개인정보보호 내부관리계획

2026. 7.

광주광역시교통문화연수원

목 차

제1장 총칙

제1조(목적)

개인정보보호 내부 관리계획(이하 '본 계획' 또는 '내부 관리계획' 이라 한다)은 개인정보 보호법 제29조(안전조치의무) 및 동법 시행령 제30조(개인정보의 안전성 확보 조치) 내부 관리계획의 수립 및 시행 의무에 따라 제정된 것으로 광주광역시교통문화연수원(이하 '연수원' 이라 한다)이 취급하는 개인정보를 체계적으로 관리하여 개인정보가 분실, 도난, 유출, 위조, 변조, 훼손, 오·남용 등이 되지 아니하도록 함을 목적으로 한다.

제2조(적용 범위)

본 계획은 정보통신망을 통하여 수집, 이용, 제공 또는 관리되는 개인정보 뿐만 아니라 서면 등 정보통신망 이외의 수단을 통해서 수집, 이용, 제공 또는 관리되는 개인정보 및 개인영상정보처리기기(CCTV)에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부 직원(계약직, 촉탁직, 인턴 근로자 포함) 및 외부업체 직원에 대해 적용된다.

제3조(용어 정의)

본 계획에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.

   가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보

   나. 해당 정보만으로 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는 지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.

   다. 가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 "가명정보"라 한다)

1의2. "가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

1의3. "익명정보"란 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보를 말하며, 이는 법 제58조의2에 따라 개인정보 보호법 적용 대상에는 제외한다.

2. “처리”란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 말한다.
3. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. “개인정보 보호책임자”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자로서, 법 제31조 및 시행령 제32조제2항에 따른 지위에 해당하는 자를 말한다.
5. “개인정보 보호담당자”란 각급기관의 실질적인 개인정보 보호업무를 담당하는 자로 개인정보 처리자가 지정한 자를 말한다.
6. “개인정보취급자”란 개인정보처리자의 지휘감독을 받아 개인정보를 처리하는 자로서 직원, 파견근로자, 시간제근로자 등을 말한다.
7. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
8. “개인정보처리시스템”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 응용시스템을 말한다.
9. "접속기록"이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 작업 내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보 주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
10. “위험도 분석"이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.
11. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다.
12. “고유식별정보”란 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 주민등록번호, 여권번호, 운전면허의 면허번호, 외국인등록번호를 말한다.
13. “민감정보”란 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활, 유전정보, 범죄경력 정보 등에 관한 정보와 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보를 말한다.

14. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.
15. “제3자”란 정보주체와 정보주체에 관한 개인정보를 수집·보유하고 있는 개인정보처리자를 제외한 모든 자를 의미하며, 정보주체의 대리인(명백히 대리의 범위 내에 있는 것에 한한다)과 법 제26조 제2항에 따른 수탁자는 제외한다.
16. “영상정보처리기기”란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 시행령 제3조에 따른 폐쇄회로 텔레비전(CCTV) 및 네트워크 카메라를 말한다.
17. “개인영상정보”란 영상정보처리기기에 의하여 촬영·처리되는 영상정보 중 개인의 초상, 행동 등과 관련된 영상으로서 해당 개인을 식별할 수 있는 정보를 말한다.
18. “영상정보처리기기운영자”란 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자를 말한다.
19. “공개된 장소”란 공원, 도로, 지하철, 상가 내부, 주차장 등 정보주체가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소를 말한다.
20. “과학적 연구”란 기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구를 말한다.

제4조(개인정보 보호원칙)

① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.

⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

⑦ 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다.

⑧ 개인정보처리자는 개인정보 보호법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

제2장 내부관리계획의 수립 및 시행

제5조(내부관리계획의 수립 및 승인)

① 개인정보 보호책임자는 연수원의 개인정보 보호를 위한 전반적인 사항을 포함하여 내부 관리계획을 수립하여야 한다.

② 개인정보 보호책임자는 개인정보 보호를 위한 내부 관리계획 수립 시 개인정보 보호와 관련한 법령 및 관련 규정을 준수하여야 한다.

③ 개인정보 보호책임자는 개인정보 보호담당자가 수립한 내부 관리계획의 타당성을 검토하여 개인정보 보호를 위한 내부 관리계획을 승인하여야 한다.

④ 개인정보 보호담당자는 개인정보 보호 관련 법령의 제·개정 사항 등을 반영하기 위하여 매년 내부관리계획의 타당성과 개정 필요성을 검토하여야 하며, 개정할 필요가 있다고 판단되는 경우 개정안을 작성하여 개인정보 보호책임자에게 보고·승인을 받아야 한다.

제6조(내부관리계획의 공표)

① 개인정보 보호책임자는 제5조에 따라 개정된 내부관리계획을 연수원 전 직원 및 관할 기관에 공표한다.

② 내부관리계획은 내부직원이 언제든지 열람할 수 있도록 하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제3장 개인정보 보호책임자의 의무와 책임

제7조(개인정보 보호책임자 및 개인정보 보호담당자의 지정)

① 연수원은 교육부 행정사무를 총괄하는 사람(교육부장)을 개인정보 보호책임자로 하며 개인정보 보호를 위한 실무 책임자인 개인정보 보호담당자를 지정한다.

○ 개인정보 보호책임자 및 보호담당자 지정현황

개인정보 보호책임자		개인정보 보호담당자
책임자	(교육부장) 전경복	(교육부 선임) 서진호
전 화	070-5005-9620	070-5005-9612

제8조(개인정보 보호책임자의 의무와 책임)

① 개인정보 보호책임자는 정보주체의 개인정보를 보호하고 개인정보와 관련한 정보주체의 불만을 처리하기 위하여 다음 각 호의 임무를 수행한다.

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독

7. 법 제30조에 따른 개인정보 처리방침의 수립 · 변경 및 시행

8. 개인정보 보호 관련 자료의 관리

9. 개인정보파일의 보유기간 산정

10. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

11. 개인정보 보호 분야별 책임자 지휘 · 감독

12. 가명정보 또는 추가정보의 관리 · 감독

13. 기타 정보주체의 개인정보 보호에 필요한 사항

② 개인정보 보호책임자는 개인정보 관련 업무의 효율적 운영을 위하여 개인정보 관리 전담부서의 직원 중 1인 이상을 개인정보 보호담당자로 임명한다.

○ 개인정보 분야별 책임자 지정 현황

부서	분야별 책임자	전화	비고
교육부	교육생 개인정보 : 서진호	070-5005-9612	

③ 개인정보 보호담당자는 개인정보 보호책임자를 보좌하여 개인정보 보호 업무에 대한 실무를 총괄하고 관리한다.

④ 개인정보 보호책임자는 개인정보관리에 대하여 분야별 책임자를 지정하여 관리할 수 있다.

⑤ 개인정보 보호책임자는 연1회 이상 내부관리계획의 이행 실태를 점검 · 관리한다.

제9조(개인정보 보호담당자의 의무와 책임)

① 개인정보 보호담당자는 정보주체의 개인정보 보호를 위하여 다음 각 호의 임무를 수행한다.

1. 개인정보 취급자의 인가 및 지정 · 관리 · 감독 · 교육

2. 개인정보파일의 지정, 보호 및 관리 · 감독

3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제

4. 각 처리와 개인정보에 대한 안정성 확보를 위한 기술적 · 물리적 보호조치 기준 이행

5. 개인정보 관련 개선 권고에 따른 조치사항 이행

6. 처리목적이 달성되거나 보유기간이 지난 개인정보의 파기

7. 개인정보 처리방침의 수립 · 변경 및 시행

8. 개인정보 보호 관련 자료의 관리

9. 개인정보 처리 실태의 정기적인 조사 및 개선

② 개인정보보호담당자는 개인정보취급자를 최소한으로 제한하여 지정하고 수시로 관리.감독하여야 하며, 직원 및 수탁자에 대한 교육 등을 통해 개인정보 침해사고를 사전에 예방한다.

③ 개인정보보호담당자는 개인정보보호 업무에 대한 실무를 총괄하고 관리한다.

제10조(개인정보취급자의 역할 및 책임)

① 개인정보취급자란 본원의 지휘 · 감독을 받아 정보주체의 개인정보 처리 업무를 수행하는 모든 근로형태의 직원(계약직, 촉탁직, 인턴 근로자 등)을 포함한다

② 개인정보취급자는 정보주체의 개인정보보호와 관련하여 다음과 같은 역할 및 책임을 이행한다.

1. 개인정보보호 활동 참여

2. 내부관리계획의 준수 및 이행

3. 개인정보의 기술적.물리적 보호조치 기준 이행

4. 법률에 근거하여 개인정보 수집, 이용, 제공, 파기 등 이행

5. 정보주체의 민원 신청접수 및 처리(열람, 정정, 삭제, 처리정지)

6. 업무상 알게 된 개인정보의 남용 및 제3자 제공 금지

7. 기타 정보주체의 개인정보보호를 위해 필요한 사항의 이행(서약서 제출 등)

제4장 개인정보의 관리 절차

제11조(개인정보의 수집 · 이용 · 제공 등)

① 개인정보처리자는 다음 각 호의 경우에 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 다만, 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

② 정보주체로부터 제1항 제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보의 수집 · 이용 목적
2. 수집하려는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 제11조 제7항에서 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다.

④ 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.

1. 정보주체의 동의를 받은 경우

2. 제11조 제1항 제2호 · 제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우

⑤ 제4항 제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

3. 개인정보를 제공받는 자의 성명(법인 또는 단체의 경우에는 그 명칭)과 연락처
4. 개인정보를 제공받는 자의 개인정보 이용 목적
5. 제공하는 개인정보의 항목
6. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
7. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

⑥ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 제11조 제7항에서 정하는 바에 따라 정보주체의 동의 없이 개인정보를 제공 할 수 있다.

⑦ 개인정보처리자는 제11조제3항 또는 제11조 제6항에 따라 정보주체의 동의 없이 개인정보를 이용 또는 제공(이하 “개인정보의 추가적인 이용 또는 제공”이라 한다)하려는 경우에는 다음 각 호의 사항을 고려해야 한다.

1. 당초 수집 목적과 관련성이 있는지 여부
2. 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부
3. 정보주체의 이익을 부당하게 침해하는지 여부
4. 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

⑧ 개인정보처리자는 제7항 각 호의 고려사항에 대한 판단 기준을 개인정보 처리방침에 미리 공개하고, 개인정보 보호책임자는 해당 기준에 따라 개인정보의 추가적인 이용 또는 제공을 하고 있는지 여부를 점검 · 관리해야 한다.

⑨ 개인정보처리자는 개인정보의 처리에 대하여 정보주체(법정대리인 포함)의 동의를 받을 때에는 정보주체가 명확하게 인지할 수 있도록 각각의 동의 사항을 구분하여 알리고 각각 동의를 받아야 한다. 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 하며, 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.

⑩ 개인정보처리자는 제11조제1항 제2호 내지 제6호에 따라 정보주체의 동의 없이 개인정보를 수집하는 경우에는 개인정보를 수집할 수 있는 법적 근거 등을 정보주체에게 알리기 위해 노력하여야 한다.

⑪ 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 제11조제2항 또는 제13조 제2항 각 호의 사항을 알리고 동의를 받아야 하며, 정보주체에게 동의 또는 동의 거부를 선택할 수 있음을 명시적으로 알려야 한다.

1. 개인정보를 수집·이용하고자 하는 경우로서 제11조 제1항 제2호 내지 제6호에 해당하지 않은 경우
2. 제13조 제1항에 따라 개인정보를 수집 목적 외의 용도로 이용하거나 제3자에게 제공하고자 하는 경우
3. 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하고자 하는 경우
4. 주민등록번호 외의 고유식별정보 처리가 필요한 경우로서 법령에 고유식별정보 처리 근거가 없는 경우
5. 민감정보를 처리하고자 하는 경우로서 법령에 민감정보 처리 근거가 없는 경우

⑫ 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하는 방법으로 전화에 의한 동의와 관련하여 통화내용을 녹취할 때에는 녹취사실을 정보주체에게 알려야 한다.

⑬ 만 14세 미만 아동의 개인정보를 처리하기 위하여 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 한다. 이 경우 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보(성명, 연락처)는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.

⑭ 선택적으로 동의할 수 있는 사항에 대한 동의를 받으려는 때에는 정보주체가 동의 여부를 선택할 수 있다는 사실을 명확하게 확인할 수 있도록 선택적으로 동의할 수 있는

사항 외의 사항과 구분하여 표시하여야 한다. 선택적으로 동의할 수 있는 사항을 동의하지 않는다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.

⑮ 제9항의 동의를 서면(「전자문서 및 전자거래 기본법」 제2조제1호에 따른 전자문서를 포함한다)으로 받을 때에는 다음 각 호에서 정하는 중요한 내용에 대하여 제16항에서 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하여야 한다.

1. 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실
2. 처리하려는 개인정보의 항목 중 다음 각 목의 사항

   가. 시행령 제18조에 따른 민감정보

   나. 여권번호, 운전면허의 면허번호 및 외국인등록번호

3. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간)
4. 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적
5. 개인정보의 수집·이용 목적, 수집·이용하려는 개인정보의 항목

⑯ 서면 동의 시 제15항의 중요한 내용의 표시 방법은 다음 각 호의 방법을 말한다.

1. 글씨의 크기는 최소한 9포인트 이상으로서 다른 내용보다 20퍼센트 이상 크게 하여 알아보기 쉽게 할 것
2. 글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 할 것
3. 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시할 것

제11조의2(가명정보의 처리 등)

① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있으며, 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 안 된다.

② 서로 다른 개인정보처리자 간의 가명정보의 결합은 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.

③ 개인정보처리자가 가명정보를 처리하는 경우에는 가명정보 및 가명정보를 원래의 상태로 복원하기 위한 추가 정보(이하 “추가정보”라 한다)에 대하여 다음 각 호의 기술적·관리적 및 물리적 안전성 확보 조치를 해야 한다.

1. 시행령 제30조에 따른 안전성 확보 조치
2. 가명정보와 추가정보의 분리 보관. 다만, 추가정보가 불필요한 경우에는 추가정보를 파기해야 한다.
3. 가명정보와 추가정보에 대한 접근 권한의 분리. 다만, 접근 권한의 분리가 어려운 정당한 사유가 있는 경우에는 업무 수행에 필요한 최소한의 접근 권한만 부여 하고 접근 권한의 보유 현황을 기록으로 보관하는 등 접근 권한을 관리·통제해야 한다.

④ 개인정보처리자는 가명정보를 처리하고자하는 경우에는 가명정보의 처리 내용을 관리하기 위하여 다음 각 호에 관한 사항에 대한 관련 기록을 작성하여 보관하여야 한다.

1. 가명정보 처리의 목적
2. 가명처리한 개인정보의 항목
3. 가명정보의 이용내역
4. 제3자 제공 시 제공받는 자
5. 그 밖에 가명정보의 처리 내용을 관리하기 위하여 보호위원회가 필요하다고 인정하여 고시하는 사항

⑤ 누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 안 된다

⑥ 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체없이 회수·파기하여야 한다. 이 경우 제3자에게 제공한 가명정보도 관련 절차에 따라 파기하여야 한다.

⑦ 가명정보를 처리하는 경우 처리 목적을 벗어나서 가명정보를 오·남용해서는 아니 된다.

⑧ 개인정보처리자는 가명 처리한 가명정보가 개인정보를 포함하고 있는지 적정성 검토를 거친 후에 가명정보를 처리할 수 있다. 적정성 검토와 관련된 주요 사항은 교육분야 가명·익명정보 처리 가이드라인을 준용한다.

⑨ 가명정보는 제14조, 제17조, 제33조부터 제35조까지, 제36조 제4항의 규정을 적용하지 않는다.

제11조의3(개인정보의 수집 제한)

① 개인정보처리자는 제11조 제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.

② 정보주체의 동의를 받아 개인정보를 수집하는 경우에는 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알려야 한다.

③ 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.

제12조(민감정보와 고유식별정보의 처리 제한)

① 개인정보처리자는 민감정보 또는 고유식별정보를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 정보주체에게 제11조제2항 각 호 또는 제11조 제5항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보 또는 고유식별정보의 처리를 요구하거나 허용하는 경우

② 개인정보처리자가 제1항 각 호에 따라 민감정보 또는 고유식별정보를 처리하는 경우에는 필요한 최소한의 한도 내에서 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

③ 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법률 · 대통령령 · 국회규칙 · 대법원규칙 · 헌법재판소규칙 · 중앙선거관리위원회규칙 및 감사원 규칙에서 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 보호위원회가 고시로 정하는 경우

제13조(개인정보의 목적 외 이용 및 제3자 제공의 제한)

① 정보주체의 개인정보를 제11조 제1항에 따른 범위를 초과하여 이용하거나 제11조 제4항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다. 다만, 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자 에게 제공할 수 있다. 단, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
5. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
6. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
7. 법원의 재판업무 수행을 위하여 필요한 경우
8. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

② 개인정보처리자는 제1항 제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보를 제공받는 자의 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처
2. 개인정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적)
3. 이용 또는 제공하는 개인정보의 항목
4. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간)
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 공공기관은 제1항 제2호부터 제6호까지, 제8호 및 제9호에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 개인정보를 목적 외 이용 등을 한 날부터 30일 이내에 다음 각 호의 사항을 관보 또는 인터넷 홈페이지에 10일 이상 계속 게재하되, 게재를 시작하는 날은 목적 외 이용 등을 한 날부터 30일 이내여야 한다.

1. 목적 외 이용 등을 한 날짜
2. 목적 외 이용 등의 법적 근거
3. 목적 외 이용 등의 목적
4. 목적 외 이용 등을 한 개인정보의 항목

④ 제13조 제1항 각호에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 “개인정보의 목적 외 이용 및 제3자 제공대장”[별지 제8 호]에 기록 · 관리한다.

⑤ 정보주체의 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 이용 기간, 이용 형태 등을 제한하거나, 개인정보의 안전성 확보를 위하여 필요한 구체적인 조치를 마련하도록 문서로 요청 하여야 한다. 이 경우 요청을 받은 자는 그에 따른 조치를 취하고 그 사실을 개인정보를 제공한 개인정보처리자에게 문서로 알려야 한다.

⑥ 개인정보의 목적 외 이용 및 제3자 제공 절차는 다음과 같다.

< 목적 외 이용 · 제3자 제공 절차 >

절 차	주 요 내 용
1. 법적근거 검토	- 목적 외 이용·제3자 제공이 가능한 경우에 해당하는지 법적근거 검토 ※제13조 제1항 제2호부터 제9호까지 해당 여부 검토
2. 동의절차 이행	- 법적 근거가 없는 경우에는 정보주체로부터 별도의 동의를 받아야 함 ※ 동의절차 이행시 제공받는자, 수집목적, 수집항목, 보유 및 이용기간, 거부시 불이익 명시
3. 대장 기록·관리	-『개인정보의 목적 외 이용 및 제3자 제공대장』을 기록·관리하여야 함 ※ [별지 제8호] 참조
4. 주요 내용 공개	- 제13조 제1항 제2호부터 제6호까지, 제8호, 제9호에 해당하는 경우 - 30일 이내에 이용 또는 제공 날짜, 법적 근거, 목적, 항목 등에 관한 사항을 관보 또는 인터넷 홈페이지(10일 이상) 등에 게재
5. 보호조치 요구	- 제3자 제공시에는 이용목적, 이용방법, 이용기간, 이용형태 등을 제한하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 문서로 요청
6. 조치결과 제출	- 안전성 확보조치 요청을 받은 자는 그에 따른 조치를 취한 후, 그 결과를 개인정보를 제공한 개인정보처리자에게 문서로 알려야 함

제14조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지)

① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 요구가 있는 날로부터 3일 이내에 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.

1. 개인정보의 수집 출처

2. 개인정보의 처리 목적

3. 법 제37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실

② 정보주체의 요구가 없더라도 다음 각 호의 기준에 해당하는 개인정보처리자가 정보주체 이외로부터 개인정보를 수집하여 처리하는 때에는 제1항 각 호의 모든 사항을 서면・전화・문자전송・전자우편 등 정보주체가 쉽게 알 수 있는 방법으로 개인정보를 제공받은 날부터 3개월 이내에 정보주체에게 알려야 한다.

다만, 개인정보처리자가 수집한 정보에 연락처 등 정보주체에게 알릴 수 있는 개인정보가 포함되지 아니한 경우에는 그러하지 아니하다.

1. 5만명 이상의 정보주체에 관하여 법 제23조에 따른 민감정보(이하 "민감정보"라 한다) 또는 법 제24조제1항에 따른 고유식별정보를 처리하는 자
2. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자

③ 제2항의 경우로서 정보주체의 동의를 받은 범위에서 연 2회 이상 주기적으로 개인정보를 제공받아 처리하는 경우에는 개인정보를 제공받은 날부터 3개월 이내에 정보주체에게 알리거나 그 동의를 받은 날부터 기산하여 연 1회 이상 정보주체에게 알려야 한다.

④ 제1항과 제2항 본문은 다음 각 호의 어느 하나에 해당하는 경우에는 적용하지 아니한다. 다만, 정보주체의 권리보다 명백히 우선하는 경우에 한한다.

1. 고지를 요구하는 대상이 되는 개인정보가 법 제32조 제2항(범죄의 수사 등에 관한 사항 등) 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우
2. 고지로 인하여 다른 사람의 생명・신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

⑤ 제2항 각 호의 어느 하나에 해당하는 개인정보처리자는 제1항에 따라 알린 경우 다음 각 호의 사항을 법 제21조(개인정보의 파기) 또는 법 제37조 제4항(개인정보의 처리정지)에 따라 해당 개인정보를 파기할 때까지 보관・관리하여야 한다.

1. 정보주체에게 알린 사실
2. 알린 시기
3. 알린 방법

⑥ 개인정보처리자는 제4항 단서에 따라 정보주체의 요구를 거부하는 경우에는 정당한 사유가 없는 한 정보주체의 요구가 있는 날로부터 3일 이내에 그 거부의 근거와 사유를 정보주체에게 알려야 한다.

제15조(개인정보 취급자의 제한)

① 개인정보보호담당자는 개인정보를 취급할 수 있는 자를 다음 각 호에 해당하는 자로 정하여 최소한으로 제한하여야 한다.

1. 정보주체를 직접 상대로 하여 업무를 수행하는 자
2. 개인정보 보호책임자 등 개인정보관리 업무를 수행하는 자
3. 개인정보가 저장된 데이터베이스를 포함한 전산 관련 업무를 수행하는 자
4. 기타 업무상 개인정보의 취급이 불가피한 자

제16조(개인정보처리의 위탁)

① 개인정보의 처리 업무를 위탁하는 때에는 수탁자의 처리업무의 지연, 처리업무와 관련 없는 불필요한 개인정보의 요구, 처리기준의 불공정 등의 문제점을 종합적으로 검토하여 이를 방지하기 위하여 필요한 조치를 마련하여야 한다.

② 제1항의 규정에 의한 위탁계약을 체결하는 때에는 수탁자와 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적 · 관리적 보호조치에 관한 사항
3. 위탁업무의 목적 및 범위
4. 재위탁 제한에 관한 사항
5. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
6. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
7. 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

③ 개인정보의 처리 업무를 위탁하는 경우 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 인터넷 홈페이지에 지속적으로 공개하여야 한다.

④ 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(이하 “서면등의 방법”이라 한다)에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다. 위탁자가 서면 등의 방법으로 정보주체에게 알릴 수 없는 경우에는 인터넷 홈페이지에 30일 이상 게재하여야 한다.

⑤ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 관리 · 감독 하여야 한다.

⑥ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.

⑦ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상 책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다.

⑧ 수탁자는 위탁받은 개인정보를 보호하기 위하여 행정안전부장관이 고시하는 「개인정보의 안전성 확보조치 기준」에 따른 기술적 · 관리적 · 물리적 조치를 하여야 한다.

제17조(개인정보(파일)의 파기)

① 개인정보취급자는 보유기간의 경과, 개인정보의 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 그로부터 5일 이내에 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니한다.

② 개인정보 보호책임자는 개인정보 일부 파기 승인 업무에 대하여 개인정보보호담당자에 위임하여 관리하며 매년 개인정보 일부 파기현황을 개인정보 보호책임자에게 보고하여야 한다. 개인정보 일부만 파기하는 경우는 다음 각 호에 준한다.

1. 운영 중인 개인정보가 포함된 여러 파일 중 특정 파일을 파기하는 경우

2. 개인정보가 저장된 백업용 디스크나 테이프에서 보유기간이 만료된 특정 파일이나 특정 정보주체의 개인정보만 파기하는 경우

3. 운영 중인 데이터베이스에서 탈퇴한 특정 회원의 개인정보를 파기하는 경우

4. 회원가입신청서 종이 문서에 기록된 정보 중 특정 필드의 정보를 파기하는 경우 등

③ 개인정보 보호담당자는 개인정보파일의 보유기간, 처리목적 등을 반영한 개인정보 파기 계획을 수립하여 시행·확인하여야 한다.

④ 개인정보취급자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각·파쇄 등)

2. 전용 소자장비를 이용하여 삭제

3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

4. 개인정보 일부 파기 시 전자적 파일은 개인정보 삭제 후 복구 및 재생되지 않도록 관리·감독하고, 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우는 해당 부분을 마스킹, 천공 등으로 삭제

⑤ 개인정보취급자는 제1항에 따른 개인정보파일 파기 사유가 발생한 경우 “개인정보 파일 파기 요청서”[별지 제9호]를 작성하여 개인정보 보호책임자의 승인을 득한 후 파기하고 연수원 교육관리시스템(CMS)의 데이터를 개인정보 보호책임자의 승인을 통해 삭제하고 “개인정보파일 파기 관리대장”[별지 제10호]에 기록·관리하여야 한다.

⑥ 개인정보취급자는 제2항의 각 호에 준하는 개인정보 일부 파기 사유가 발생한 경우 개인정보 보호담당자의 승인을 득한 후 파기하고 이를 기록·관리한다. 이때, 파기 승인과 기록·관리는 “개인정보파일 파기 관리대장”[별지 제10호]를 이용한다.

⑦ 제1항 단서에 따라 법령에 근거하여 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 물리적 또는 기술적 방법으로 분리하여서 저장·관리하여야 하고 개인정보처리방침 등을 통하여 정보주체가 이를 알 수 있도록 하여야 한다.

제18조(개인정보파일의 등록 및 공개)

① 개인정보 보호담당자는 1개의 개인정보파일에 대하여 1개의 개인정보파일 대장을 작성하여 관리하여야 한다.

② 개인정보보호담당자는 개인정보보호 종합지원시스템에 접속하여 개인정보파일을 등록 및 변경 신청하여야 한다.

③ 다음 각 호의 어느 하나에 해당하는 개인정보파일에 대하여는 제1항부터 제3항까지 적용하지 아니한다.

1. 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일

2. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일

3. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일

4. 개인정보처리자의 내부적 업무처리만을 위하여 사용되는 개인정보파일

5. 다른 법령에 따라 비밀로 분류된 개인정보파일

6. 법 제58조제1항에 따라 적용이 제외되는 다음 각 목의 개인정보파일

   가. 「통계법」에 따라 수집되는 개인정보파일

   나. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보파일

   다. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일

7. CCTV 등 영상정보처리기기를 통하여 처리되는 개인영상정보파일

8. 자료·물품 또는 금전의 송부, 1회성 행사 수행 등의 목적만을 위하여 운용하는 경우로서 저장하거나 기록하지 않고 폐기할 목적으로 수집된 개인정보파일

④ 제3항 제4호에 해당하는 내부적 업무처리만을 위하여 사용되는 개인정보파일에는 임직원 전화기록부, 비상연락망, 인사기록파일, 요금정산, 회의 참석자 수당지급, 자문 기구 운영 등이 있다.

제19조(개인정보 처리방침의 수립 및 공개)

① 개인정보 보호책임자는 개인정보처리방침을 수립하고 운영 중인 인터넷 홈페이지를 통해 첫 화면 또는 첫 화면과의 연결화면에 지속적으로 게재하여야 한다.

② 별도 업무용 홈페이지를 운영하는 개인정보 보호담당자는 등록대상이 되는 개인정보 파일에 대하여 별도의 개인정보처리방침을 정한다.

③ 개인정보처리방침을 게재하는 경우에는 “개인정보처리방침” 이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.

④ 개인정보처리방침에 반드시 포함되어야 할 사항은 다음 각 호와 같다.

1. 개인정보의 처리 목적
2. 처리하는 개인정보의 항목
3. 개인정보의 처리 및 보유 기간
4. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
5. 개인정보의 파기절차 및 파기방법(제17조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
6. 개인정보 처리 수탁자 담당자 연락처, 수탁자의 관리 현황 점검 결과 등 개인정보처리 위탁에 관한 사항(해당하는 경우에만 정한다)
7. 시행령 제30조 제1항에 따른 개인정보의 안전성 확보조치에 관한 사항
8. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
9. 개인정보 처리방침의 변경에 관한 사항
10. 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
11. 개인정보의 열람청구를 접수·처리하는 부서
12. 정보주체의 권익침해에 대한 구제방법
13. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)

⑤ 개인정보 보호책임자 또는 개인정보보호담당자가 개인정보처리방침을 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 인터넷 홈페이지 등에 지속적으로 공

개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개하여야 한다.

제20조(개인정보 영향평가)

① 개인정보보호담당자는 다음 각 호의 어느 하나에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우 그 위험요인의 분석과 개선사항도 도출을 위하여 개인정보 영향평가를 의무적으로 수행한 후 개인정보 보호책임자에게 그 결과를 제출하여야 한다.

1. 구축 · 운용 또는 변경하려는 개인정보파일로서 5만 명 이상의 정보주체에 관한 법 제23조에 따른 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축 · 운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축 · 운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만 명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축 · 운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인 정보파일
4. 법 제33조제1항에 따른 개인정보 영향평가를 받은 후에 개인정보 검색 체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정

제5장 개인정보의 안전성 확보조치

제21조(물리적 안전조치)

① 개인정보보호담당자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 장소에 대하여 제한구역 또는 통제구역으로 지정하고 이에 대한 출입통제 절차를 수립·운영하여야 하며, 잠금장치를 설치하고 출입자 관리대장을 비치하여 허가받지 않은 자의 출입을 통제하여야 한다.

1. 출입을 통제하는 방법으로는 물리적 접근 방지를 위한 장치를 설치·운영하고 이에 대한 출입 내역을 전자적인 매체 또는 수기문서 대장에 기록하여야 한다.
2. 수기문서 대장을 이용하여 출입내역을 기록할 때에는 출입자, 출입일시, 출입목적, 소속 등이 포함되어 있어야 한다.

② 개인정보 보호담당자는 물리적 접근제한 관리대장의 출입 및 열람 내용을 주기적으로 검토하여 정당하지 않은 권한으로 출입하거나 열람하는 경우가 있는지를 점검하여 확인하여야 한다.

③ 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 캐비넷 등 안전한 장소에 보관하여야 하며, 개인정보가 포함된 보조저장매체의 반 출·입 통제를 위한 보안대책을 마련하여야 한다.

제22조(출력 복사시 보호조치)

① 개인정보 보호담당자는 개인정보가 포함된 정보를 출력하거나 복사할 경우에 개인정보 유출사고를 방지하기 위한 보호조치를 취하여야 한다.

② 개인정보 보호담당자는 민감한 개인정보 또는 다량의 개인정보가 포함된 정보를 출력하거나 복사할 경우 출력·복사자의 성명, 일시, 활용목적, 활용기간 등을 별도의 대장에 기록·관리하고, 출력·복사물을 보관하는 경우 제21조의 물리적 안전조치를 준수하여 개인정보 유출 등에 대한 책임 소재를 확인할 수 있도록 강화된 보호조치를 추가로 적용하여야 한다.

③ 개인정보취급자는 개인정보의 이용을 위하여 출력 및 복사한 개인정보의 이용 목적이 완료된 경우 분쇄기로 분쇄하거나 소각하는 등의 안전한 방법으로 파기하여야 한다.

제23조(접근권한의 관리)

① 개인정보 보호담당자는 개인정보처리시스템에 대한 접근권한을 업무수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 개인정보 보호담당자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보 처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

③ 개인정보 보호담당자는 제1항 및 제2항에 따른 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 개인정보 보호담당자는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자 계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 개인정보 보호담당자는 개인정보처리시스템에 대하여 다음 각 호의 내용이 포함된 접근권한 관리지침을 수립하여 운영하여야 한다.

1. 권한에 대한 총괄 관리책임자 지정에 관한 사항
2. 접근권한의 정의 및 업무분장, 책임 및 역할에 관한 사항
3. 사용자 등록, 권한 부여·변경·중지 절차 및 방법 등에 관한 사항
4. 사용자 및 정보 중요도별 접근권한 차등 부여에 관한 사항
5. 외부인력 및 업무보조자의 권한 관리에 관한 사항
6. 접근권한 관리이력 보관에 관한 사항
7. 보안서약서 징구 등에 관한 사항

⑥ 개인정보 보호담당자는 개인정보처리시스템의 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보 처리시스템에 대한 접근을 제한하는 방법 등 필요한 기술적 조치를 하여야 한다.

⑦ 개인정보 보호담당자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 다음 각 호의 사항을 포함하여 비밀번호 작성규칙을 수립하여 적용하여야 한다.

1. 영문, 숫자, 특수문자를 조합하여 최소 9자리 이상의 길이로 구성

2. 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고
3. 비밀번호 변경은 분기별 1회 이상 정기적으로 변경하고 제3자에게 노출되었을 경우 즉시 새로운 비밀번호로 변경

제24조(접근통제)

① 개인정보 보호담당자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.
1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응

② 개인정보 보호담당자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN:Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

③ 개인정보 보호담당자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통해 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일기기 및 관리용 단말기 등에 접근통제에 관한 다음 각 호의 조치를 취하여야 한다.
1. 인터넷 홈페이지 중 서비스 제공에 사용되지 않거나 관리되지 않는 사이트 또는 URL에 대한 삭제·차단 조치
2. 인터넷 홈페이지 설계·개발 오류 또는 개인정보취급자의 업무상 부주의 등으로 인터넷 서비스 검색엔진(구글링 등) 등을 통해 관리자 페이지와 취급중인 개인정보가 노출되지 않도록 조치
3. 개인정보취급자는 개인정보처리시스템, 업무용 컴퓨터 및 모바일기기 및 관리용 단말기 등에 P2P, 공유설정은 기본적으로 사용하지 않는 것이 원칙이나, 업무상 반드시 필요한 경우에는 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 접근통제 등에 관한 안전조치
4. 개인정보취급자의 부주의로 인한 개인정보 및 개인정보파일 인터넷 홈페이지 게시 방지

④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·위조·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하여야 하며, 그 결과에 따른 보완 조치를 하여야 한다.

⑤ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.

⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System) 나 보안프로그램 등에서 제공하는 접근 통제 기능을 이용할 수 있다.

⑦ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

제25조(개인정보의 암호화)

① 개인정보보호담당자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조 저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

② 개인정보 보호담당자는 비밀번호 및 바이오정보를 암호화하여 저장하여야 한다. 다만 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

③ 개인정보 보호담당자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 개인정보보호담당자는 내부망에 고유식별정보를 저장하는 경우, 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 경우 해당 개인정보 영향평가의 결과
2. 암호화 미적용시 위험도 분석에 따른 결과

⑤ 개인정보 보호담당자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑥ 개인정보 보호담당자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

⑦ 개인정보보호담당자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

제26조(접속기록의 보관 및 위·변조 방지)

① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 5만명 이상의 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.

② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 하며, 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 그 사유를 반드시 확인하여야 한다.

③ 접속기록을 월 1회 이상 정기적으로 점검 시에는 다음과 같이 접속기록 내 비정상 행위의 여부를 점검하여야 한다.

1. 계정 : 접근권한이 부여되지 않은 계정으로 접속한 행위 등
2. 접속일시 : 출근시간 전, 퇴근시간 후, 새벽시간, 휴무일 등 업무시간 외에 접속한 행위 등
3. 접속지 정보 : 인가되지 않은 단말기 또는 지역(IP)에서 접속한 행위 등
4. 정보주체 정보 : 특정 정보주체에 대하여 과도하게 조회, 다운로드 등의 행위 등
5. 수행업무 : 대량의 개인정보에 대한 조회, 정정, 다운로드, 삭제 등의 행위 등
6. 그 밖에 짧은 시간에 하나의 계정으로 여러 지역(IP)에서 접속한 행위 등

④ 개인정보처리시스템에 접근하여 개인정보를 다운로드한 경우에는 그 사유를 확인하고, 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드한 것으로 확인이 되었다면 개인정보취급자가 다운로드 한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다.

⑤ 개인정보처리자의 업무 현황을 고려하여 다운로드한 사유를 확인하여야하는 기준은 다음과 같다.

1. **(다운로드 정보주체의 수)** 통상적으로 개인정보 처리 건수가 일평균 20건 미만인 소규모에서 개인정보취급자가 100명 이상의 정보주체에 대한 개인정보를 다운로드한 경우 사유 확인
2. **(일정기간 내 다운로드 횟수)** 개인정보취급자가 1시간 내 다운로드한 횟수가 20건 이상일 경우 단시간에 수차례에 걸쳐 개인정보를 다운로드 한 행위에 대한 사유 확인
3. **(업무시간 외 다운로드 수행)** 새벽시간, 휴무일 등 업무시간 외 개인정보를 다운로드 한 경우 사유 확인

⑥ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제27조(관리용 단말기 안전조치 및 악성프로그램 등 방지)

① 개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.

1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
2. 본래 목적 외로 사용되지 않도록 조치
3. 악성프로그램 감염 방지 등을 위한 보안조치 적용

② 개인정보처리자는 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성 프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시
3. 발견된 악성프로그램에 대한 삭제 등 대응 조치

③ 보안 프로그램의 실시간 감시 기능을 적용하여야 한다.

제28조(재해·재난 대비 안전조치)

① 개인정보 보호담당자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

② 개인정보 보호담당자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 하며, 개인정보처리시스템 백업 및 복구를 위한 계획은 위기대응 매뉴얼에 포함할 수 있다. 백업 및 복구 계획에는 다음 각 호의 사항을 포함하도록 한다.

1. 개인정보처리시스템 구성 요소(개인정보 보유량, 개인정보 항목, 중요도, 시스템 연계 장비 · 설비 등)
2. 재해 · 재난 등에 따른 파급효과(개인정보 유출, 손실, 훼손 등) 및 초기대응 방안
3. 개인정보처리시스템 백업 및 복구 우선순위, 목표시점 · 시간
4. 개인정보처리시스템 백업 및 복구 방안, 절차
5. 업무분장, 책임 및 역할
6. 실제 발생 가능한 사고에 대한 정기적 점검, 사후처리 및 지속관리 등

제29조(위험도 분석)

① 개인정보 보호담당자는 개인정보처리시스템에 대하여 내부망에 고유식별정보를 저장하는 경우에는 위험도 분석을 실시하여 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안을 마련하여야 한다.

② 개인정보 보호담당자는 개인정보처리시스템에 대한 위험도 분석을 실시한 후 개인정보 보호책임자에게 그 결과를 제출하여야 한다.

③ 위험도 분석 절차는 아래와 같다.

1. 위험도 분석을 위해 개인정보 파일 및 고유식별정보 보유 여부 등 현황조사
2. 개인정보 파일 단위별로 위험도 분석 항목별 점검을 수행
3. 위험도 분석 결과보고서를 작성하여 내부결재 후 보관
4. 점검 결과에 따라 고유식별정보 암호화 등을 수행

제30조(영상정보처리기기의 설치 · 운영 제한)

① 영상정보처리기기운영자는 개인영상정보의 처리에 관한 업무를 총괄해서 책임질 개인영상정보 관리책임자를 지정하여야 한다. 다만 개인영상정보 관리책임자를 개인정보 보호책임자로 지정하여 운영할 수 있다.

② 영상정보처리기기를 설치·운영 하려는 경우 "개인정보 보호법 제25조"에 따라 전문가 및 이해관계인의 의견수렴 절차를 거쳐야 하며, 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 하여서는 아니 된다.

③ 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.

④ 개인영상정보 관리책임자는 다음 각 호의 항이 포함된 안내판을 설치하여야 한다.

1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자의 성명 및 연락처
4. 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 수탁자의 명칭 및 연락처

⑤ 개인영상정보 관리책임자는 영상정보처리기기 운영·관리 방침을 수립하여 홈페이지 등에 공개하여야 한다.

⑥ 개인영상정보 관리책임자는 개인영상정보처리기기의 운영을 위하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부관리계획 제21조에서 제27조까지의 안전성 확보에 필요한 관리적·기술적·물리적 보호조치를 준수하여야 한다.

⑦ 개인영상정보 관리책임자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다. 다만, 공공기관이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서로 하여야 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

제6장 개인정보보호 교육

제31조(개인정보보호 교육계획의 수립)

① 개인정보 보호책임자는 다음 각 호의 사항을 포함하는 연간 개인정보보호 교육계획을 매년 수립하여야 한다.

1. 교육목적 및 대상
2. 교육내용
3. 교육 일정 및 방법

② 개인정보 보호책임자는 수립한 개인정보보호 교육계획을 실시한 이후에 교육의 성과와 개선 필요성을 검토하여 차년도 교육계획 수립에 반영하여야 한다.

제32조(개인정보보호 교육의 실시)

① 개인정보 보호책임자는 개인정보보호에 대한 직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 직원 및 관할기관을 대상으로 연 1회 이상 개인정보보호 교육을 실시한다.

② 개인정보 보호담당자는 개인정보 처리 업무의 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 연 1회 이상 수탁자 개인정보보호 교육을 실시한다.

③ 교육 대상에 따라 역할에 맞게 차별화된 교육 내용을 포함하여 개인정보보호 교육을 실시한다.

대상	교육 내용
개인정보 보호책임자	개인정보 보호책임자의 역량 및 관리책임 강화 등
개인정보 보호담당자	개인정보 라이프 사이클에 따른 처리단계별 조치사항, 개인정보의 안전성 확보 조치 기준, 개인정보파일 관리, 정보주체의 권리보장, 노출방지 및 자율개선 등
개인정보취급자(전직원)	개인정보 보호법 준수사항 안내, 개인정보 수집, 관리, 파기 절차 안내, 안전성 확보 조치, 각종 사례 안내 등
수탁자	위탁업무 준수사항, 안전성 확보 조치, 재위탁 금지 등

④ 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 상급기관, 외부 전문기관이나 전문요원에 위탁하여 교육을 실시할 수 있다.

⑤ 개인정보 보호책임자는 신규 채용자, 전입자에게 개인정보보호 교육을 실시하여야 하며, 개인정보 관련 전문기관 교육 및 기술 세미나 참석 등을 장려하는 등 개인정보 보호담당자의 업무 전문성을 제고하기 위하여 노력하여야 한다.

⑥ 개인정보보호에 대한 중요한 전파 사례가 있거나 개인정보보호 업무와 관련하여 변경된 사항이 있는 경우, 개인정보 보호책임자는 부서 회의 등을 통해 수시 교육을 실시할 수 있다.

제7장 정보주체의 권리보장

제33조(개인정보의 열람)

① 정보주체는 자신의 개인정보에 대한 열람을 요구하려면 다음 각 호의 사항 중 열람하려는 사항을 표시하여 [별지 제1호]에 따른 “개인정보 열람요구서”를 개인정보처리자에게 제출하여야 한다.

1. 개인정보의 항목 및 내용
2. 개인정보의 수집·이용의 목적
3. 개인정보 보유 및 이용 기간
4. 개인정보의 제3자 제공 현황
5. 개인정보 처리에 동의한 사실 및 내용

② 제1항의 요구를 받은 개인정보처리자는 개인정보 열람요구서를 받은 날부터 10일 이내에 정보주체가 해당 개인정보를 열람할 수 있도록 하여야 한다. 이 경우 해당 기간 내에 열람하게 할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리고 열람을 연기할 수 있으며, 그 사유가 소멸하면 그 날로부터 10일 이내에 열람하게 하여야 한다.

③ 개인정보 열람요구를 받은 업무부서는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있으며, 열람이 제한되는 사항을 제외한 부분은 열람할 수 있도록 하여야 한다.

1. 법률에 따라 열람이 금지되거나 제한되는 경우
2. 타인의 생명·신체를 해할 우려가 있거나 타인의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

④ 제2항에 따라 열람을 연기하거나 제3항에 따라 열람을 제한·거절하려는 경우에는 열람 요구를 받은 날부터 10일 이내에 연기 또는 제한이나 거절의 사유 및 이의제기 방법을 [별지 제3호] “개인정보 일부열람·열람연기·열람거절 통지서”로 해당 정보주체에게 알려야 한다.

제34조(개인정보의 정정·삭제)

① 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 [별지 제1호] “개인정보 정정·삭제 요구서”를 통해 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다.

② 개인정보처리자는 정당한 사유가 없는 한 제1항에 따른 개인정보 정정·삭제 요구를 받은 날부터 10일 이내에 다음 각 호 중 하나의 조치를 한 후 [별지 제4호] “개인정보 정정·삭제 결과통지서”로 해당 정보주체에게 알려야 한다.

1. 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 사실
2. 제1항 단서에 해당하여 삭제 요구에 따르지 아니한 경우에는 그 사실 및 이유 (근거법령의 내용 등)와 이의제기방법

③ 개인정보처리자가 제2항의 조치를 취하기 위하여 그 개인정보를 조사할 때 필요하면 해당 정보주체에게 정정·삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있다.

④ 개인정보처리자가 제2항에 따라 개인정보를 삭제할 때에는 그 개인정보가 복구 또는 재생되지 아니하도록 조치하여야 한다.

제35조(개인정보의 처리정지)

① 정보주체는 개인정보처리자에게 [별지 제1호] “개인정보 처리정지 요구서” 를 통하여 제18조에 따라 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구할 수 있다.

② 제1항의 요구를 받은 개인정보처리자는 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 단, 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.

1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
2. 타인의 생명·신체를 해할 우려가 있거나 타인의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우
4. 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우

③ 제1항의 요구를 받은 개인정보처리자는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 다음 각 호 중 하나의 조치를 한 후 그 사실을 [별지 제4호]에 따른 ‘개인정보 처리정지 요구에 대한 결과통지서’로 해당 정보주체에게 알려야 한다.

1. 처리정지 조치를 한 사실
2. 제2항 단서에 해당하여 처리정지 요구에 따르지 아니한 경우에는 그 사실 및 이유와 이의제기 방법

④ 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다.

제8장 개인정보 침해대응 및 피해구제

제36조(개인정보 침해사고 대응)

① 개인정보의 유출이라 함은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 것으로서, 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우

2. 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우

3. 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 그 밖에 저장매체가 권한이 없는 자에게 잘못 전달된 경우

4. 그 밖에 권한이 없는 자에게 개인정보가 전달된 경우

② 개인정보 노출이라 함은 일반 인터넷 이용자가 해킹 등 특별한 방법을 사용하지 않고 정상적으로 인터넷을 이용하면서 다른 사람의 개인정보를 취득할 수 있도록 인터넷 상에서 관련 정보가 방치되어 있는 경우를 말한다.

③ 개인정보취급자는 개인정보 침해(유출 · 노출)가 발생한 것을 인지한 경우 또는 그러한 침해의 발생이 의심되는 경우 지체 없이 업무부서의 개인정보보호 보호담당자에게 이를 알려야 한다.

④ 실제로 유출 사고가 발생한 것으로 확인된 때에는 정당한 사유가 없는 한 5일 이내에 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검 · 보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후부터 5 일 이내에 정보주체에게 알릴 수 있다.

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 피해구제절차

5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

⑤ 제4항 각 호의 사항을 모두 확인하기 어려운 경우에는 정보주체에게 다음 각 호의 사실만을 우선 알리고, 추후 확인되는 즉시 알릴 수 있다.

1. 정보주체에게 유출이 발생한 사실

2. 제4항의 통지항목 중 확인된 사항

⑥ 개인정보 보호담당자는 개인정보 유출 사고의 미인지로 인해 해당 정보주체에게 개인정보 유출 통지를 하지 아니한 경우에는 실제 유출 사고를 알게 된 시점을 입증하여야 한다.

⑦ 개인정보 보호담당자는 1명이라도 정보주체에 관한 개인정보가 유출된 경우에는 [별지 제5 호] “개인정보 유출신고(보고)서” 를 작성하여 개인정보 보호책임자에게 제출하여야 하며, 개인정보 보호책임자는 유출내용 및 조치결과를 5일 이내에 교육부에 보고하여야 한다. 1천명 이상의 개인정보가 유출된 경우에는 보호위원회 또는 전문기관(한국인터넷진흥원)에 신고하여야 하며, 제4항에 따른 통지와 함께 인터넷 홈페이지에 통지항목을 7일 이상 게재하여야 한다.

제37조(개인정보 보호조직 구성 및 운영)

① 개인정보 침해사고 발생 시 신속한 대응, 공격탐지, 피해복구, 예방 등 종합적이고 체계적인 공동대응 체제구축을 위해 개인정보 보호책임자(교육부장) 주관 하에 “개인정보 보호조직(침

해사고 대응반)”을 편성하고, 24시간 비상근무체제를 운영하며, 광주광역시청 주무부서 및 유관단체(각 조합 및 협회)와 긴밀한 협조체제를 유지함으로써 침해사고에 신속히 대처한다.

② 중요정보시스템에 대한 백업(시스템, DB 등)을 실시하고, 백업된 자료는 원격지로 소산하여 중요 정보 유실을 방지한다.

③ 각 조직별 역할은 아래와 같다.

구 분	내 용
개인정보 보호책임자	- 개인정보 침해사고 예방, 처리 및 재발방지 총괄 관리 - 개인정보 침해사고 발생 시 침해사고 처리책임자를 지정 - 침해사고 대응조직 구성 및 운영
개인정보 보호조직 (개인정보 침해사고대응팀)	- 개인정보 보호책임자가 침해사고분석, 대응 및 복구에 필요한 관련자를 지정하여 소집 - 개인정보 보호전문가, 정보보안전문가 등 필요시 외부 전문가 등으로 구성 가능 - 해당기관 침해사고로 인하여 발생한 사고의 조사 및 복구
개인정보 보호담당자, 취급자	- 개인정보 침해사고를 접수하고 침해사고 대응절차를 개시 - 대내(부서·팀 내)·외 비상연락 및 절차별 업무추진 - 개인정보 침해기록을 관리하고 필요시 관련자 및 기관에 보고
전 직원(개인정보취급자)	- 모든 직원은 개인정보에 대한 침해사고가 발생한 것을 인지할 경우 개인정보보호 분야별 책임자를 경유하여 개인정보 보호담당자에게 신고

제38조(개인정보 유출신고)

① 개인정보처리자는 1명이라도 정보주체에 관한 개인정보가 유출된 경우에는 유출 내용 및 조치결과를 5일 이내에 개인정보 보호담당자 및 관할 주무부서에 보고하고, 1천명 이상 유출된 경우는 보호위원회 또는 한국인터넷진흥원에 신고하여야 한다.

② 제1항에 따른 보고 및 신고는 [별지 제5호] “개인정보 유출신고(보고)서” 를 통하여 하여야 하며, 신고시 전자우편, 팩스, 개인정보보호 종합지원포털(www.privacy.go.kr)에 접속하여 개인정보 유출신고 메뉴를 통하여 신고한다.

③ 유출 보고 또는 신고를 할 시간적 여유가 없거나 그 밖에 특별한 사정이 있는 경우, 전화로 사전 신고 후 [별지 제5호] “개인정보 유출신고(보고)서” 를 제출할 수 있다.

제38조의2(개인정보의 유출조사)

① 개인정보처리자는 개인정보 유출이 발생되었을 경우 유출 원인을 조사하고 다음 각 호 사항을 준수해야 한다.

1. 유출원인 보완 및 재발방지 조치계획 수립 · 이행
2. 개인정보취급자(전직원) 대상 사례 전파 및 재발방지 교육
3. 그 밖에 개인정보의 유출 방지를 위해 필요하다고 판단되는 사항

② 개인정보처리자는 개인정보 유출신고를 받고 필요하다고 판단되는 경우 관련 자료제출을 요구하거나 개인정보취급자 및 해당 유출원인과 관련한 관계인에 대해 조사를 실시하고 제36조제4항 각 호에 따른 사항을 요구할 수 있다. 해당 요구를 받은 개인정보 취급자 등은 특별한 사정이 없으면 이에 응하여야 한다.

③ 개인정보의 유출 조사를 위해서는 정보주체 및 유출사고 관련자의 사생활 침해를 최소화하는 방법(익명처리 등)으로 처리될 수 있도록 노력하여야 한다.

제39조(권익침해 구제방법)

① 개인정보주체는 개인정보침해로 인한 구제를 받기 위하여 개인정보 분쟁조정위원회, 한국인터넷진흥원 개인정보침해신고센터 등에 분쟁해결이나 상담 등을 신청한다.

이 밖에 기타 개인정보침해의 신고 및 상담에 대하여는 아래의 기관에 문의한다.

1. 개인정보 분쟁조정위원회 : 1833-6972(www.kopico.go.kr)

2. 개인정보 침해신고센터 : (국번없이) 118 (내선2번)(http://privacy.kisa.or.kr)

3. 대검찰청 사이버수사과 : (국번없이) 1301, privacy@spo.go.kr, (www.spo.go.kr)

4. 경찰청 사이버안전국 : (국번없이) 182, (cyberbureau.police.go.kr)

② 개인정보의 열람, 정정·삭제, 처리정지 등에 대한 정보주체의 요구에 대하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익을 침해 받은 자는 행정심판법이 정하는 바에 따라 행정심판을 청구할 수 있다.

1. 중앙행정심판위원회(www.simpan.go.kr)의 전화번호 안내 참조

부칙

1) 본 계획은 2026년 8월 1일부터 시행한다.

[별지 제1호]

개인정보([ ] 열람 [ ] 정정·삭제 [ ] 처리정지) 요구서

※ 아래 작성방법을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다. (앞 쪽)

접수번호	접수일	처리기간 10일 이내

정보주체	성 명	전 화 번 호
	생년월일	
	주 소	

대리인	성 명	전 화 번 호
	생년월일	정보주체와의 관계
	주 소	

요구내용	[ ] 열람	[ ] 개인정보의 항목 및 내용 [ ] 개인정보 수집·이용의 목적 [ ] 개인정보 보유 및 이용 기간 [ ] 개인정보의 제3자 제공 현황 [ ] 개인정보 처리에 동의한 사실 및 내용
	[ ] 정정·삭제	※ 정정·삭제하려는 개인정보의 항목과 그 사유를 적습니다.
	[ ] 처리정지	※ 개인정보의 처리정지를 원하는 대상·내용 및 그 사유를 적습니다.

「개인정보 보호법」 제35조 제1항·제2항, 제36조 제1항 또는 제37조 제1항과 같은 법 시행령 제41 조 제1항, 제43조 제1항 또는 제44조 제1항에 따라 위와 같이 요구합니다.

년 월 일

요구인 (서명 또는 인)

광주광역시교통문화연수원장 귀하

작 성 방 법

1. '대리인'란은 대리인이 요구인일 때에만 적습니다.
2. 개인정보의 열람을 요구하려는 경우에는 '열람' 란에 [√] 표시를 하고 열람하려는 사항을 선택하여 [√] 표시를 합니다. 표시를 하지 않은 경우에는 해당 항목의 열람을 요구하지 않은 것으로 처리됩니다.
3. 개인정보의 정정·삭제를 요구하려는 경우에는 '정정·삭제' 란에 [√] 표시를 하고 정정하거나 삭제하려는 개인정보의 항목과 그 사유를 적습니다.
4. 개인정보의 처리정지를 요구하려는 경우에는 '처리정지' 란에 [√] 표시를 하고 처리정지 요구의 대상·내용 및 그 사유를 적습니다.

[별지 2호]

위 임 장

위임받는 자	성명	전 화 번 호
	생년월일	정보주체와의 관계
	주소	
위임자	성명	전화번호
	생년월일	
	주소	

「개인정보 보호법」 제38조 제1항에 따라 위와 같이 개인정보 (□ 열람, □ 정정·삭제, □ 처리정지)의 요구를 위의 자에게 위임합니다.

년 월 일

위임자 (서명 또는 인)

광주광역시교통문화연수원장 귀하

[별지 제3호]

개인정보([ ] 열람 [ ] 일부열람 [ ] 열람연기 [ ] 열람거절) 통지서

(앞 쪽)

수신자 (우편번호: , 주소:)

요구 내용	

열람 일시		열람 장소	
통지 내용 ([ ] 열람 [ ] 일부열람 [ ] 열람연기 [ ] 열람거절)			
열람 형태 및 방법	열람 형태	[ ]열람·시청 [ ]사본·출력물 [ ]전자파일 [ ]복제물·인화물 [ ]기타	
	열람 방법	[ ]직접방문 [ ]우편 [ ]팩스 [ ]전자우편 [ ]기타	
납부 금액	①수수료 원	②우송료 원	계(①+②) 원
	수수료 산정 명세		

사 유	
이의제기방법	※ 개인정보처리자는 이의제기방법을 적습니다.

「개인정보 보호법」 제35조 제3항·제4항 또는 제5항과 같은 법 시행령 제41조 제4항 또는 제42조 제2 항에 따라 귀하의 개인정보 열람 요구에 대하여 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

[별지 제4호]

개인정보 ([ ]정정·삭제 [ ]처리정지) 요구에 대한 결과 통지서

수신자 (우편번호: , 주소:)

요구 내용	
□ 정정 · 삭제 □ 처리정지 조치 내용	
□ 정정 · 삭제 □ 처리정지 결정 사유	
이의제기방법	※ 개인정보처리자는 이의제기방법을 기재합니다.

「개인정보 보호법」 제36조 제6항 및 같은 법 시행령 제43조 제3항 또는 같은 법 제37조 제5항 및 같은 법 시행령 제44조제2항에 따라 귀하의 요구에 대한 결과를 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

유의사항

개인정보의 정정·삭제 또는 처리정지 요구에 대한 결정을 통지받은 경우에는 개인정보처리자가 '이의제기방법'란에 적은 방법으로 이의제기를 할 수 있습니다.

[별지 제5호]

개인정보 유출신고(보고)서

<table>
<tr><td>기관명</td><td colspan="5"></td></tr>
<tr><td>정보주체에의
통지 여부</td><td colspan="5"></td></tr>
<tr><td>유출된 개인정보의
항목 및 규모</td><td colspan="5"></td></tr>
<tr><td>유출된 시점과 그
경위</td><td colspan="5"></td></tr>
<tr><td>유출피해 최소화
대책·조치 및 결과</td><td colspan="5"></td></tr>
<tr><td>정보주체가 할 수
있는 피해 최소화
방법 및 구제절차</td><td colspan="5"></td></tr>
<tr><td rowspan="3">담당부서·담당자 및
연락처</td><td></td><td>성명</td><td>부서</td><td>직위</td><td>연락처</td></tr>
<tr><td>개인정보
보호책임자</td><td></td><td></td><td></td><td></td></tr>
<tr><td>개인정보
취급자</td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">유출신고(보고)
접수기관</td><td>기관명</td><td colspan="2">담당자명</td><td colspan="2">연락처</td></tr>
<tr><td></td><td colspan="2"></td><td colspan="2"></td></tr>
</table>

[별지 제6호]

개인정보파일 ([ ] 등록 [ ] 변경등록) 신청서

※ '변경정보 및 변경사유' 란은 변경등록시에만 작성합니다.

접수번호	접수일	처 리 기 7일간

공공기관 명칭	주소	등록부서	전화번호

등록항목	등록정보	변경정보 및 변경사유
개인정보파일 명칭		
개인정보파일의 운영 근거 및 목적		
개인정보파일에 기록되는 개인정보의 항목		
개인정보의 처리방법		
개인정보의 보유기간		
개인정보를 통상적 또는 반복적으로 제공하는 경우 그 제공받는 자		
개인정보파일을 운용하는 공공기관의 명칭		
개인정보파일로 보유하고 있는 개인정보의 정보주체 수		
해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서		
개인정보의 열람 요구를 접수·처리하는 부서		
개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유		

「개인정보 보호법」 제32조 제1항과 같은 법 시행령 제34조 제1항에 따라 위와 같이 개인정보파일 ([ ] 등록 [ ] 변경등록)을 신청합니다.

년 월 일

신청기관 (서명 또는 인)

광주광역시교통문화연수원장 귀하

[별지 제7호]

개인정보파일대장

기관 명칭	주소	등록부서	전화번호

등록항목	등록정보
① 개인정보파일 명칭	
② 개인정보파일의 운영 근거 및 목적	
③ 개인정보파일에 기록되는 개인 정보의 항목	
④ 개인정보의 처리방법	
⑤ 개인정보의 보유기간	
⑥ 개인정보를 통상적 또는 반복적으로 제공하는 경우 그 제공받는 자	
⑦ 개인정보파일을 운용하는 기관 의 명칭	
⑧ 개인정보파일로 보유하고 있는 개인정보의 정보주체 수	
⑨ 해당기관에서 개인정보 처리 관련업무를 담당하는 부서	
⑩ 개인정보의 열람 요구를 접수·처 리하는 부서	
⑪ 개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유	

[별지 제8호]

개인정보의 목적 외 이용 및 제3자 제공 대장

개인정보 또는 개인정보파일 명칭			
이용 또는 제공 구분	[ ] 목적 외 이용 [ ] 목적 외 제3자 제공		
목적 외 이용기관의 명칭(목적 외 이용의 경우)		담당자	소 속 성 명 전화번호
제공받는 기관의 명칭 (제3자 제공의 경우)		담당자	성 명 소 속 전화번호
이용하거나 제공한 날짜, 주기 또는 기간			
이용하거나 제공한 형태			
이용 또는 제공의 법적 근거			
이용 목적 또는 제공받는 목적			
이용하거나 제공한 개인정보의 항목			
「개인정보 보호법」제18조 제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용			

[별지 제9호]

개인정보파일 파기 요청서

작성일		작성자	
파기 대상 개인정보파일			
생성일자		개인정보취급자	
주요 대상업무		현재 보관건수	
파기 사유			
파기 일정			
특기사항			
파기 승인일		승인자 (개인정보 보호책임자)	
파기 장소			
파기 방법			
파기 수행자		입회자	
파기 확인 방법			
백업 조치 유무			
매체 파기 여부			

[별지 제10호]

개 인 정 보 보 호 서 약 서

본인은 광주광역시교통문화연수원 재직 중에 직무상 알게 된 개인정보를 다른 사람에게 누설하거나 직무상 목적 외의 용도로 이용하지 않겠으며, 개인정보 보호법을 준수하고 다음 사항에 해당하는 행위를 하지 않을 것을 서약합니다.

1. 법률상 규정이 있는 경우 등의 정당한 사유 없이 정보주체의 동의를 받지 않고 개인정보를 수집·이용·제공 하는 행위
2. 부정한 방법으로 개인정보를 취득하거나 처리에 관한 동의를 받는 행위
3. 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용 하도록 제공하는 행위
4. 정당한 권한 없이 또는 허용된 권한을 초과하여 개인정보를 무단으로 조회하거나, 훼손, 멸실, 변경, 위조 또는 유출하는 행위

2026년 8월 1일

서 약 자 소 속 광주광역시교통문화연수원

직 위(급) :

성 명: (서명)

[별지 제11호]

개인정보보호 내부관리계획 이행실태 점검 결과

○ 점검항목 : 개인정보의 안전성 확보조치기준 제4조

번호	점검항목	점검여부 (O, X)
1	개인정보 보호책임자의 지정에 관한 사항	O
2	개인정보 보호책임자 및 개인정보 취급자의 역할 및 책임에 관한 사항	O
3	개인정보 취급자에 대한 교육에 관한 사항	O
4	접근 권한의 관리에 관한 사항	O
5	접근 통제에 관한 사항	O
6	개인정보의 암호화 조치에 관한 사항	O
7	접속기록 보관 및 점검에 관한 사항	O
8	악성프로그램 등 방지에 관한 사항	O
9	물리적 안전조치에 관한 사항	O
10	개인정보 보호조직에 관한 구성 및 운영에 관한 사항	O
11	개인정보 유출사고 대응 계획 수립·시행에 관한 사항	O
12	그 밖에 개인정보 보호를 위하여 필요한 사항	O

◈ 관련 근거

※ 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립 · 시행)

① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다. (1번~12번 항목)

④ 개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리하여야 한다.

[개인정보보호법 시행령 제30조(개인정보의 안전성 확보 조치) 제3항 참고]