명 미만	14
200명 미만	16
300명 미만	18
500명 미만	20
700명 미만	22
1,000명 미만	24
1,500명 미만	26
2,000명 미만	28
3,000명 미만	30
5,000명 미만	32
7,000명 미만	34
10,000명 미만	36
15,000명 미만	38
20,000명 미만	40
20,000명 이상	40 + 협의조정

③ 위탁기관 수

○ 인증범위내의 개인정보를 위탁하여 처리하는 위탁기관 수

<위탁기관 수에 따른 투입공수>

위탁기관 수	투입공수(MAN/DAY)
1개 미만	0
3개 미만	2
5개 미만	4
10개 미만	6
20개 미만	8
30개 미만	10
40개 미만	12
50개 미만	14
70개 미만	16
100개 미만	18
150개 미만	20
150개 이상	20 + 협의조정

④ 정보주체 수(평균) = 인증범위 내 정보주체 수의 평균

○ 정보주체 수(평균) = 인증범위 개인정보처리시스템 내 정보주체 수의 합 ÷ 개인정보처리시스템 수

- 동일 업무 내에서 한 개인에 대해 여러 건의 처리내역을 보유한 경우에는 1명으로 산정

※ 구매자 1인에 대해 여러 건의 구매내역을 보유한 경우 정보주체 수는 1명으로 처리. 단, 구매내역에 있는 정보주체라도 다른 업무인 카드 결재내역에서 동일인일 경우는 별도로 추가하여 산정

< 정보주체 수에 따른 투입공수 >

정보주체 수(평균)	투입공수(MAN/DAY)
10,000명 미만	1
30,000명 미만	2
50,000명 미만	3
100,000명 미만	4
300,000명 미만	5
500,000명 미만	6
700,000명 미만	7
1,000,000명 미만	8
3,000,000명 미만	9
5,000,000명 미만	10
7,000,000명 미만	11
10,000,000명 미만	12
30,000,000명 미만	13
50,000,000명 미만	14
70,000,000명 미만	15
100,000,000명 미만	16
300,000,000명 미만	17
500,000,000명 미만	18
700,000,000명 미만	19
1,000,000,000명 미만	20
1,000,000,000명 이상	20 + 협의조정

⑤ 가중치

○ 가중치는 인증대상 범위내 고유식별정보 등 중요정보 보유여부와 인증 신청기관의 신청유형에 따라 다음과 같이 산정한다.

가중치 = 중요정보 보유 여부에 따른 가중치 + 신청유형에 따른 가중치

가) 중요정보 보유여부에 따른 가중치

○ 인증대상 범위내 민감정보, 고유식별정보 등 중요정보 보유 여부에 따라 가중치 적용

- 인증범위 내 민감정보, 고유식별정보 보유 여부에 따라 각 항목별 5%씩 가산

< 중요정보 보유 여부에 따른 가중치>

구분	가중치(%)
민감정보 보유	5
고유식별정보 보유	5

나) 신청유형에 따른 가중치

○ 소상공인, 중소기업, 대기업·공공기관 등 인증 신청기관의 신청유형에 따라 가중치 적용

< 신청유형(기업유형)에 따른 가중치>

구분	가중치(%)
소상공인(유형1)	0
중소기업(유형2)	5
공공기관·대기업(유형3)	10

3. 직접경비는 인증심사업무에 필요한 직접 경비를 산정할 수 있다.

○ 직접경비는「SW사업 대가산정 가이드」의 직접경비 범위를 준용하여 산정할 수 있다.

항목	설명
출장비	교통비, 숙박비, 식대 등으로 인증기관 출장규칙에 따름
장비사용료	당해 사업 수행시 사용되는 컴퓨터 기기나 장비 또는 S/W 사용료임차할 경우에는 임차료
특정기술자문비	특정기술과 관련된 전문가 자문이 필요한 경우에 산정
인쇄비	당해 사업 수행시 발생되는 공정별 산출물, 보고서 인쇄비, 복사비 등을 포함
자료조사비	당해 사업 수행 시 소요되는 문헌, 전문도서 등의 구입과 이에 소요되는 비용을 포함
기자재시험비	당해 사업의 수행 과정에서 기자재의 시험이 요구되는 경우 해당기자재의 시험에 소요되는 비용을 의미
현장운영비	직접인건비에 포함되지 아니한 보조요원의 급여와 현장사무실 임차료 및 운영비를 말한다. 당해 사업 수행에 필요한 보조요원의 급여와 수주자가 현장에 사무실을 설치하여 운영할 경우의 임차료와 현장운영경비를 포함
기타 직접경비	기타 직접경비는「SW사업 대가산정 가이드」의 직접경비 범위를 준용하여 산정

4. 기술료는 다음과 같다.

○ 기술료란 인증심사업무 관련자가 보유한 기술의 사용 및 기술축적을 위한 대가로서 조사연구비, 기술개발비, 기술훈련비 등을 포함한다.

기술료 = (직접인건비 + 제경비) × 20%(최대)

5. 제경비는 다음과 같다.

○ 제경비란 직접비에 포함되지 아니하고 인증심사업무의 행정운영 등을 위한 기획, 경영, 총무 등에서 발생하는 간접경비로서 급여, 사무실비, 사무용 소모품비, 비품비, 기계기구의 수선 및 상각비, 통신운반비, 회의비, 공과금, 운영활동 비용 등을 말한다.

제경비 = 직접인건비 × 110%(최대)

6. 최초 인증심사를 취득한 기관에서 유지관리심사, 변경심사, 갱신심사를 신청한 경우 심사구분에 따른 투입공수는 다음과 같다.

○ 유지관리심사는 최초 인증심사에 투입된 공수의 2분의 1로 산정한다.

○ 변경심사는 최초 인증심사에 투입된 공수의 3분의 2와 변경된 대상범위에 대하여 투입공수를 가감하여 산정한다.

○ 갱신심사는 최초 인증심사에 투입된 공수의 3분의 2와 갱신된 대상범위에 대하여 투입공수를 가감하여 산정한다.

심사구분	투입공수
유지관리심사	최초 인증심사의 1/2
변경심사	최초 인증심사의 2/3 ± 변경·갱신된 대상범위에 대한 투입공수
갱신심사	

7. 수수료의 감경

○ 인증기관은 신청기관에 대하여 다음의 경우 수수료를 감경할 수 있다.

- 대통령·국무총리 또는 안전행정부장관으로부터 개인정보 보호 관련 수상 실적이 있는 경우 수수료의 100분의 10의 범위 내에서 감경
- 중소기업기본법 시행령 제8조에 따른 소기업의 경우 수수료의 100분의 10의 범위 내에서 감경
- 소기업 및 소상공인 지원을 위한 특별조치법 제2조제2호에 따른 소상공인의 경우 수수료의 100분의 15의 범위 내에서 감경

○ 위 사항에 따른 수수료의 감경은 중복하여 적용할 수 없다.