

1 개요

1 목 적

- 본 지침은 보건복지부 및 지자체, 영유아보육법에 따른 어린이집, 유관기관 등에서 보육통합정보시스템(이하 “시스템”이라 한다)을 구축·운영 또는 이용함에 있어 개인정보를 보호하는데 필요한 사항을 규정하여 아동·보육교직원 등의 권리를 보호하고자 함

2 적용 범위

- 본 지침은 시스템을 직접 또는 연계 활용하는 보건복지부와 지방자치단체, 어린이집, 유관기관(한국보육진흥원, 어린이집 안전공제회, 육아종합지원센터, 인구보건복지협회), 시스템을 개발·운영하는 한국사회보장정보원을 적용 대상으로 함
- 관련 법령 등에 따라 위 대상기관 사무의 일부 또는 전부를 위탁(대행)하여 운영하는 자는 위 대상기관의 종사자로 간주함

3 용어의 정의

- “**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 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.

- 다. 가목 또는 나목을 가명처리*함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 “가명정보”라 한다)

* “가명처리”란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

- “**개인정보의 처리**”란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
- “**정보주체**”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
- “**개인정보파일**”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
- “**개인정보수집**”이란 정보주체로부터 직접 이름, 주소, 전화번호 등의 정보를 제공받는 것 뿐 아니라 정보주체에 관한 모든 형태의 개인정보를 취득하는 것을 말한다.
- “**고유식별정보**”란 법령에 따라 개인을 고유하게 구별하기 위해 부여된 식별정보로서 주민등록번호, 외국인등록번호, 운전면허번호, 여권번호를 말한다.
- “**민감정보**”란 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활에 관한 정보, 유전자검사 등의 결과로 얻어진 유전정보, 「형의 실효 등에 관한 법률」 제 2조제5호에 따른 범죄경력 자료에 해당하는 정보, 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보, 인종이나 민족에 관한 정보 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보를 말한다.
- “**개인정보처리자**”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
- “**개인정보취급자**”란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖에 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자를 말한다.
- “**개인정보 유출**”이란 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용한 것을 말한다.

- “개인정보보호 통합관제”란 개인정보 유출 및 오·남용 방지를 위해 접속기록의 수집, 분석, 소명, 판정 등 일련의 관제활동을 말한다.
- “암호 키”란 정보의 비밀성을 보장하기 위해 암호알고리즘에 의하여 평문을 암호문으로 바꾸는 과정 또는 암호문을 평문으로 바꾸는 과정에서 사용되는 인증값을 말한다.
- “접속기록”이란 개인정보취급자 등이 시스템에 접속하여 수행한 업무내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다.
- “국가정보자원관리원”이란 중앙행정기관의 정보시스템과 국가정보통신망 등의 안정적인 운영, 효율적 통합·구축관리와 보호·보안 등에 관한 사항 등의 사무를 관장하는 데이터 센터를 말한다.

4 다른 지침과의 관계

- 시스템의 개인정보보호에 관한 사항은 다른 지침에 특별한 규정이 있는 경우를 제외하고는 본 지침에서 정하는 바에 따름
- 본 지침에 기술되지 않은 사항에 대하여는 「개인정보보호법」 등 관계 법령 및 개인정보보호위원회 「표준 개인정보 보호지침」, 보건복지부 「개인정보 보호지침」 등을 준용함

2 개인정보 보호 체계

1 관리적 보호체계

가. 개인정보보호 관리체계

- 개인정보보호 총괄책임관(이하 “총괄책임관”)의 지정 및 역할
 - － 총괄책임관은 시스템 운영부서의 장인 보건복지부 보육정책과장으로 함
 - － 총괄책임관은 시스템에 있는 개인정보파일의 안전성을 확보하기 위하여 다음의 업무를 수행함
 - 시스템 개인정보보호 지침 수립 시행
 - 개인정보보호체계 운용 및 관리·감독
 - 개인정보에 대한 안전한 관리 및 정기적인 영향평가(실태점검) 실시
 - 개인정보보호 통합관계 운영
 - 개인정보보호 교육 등 기타 개인정보보호를 위하여 필요한 업무
 - － 총괄책임관은 개인정보보호 업무의 일부를 한국사회보장정보원에 위탁 가능함
- 개인정보보호 책임관(이하 “책임관”)의 지정 및 역할
 - － 책임관은 시스템을 위탁받아 운영 중인 한국사회보장정보원의 보육통합정보시스템 운영 본부장으로 함
 - － 책임관은 총괄책임관으로부터 다음의 업무를 위탁받아 수행
 - 개인정보보호법에 따른 관리적·물리적·기술적 보호장치 마련 및 적용
 - 시스템 개인정보보호 실태에 대한 정기적 점검
 - 시스템 접근권한 통제·관리 및 주기적 모니터링 실행
 - 개인정보에 대한 안전한 관리 및 파기
 - 홈페이지 개인정보 노출점검 및 노출 유형에 따른 기술적 조치사항 적용
 - 개인정보보호 통합관계 운영지원(로그관리, 개인정보취급자 관리·지원 등 포함)
 - 기타 총괄책임관으로부터 위탁받은 개인정보보호 업무
- 개인정보보호 개별책임관(이하 “개별책임관”)의 지정 및 역할
 - － 개별책임관은 각 지자체의 보육주무부서의 장 및 유관기관의 개인정보보호 책임자로 함
 - 보육주무부서의 장은 각 지자체 및 소관 어린이집까지 해당 기관으로 봄
 - － 개별책임관은 다음의 업무를 수행

- 해당 기관의 개인정보보호에 관한 실무 및 시스템 접근권한 등을 관리하는 개인정보보호 담당자(또는 권한 관리 담당자)를 지정·운영하여 개인정보관리 실태 감독
- 개인정보보호 담당자는 개인정보취급자의 접근권한을 통제·관리하고(사용자 승인·탈퇴 및 보안서약서 징구 등), 단말기 설정 등 제반 보호정책의 실행을 확인·감독
- 개인정보 통합관계 관련 개인정보보호 위반실태 파악 및 확인, 위반자에 대한 징계조치 등 수행
- 개별책임관은 해당 기관의 시스템 사용자를 대상으로 개인정보보호 교육 추진
- 개인정보보호 취급자(시스템 사용자)의 역할
 - 개별책임관의 지휘·감독 하에 개인정보를 안전하게 처리해야 하며, 권한 없이 개인정보를 처리하거나 접근 권한을 임의 양도 또는 대여 불가
 - 업무 이외 목적으로 처리(단순조회 포함)하거나, 직무상 알게 된 개인정보를 타인에게 누설 또는 제공하지 않도록 안전하게 취급
 - 개인정보보호 실태파악 및 확인업무(위반사항에 대한 소명 요구 포함)에 대하여 성실히 대응해야 함

나. 접근권한의 관리

- 시스템에 대한 접근권한은 업무 수행에 필요한 최소한의 범위로 담당자에 차등 부여하며, 전보 또는 퇴직 등 인사이동 발생 시 지체 없이 접근권한을 변경 또는 삭제하고 해당내역을 3년 이상 보관 해야함
- 책임관은 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리 계획의 이행 실태를 연1회 이상으로 점검·관리해야 함
- 시스템 접속기록은 1년 이상 보관·관리해야 하며, 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 경우에는 2년 이상 보관·관리해야 함
- 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위해 시스템의 접속기록을 월 1회 이상 점검하여야 하며 특히 개인정보를 다운로드 한 것이 발견될 경우 내부관리 계획으로 정하는 바에 따라 그 사유를 반드시 확인해야 함

업무처리자	접근권한 승인절차
시·도 관리자 시·군·구 관리자	보건복지부 관리자로부터 승인을 받아 업무처리
시·도 담당자 시·군·구 담당자	시·도 및 시·군·구의 관리자로부터 승인을 받아 업무처리
어린이집 원장, 보육교직원	시·군·구 관리자로부터 원장업무 승인을 받은 원장이 해당 어린이집 내 사용자를 승인하여 업무 처리
유관기관 담당자	사회보장정보원 관리자로부터 승인을 받아 업무처리

* 사용자 가입 및 승인·탈퇴 등 권한부여 기준 절차는 “부록 12. 보육통합정보시스템 사용자 관리 지침”에 따름

- 책임관 및 별책책임관은 주기적으로 사용자 계정 이용현황을 점검하여 비정상적인 사용자가 발생하지 않도록 관리하고, 1개월 이상 시스템 장기 미사용자는 권한을 자동 회수 처리해야 함

다. 개인정보보호 교육

- 책임관 및 개별책임관은 개인정보취급자 및 업무 관계자 등을 대상으로 개인정보 보호 정책 전달 및 인식제고를 위한 교육계획을 수립·시행해야 함
 - － 교육계획에는 교육대상, 목적, 교육내용, 일정 및 방법 등 구체적으로 명시
 - － 교육은 개인정보취급자의 특성을 고려하여 집합·사이버교육, 워크숍 등 다양한 방식으로 실시해야 하며, 수시 또는 정기적(최소 년 1회)으로 개인정보보호 및 보안 교육 실시
- 개별책임관은 해당 기관의 신규채용, 전입 및 퇴직자에 대하여 별도의 개인정보보호 및 보안 교육을 실시해야 함

2 기술적 보호체계

- 응용 프로그램 및 연계 보안
 - － 웹 어플리케이션 개발 시 OWASP Top10 보안취약점(www.owasp.org) 및 국가정보원 국가사이버안전센터(NCSC)의 8대 웹 취약점에서 언급된 주요 항목에 대해 개발단계에서 보안사항을 고려하여 개발하고, 연 1회 이상 취약점 점검과 업데이트를 수행

- 연계서버는 물리적으로 분리하고, 외부 연계기관과 자료 송수신을 하는 경우 행정전자서명표준보안 API 적용을 통해 데이터를 암호화하여 송수신
- 네트워크 보안
 - 시스템은 국가정보자원관리원 내 설치하고 외부 인터넷망과는 물리적으로 분리하여 외부의 정보접근을 원천적으로 차단
 - 개인정보취급자 PC와 웹서버간 SSL 인증서 또는 응용프로그램을 통하여 암호화 조치하여 개인정보 수집·처리시 안전성 확보
 - 보육료 결제 등 금융기관과 정보연계를 위해 VPN을 설치하여 네트워크 보안 조치
- 사용자 PC 보안
 - 키보드 해킹방지를 도입하여 사용자가 키보드로 입력한 정보를 보호하고, 해킹 툴 및 시스템 바이러스 등에 의한 개인정보 유출 방지
 - 화면캡처 방지를 도입하여 웹 브라우저를 통해 표현되는 개인정보 유출방지
 - 개인정보취급자는 주기적으로 PC 내 개인정보 저장여부를 점검하여, 불필요한 개인정보는 즉시 삭제하거나 필요한 경우 암호화하여 저장
- 서버 및 데이터 접근 통제
 - **(사용자 인증)** 아이디/패스워드 및 인증서 방식의 2중 체계로 인증
 - 아이디/패스워드방식의 경우 비밀번호 유효기한 설정, 동일 비밀번호 재이용 제한, 비밀번호 9자리이상(문자·숫자·특수문자를 포함) 등 적용
 - 보육료 결제 등은 공동인증서 방식의 강화된 보안체계 적용
 - 특히, 아이사랑보육포털을 통한 개인정보 수집 시에는 암호화 및 전자서명 기술(GPKI, NPKI, I-PIN 등) 등을 활용하여 개인정보 수집 최소화
 - 대량의 개인정보 또는 민감한 개인정보를 취급하는 자에 대해서도 공동인증서 (GPKI, NPKI 등) 등의 안전한 방식으로 인증
 - 일정 횟수 이상의 입력오류가 발생할 경우, 경고 메시지와 함께 추가적인 접속 시도를 제한할 수 있는 보호조치
 - **(접근권한)** 시스템·DB 접근권한을 최소화하여 사용자 및 그룹별로 구분 관리하고, 사용자 접속 정보 등을 관리하여 권한 없는 자의 접근 통제
 - * 개인정보파일 명칭, 접근 데이터 항목, 접근일시, 접근주체 및 해당 IP 등 이력 관리
 - **(접근통제)** 시스템의 불법적인 접근 및 침해사고 방지를 위해 개인정보취급자가 일정시간 이상 업무처리를 하지 않을 경우 자동으로 시스템 접속이 차단되도록 보호 조치
 - **(네트워크)** 외부 공격으로부터 내부 네트워크를 보호하기 위한 보안시스템을 설치

운영하거나 물리적인 네트워크 분리

- 허가되지 않은 불법 인터넷사이트 및 P2P, 메신저, 웹하드, FTP 파일 송수신, Telnet, 공유폴더 등 내부정보 유출 매체가 되는 인터넷서비스의 이용 통제
- 시스템 개발 및 운영부서(한국사회보장정보원, 용역업체 포함)는 시스템 관리 PC를 인터넷망과 물리적으로 분리하여 운영

* 침입차단시스템(Firewall), 침입탐지시스템(IDS), 침입방지시스템(IPS), 위협관리시스템(TMS) 등 정부통합 전산센터 장비 활용

○ Data 보안

- 개인정보 중 중요정보(고유식별번호, 민감정보, 비밀번호 등)의 경우 시스템 부하를 최소화하는 범위 내에서 DB 암호화 조치
 - 비밀번호는 정보식별이 불가하도록 일방향 암호화하여 피해 최소화
 - 데이터 또는 DB는 비인가 접근 및 의도적 변경·파괴로부터 보호하기 위한 DB 보안 툴 적용
- 중요 개인정보에 대한 사용자 및 그룹별 접근권한을 최소화하고, 그에 따른 접근통제

○ 암호 키 관리

- (준비단계) 데이터를 암호화 할 경우 총괄책임관이 암호 키를 생성하여 분배하고 책임관이 시스템에 적용 후 별지 제8호 서식의 암호 키 관리대장에 기록
- (운영단계) 책임관은 비인가 된 사용자에게 의한 암호 키 사용이 불가하도록 강력한 접근통제를 시행하며 암호 키를 백업해야 하는 경우 운영데이터와 분리하여 보관
- (정지단계) 암호 키의 사용용도가 다하거나 사용기한이 지난경우 책임관은 암호 키가 사용 되지 않도록 조치
- (폐기단계) 책임관은 정지 후 6개월 경과된 암호 키를 삭제하며 별지 제8호 서식의 암호 키 관리대장에 기록

* 암호 키 관리 대상 : GPKI 인증서, SSL 인증서, DB암호화 키

3 물리적 보호체계

- 시스템이 설치된 전산실이나 개인정보파일을 보관하는 자료실에는 CCTV를 설치하거나 전자출입증 등의 출입통제장치를 설치하고, 출입내역을 기록·관리
- CD/USB 등 보조기억매체는 원칙적으로 사용 금지
 - 불가피한 경우 비밀번호 설정 또는 암호화 등의 보안 조치 후 저장하고 ‘보조기억매체 반출·입 대장’(별지 제1호 서식)에 기록 관리해야 함
- 책임관은 화재, 홍수, 단전 등의 재해·재난 발생 시 업무연속성 확보를 위해 위기 대응 매뉴얼을 수립
 - 책임관은 복구우선 순위, 복구방안, 업무분장 등을 구체적으로 명시하며 정적성과 실효성을 보장할 수 있도록 국가정보자원관리원과 협의하여 수립
 - 책임관은 위기대응매뉴얼을 매년 말 1회 점검하고 점검결과를 총괄책임관에게 보고

3 개인정보 처리기준

1 개인정보의 수집, 이용·제공, 파기

가. 개인정보의 수집

- 보육서비스제공을 위한 개인정보 수집 시, 수집 목적을 명확히 하고 목적에 필요한 최소한의 범위 안에서 적법하고 정당하게 수집해야 함
 - － 정보주체에게 수집목적, 항목, 보유 및 이용기간, 동의 거부권리 등을 고지하고 동의를 얻거나, 영유아보육관련 법령 등에 명시된 경우 수집 가능
 - * 정보주체의 동의를 얻을 경우, 정보주체에게 서면, 우편, 팩스, 유선, 인터넷, 이메일 등의 방법으로 내용고지 및 동의 확인 필요
- 수집한 개인정보파일은 운용을 시작한 날로부터 60일 이내에 “개인정보보호 포털(privacy.go.kr)”에 등록해야 함

나. 개인정보의 이용 및 제공

- 「영유아보육법」 시행령 제26조의3에서 정한 사무에 대해서는 아래 정보가 포함된 자료를 처리할 수 있음
 - － 주민등록번호, 여권번호, 외국인등록번호 등 고유식별정보 및 건강, 범죄경력 등 민감정보
- 시스템에서 보유하고 있는 개인정보는 보유목적 외의 용도로 이용하거나 제공이 원칙적으로 불가함. 다만, 다음의 경우는 예외로 함
 - － 정보주체로부터 별도 동의를 받은 경우
 - － 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
 - － 국회 또는 감사원 직무감찰 목적의 자료 요구 등 권한 있는 기관의 감사 또는 조사에 응해야 하는 경우
 - － 검찰청·경찰청의 범죄의 수사와 공소의 제기 및 유지에 필요한 경우
 - － 법원의 재판업무 수행에 필요한 경우
- 개인정보를 제공받아 이용하고자 하는 기관은 이용 목적 및 개인정보 항목, 이용기간 등을 명시하여 총괄책임관에게 문서로 요청
 - － 총괄책임관은 개인정보 제공여부와 이용기간 등을 결정·통보하고, 책임관은 이를

- ‘개인정보의 목적 외 이용 및 제3자 제공대장’(별지 제2호 서식)에 기록 관리
 - 개인정보를 제공받은 기관은 이용기간 만료 후 즉각 파기
- 책임관은 개인정보를 제공받은 기관에 대하여 사용목적 및 방법 등 필요한 사항에 대해 제한하거나 처리정보의 안전성 확보를 위하여 필요한 조치를 강구하도록 요청
 - 이를 이행하지 아니한 경우에는 즉시 정보 제공을 중지하고 제공된 정보에 대한 이용 중지 또는 파기 조치
- 정보통신망을 이용하여 개인정보를 제공하거나 제공받는 경우, 분실·도난·유출·변조, 훼손되지 않도록 기술적·관리적 및 물리적 조치를 취해야 함
- 외부저장매체(USB, CD 등)를 이용하여 제공하는 경우에는 문서파일 암호화 등 안전대책을 강구해야 함

다. 개인정보의 파기

- 보유 중인 개인정보에 대하여 다음과 같은 사유가 발생한 경우, 지체 없이 파기하고 그 내역을 ‘개인정보파일 파기 관리대장’(별지 제3호 서식)에 기록 관리해야 함
 - 정보주체가 자신의 개인정보에 대해 삭제를 요구하였을 경우
 - 개인정보파일의 목적이 달성되어 더 이상 보유가 불필요하게 된 경우
 - 개인정보파일의 지정된 보유기간이 경과하였을 경우
- 다만, 다음의 경우에는 파기 대상에서 제외 가능함
 - 보육료 및 보조금 등의 정산과 환수 등 사후 관리 대상자
 - 법적분쟁 관련 정보로서 필요한 경우
 - 총괄책임관에 승인을 얻어 시스템 운영에 필요하다고 인정되는 경우
- 개인정보파일을 파기할 때에는, 복구 또는 재생이 불가능하도록 파기
 - 개인정보가 포함된 출력물을 파기하는 경우에는 분쇄기나 소각기와 같은 장치를 이용하여 식별 불가능하도록 물리적으로 파기
 - 개인정보 저장매체를 파기하는 경우, 원상회복이 불가능한 방법으로 파기
- 책임관은 보유기간이 경과한 개인정보에 대해 최소 분기별로 파기하고, 파기로 인한 영향도를 최소화할 수 있도록 노력해야 함



■ 시스템 내 개인정보 파일의 보유기간 ■

개인정보파일명	주요 정보	보유기간
포털 회원정보	ID, 성명, 연락처 등	• 회원 탈퇴 시까지
보육료 결제정보	주민등록번호, 금융정보	• <u>퇴소(방과후 포함) 후 5년</u>
아동 정보	성명, 주민등록번호, 연락처, 보육료지원자격, 건강검진, 예방 접종 등	• <u>퇴소(방과후 포함) 후 5년</u>
보육교직원 정보*	ID, 성명, 연락처, 자격정보, 범죄경력**, 금융정보 등	• 준영구
입소대기 정보	출생순위, 보호자 성명, 연락처 등	• <u>퇴소 후 3년 또는 만 7세(장애아동은 만 13세)까지 (단, 입소대기 신청정보가 있을 경우 계속 보유)</u>
국민행복카드 신청·발급 정보	성명, 주민등록번호, 연락처, 금융정보 등	• (발급카드)최종 결제 후 5년
어린이집 정보공개 포털 정보수정 요청	성명, 연락처 등	• 민원 처리 종료 시 까지
어린이집 이용불편신고자 정보	이름, < <u>삭 제</u> > 연락처 등	• 민원 처리 종료 후 5년
상담 예약 신청 정보	성명, 연락처	• 예약 신청 후 1년
어린이집 · 위탁운영단체의 대표자 정보	성명, <u>주민등록번호</u> , 주소, 연락처, 법인·단체명	• 준영구

* 행정안전부 개인정보보호과-2511(2010. 9. 28.)에 의거, 보육교직원 정보(준영구) 및 영유아 정보(최종 퇴소후 5년)의 보유기간 적용

** 보육교직원의 범죄경력 정보는 조회후 5년 경과 시 파기하고 보건복지부 개인정보보호지침 제11조 3항 1호에 의거 관리

2 개인정보처리의 위탁

- ‘개인정보 처리 위·수탁’이란 개인정보처리자(위탁자)가 개인정보 수집·이용 등의 처리 자체를 제3자(수탁자)에게 위·수탁하거나, 개인정보의 이용·제공 등 처리가 수반되는 업무를 수탁자에게 위·수탁하는 것을 의미함
- 개인정보처리를 다른 기관에 위탁하는 경우, 수탁기관으로 하여금 다음의 사항을 준수하도록 해야 함
 - 개인정보에 관한 비밀유지 의무, 재 위탁 금지에 관한 사항, 위탁업체 직원에 대한 교육, 위탁기관에서 준수해야 할 의무를 위반한 경우 손해배상 등에 관한 사항 등
- 개인정보처리를 위탁하는 경우 “개인정보처리 위탁 계약서”를 작성하고, 다음 사항을 정기적으로 확인·점검해야 함
 - 개인정보의 목적 외 이용 여부
 - 개인정보 접근자에 대한 제한 및 이력관리 수행
 - 개인정보 취급 과정에서 발생한 출력물 관리
 - 개인정보에 대한 물리적인 안전성 확보 조치
 - 보유목적 달성 후 개인정보 파기 및 파기 이력관리 수행
 - 개인정보를 처리하는 업무 PC에 대한 안전성 확보 조치
 - 신규 개인정보취급자에 대한 교육 수행 및 보안서약서 징구 여부 등
- 위탁기관은 위탁하는 업무의 내용과 수탁자의 이름 등을 인터넷 홈페이지에 공개해야 함
- 개인정보처리 수탁기관은 개인정보 보호를 위하여 개인정보보호위원회 고시 “개인정보의 안전성 확보조치 기준”이 정하고 있는 기술적·물리적·관리적 조치를 해야 함
- 어린이집으로부터 회계업무 처리를 위탁받아 보육통합정보시스템 내 회계정보를 연계하고자 하는 수탁기관은 확약서(별지 제4호 서식)를 작성하여 책임관에게 제출해야 함
- 어린이집으로부터 회계업무 처리를 위탁받아 보육통합정보시스템 내 회계정보를 연계하고자 하는 수탁기관은 개인정보안전성 확보 조치 체크리스트(별지 제5호 서식)를 작성하여 보관하여야 하며 보육통합정보시스템 연계 승인기관이 확인·점검 할 수 있고 점검결과에 따라 시스템 연계 승인이 취소 될 수 있음

3 개인정보 유출 및 보호위반 조치

가. 개인정보 유출시 대응조치

- ‘개인정보의 유출’이란 다음의 어느 하나에 해당하는 경우를 말함
 - － 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
 - － 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근하여 개인정보를 유출한 경우
 - － 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 그 밖에 저장매체가 권한이 없는 자에게 잘못 전달된 경우
 - － 그 밖에 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우
- 개인정보처리자는 개인정보의 외부 유출 사실을 알았을 경우, 책임관 또는 개별책임관에게 즉시 보고하고, 해당 개인정보의 유출 피해 최소화 방안을 마련하여 지체 없이 해당 정보주체에게 다음의 사항을 알려야 함
 - － 유출된 개인정보의 항목, 유출시점과 경위, 유출로 인한 정보주체의 피해 최소화 방안, 대응조치 및 피해구제절차, 피해신고 접수부서 및 연락처 등
- 위 사항을 통지할 때에는 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 등 이와 유사한 방법을 통하여 지체없이 정보주체에게 알려야 함
- 개인정보처리자는 1천명 이상의 개인정보가 유출된 경우, 정보주체에 대한 통지 및 조치 결과를 5일 이내에 총괄책임관에게 보고하고, 개인정보보호위원회 또는 한국인터넷진흥원에 신고해야 함
 - － 또한, 인터넷 홈페이지에 정보주체에게 통지한 내용을 7일 이상 게재해야 함

나. 개인정보보호 위반자 조치

- 총괄책임관은 개인정보 유출 및 무단조화·열람, 관리소홀 등 개인정보보호 위반사항에 대해 해당 책임관 또는 개별책임관에게 징계 등의 조치를 요구할 수 있음
 - * 징계 세부 기준은 「개인정보보호법」, 「사회복지사업법」, 「영유아보육법」, 「국가공무원법」, 「공무원징계령」, 「보건복지부 감사규정」, 「지방공무원법」, 「지방공무원 징계 및 소청규정」 등 준용
- 개인정보보호 위반사항을 통보 받은 책임관 또는 개별책임관은 해당 개인정보취급자에 대해 1개월 이내에 징계 조치를 하고 그 결과를 총괄책임관에게 통보해야 함
- 총괄책임관은 징계조치 결과가 불충분하다고 판단될 경우, 재 징계를 권고할 수 있으며, 해당 책임관 또는 개별책임관은 1개월 이내에 그 결과를 총괄책임관에게 통보해야 함

4 개인정보보호 통합관제

1 통합관제 운영체계

- 시스템 접근기록(로그)을 분석하여 개인정보 유출 및 오·남용사고를 사전 예방하기 위함
 - － 보건복지부 통합관제센터를 통한 개인정보보호 위반 의심상황 모니터링, 의심사례에 대한 소명요청, 소명답변, 판정, 행정조치 및 결과등록 등
 - ※ (붙임 1) 개인정보보호 통합관제 업무 절차 참고

2 개인정보보호 위반여부 판정 및 행정조치

가. 개인정보보호 위반 의심자 모니터링

- 개인정보보호센터 담당자는 모니터링 절차에 따라, 책임관으로부터 제공받은 개인정보 접속로그 정보를 분석하여 개인정보 오·남용 의심자를 추출, 다시 책임관에게 제공

나. 소명요청 및 답변

- 책임관은 개인정보보호센터로부터 제공받은 개인정보 오·남용 의심사례에 대해 해당 개별책임관에게 소명 요청(별지 제6호 서식)하며 개별책임관은 개인정보 취급자를 조사할 수 있음
- 소명요청 받은 개별책임관 및 개인정보취급자는 10일 이내에 사실에 입각하여 성실히 소명답변(별지 제7호 서식)해야 함
 - － 책임관은 소명 답변의 내용이 충분하지 않거나 당초 소명요청 의도와 상이하다고 판단되는 경우, 추가 소명 또는 근거자료 제출 등을 요청할 수 있음
 - － 책임관은 소명 답변의 지연, 답변의 내용이 불충분한 경우에는 현장 점검을 통해 현황을 파악할 수 있으며, 이 경우 개별책임관 또는 개인정보취급자는 성실히 협조해야 함
 - ※ 소명요청 및 답변처리하는 보육통합정보시스템 내 개인정보 열람소명관리시스템을 통하여 전자적으로 처리

다. 위반여부 판정절차

- 책임관은 제출된 소명답변서를 참고하여 개인정보 오·남용 의심사례에 대한 위반 여부를 검토한 후 총괄책임관에게 보고
- 총괄책임관은 책임관이 제출한 검토결과를 참고하여 위반여부를 최종 판정하고, 위반사항 발견시 “개인정보보호 위반 징계 요구 세부기준”(붙임2)에 따라 책임관 또는 개별책임관에게 징계 조치를 요구할 수 있음
- 개인정보취급자는 총괄책임관의 판정결과에 대해 이의가 있는 경우, 관련 사항을 작성하여 재판정을 요청할 수 있음
 - － 총괄책임관은 관련 사항을 검토하여 그 결과를 통보해야 함

라. 행정조치

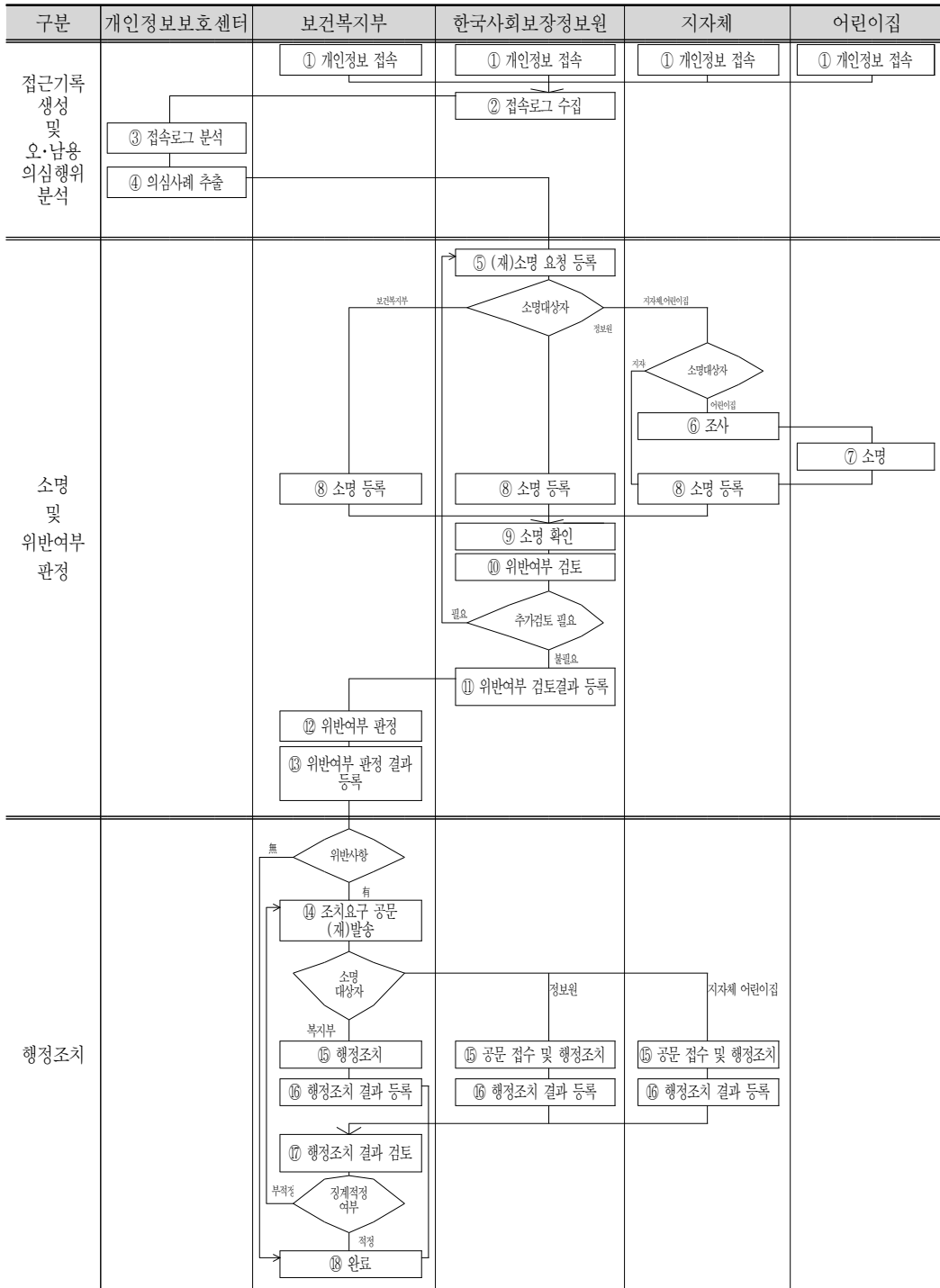
- 총괄책임관으로부터 징계 조치요구를 받은 책임관 또는 개별책임관은 1개월 이내에 해당 소명대상자를 징계 조치하고 그 결과를 총괄책임관에게 통보해야 함
- 징계 조치결과를 받은 총괄책임관은 법령의 적용 및 증거, 사실조사 결과에 비해 경미하게 처리되었다고 판단되는 경우, 책임관 또는 개별책임관에게 재 징계 조치를 요청할 수 있음

5 시행

- 이 지침은 통보한 날부터 시행함

[붙임 1]

개인정보 통합관제 업무 절차



[붙임 2]

개인정보보호 위반 징계 요구 세부기준

구분	종류	개인정보보호 위반 내용	법적근거
중징계	1. 파면-해임	개인정보 부정이용, 무단유출, 무단조회·열람 및관리소홀 중 비위의 정도가 심하고 고의성이 있는 경우	공무원 징계령 시행규 칙 제2조 준용
	2. 해임-강등	개인정보 부정이용, 무단유출 정도가 심하고 중과실이거나, 비위의 정도가 약하고 고의가 있는 경우	
	3. 강등-정직	개인정보 무단조회·열람 및 관리소홀 중 비위의 정도가 심하고 중과실이거나, 비위의 정도가 약하고 고의가 있는 경우	
	4. 정직	개인정보 부정이용 및 무단유출의 비위의 정도가 심하고 경과실이거나, 비위의 정도가 약하고 중과실인 경우	
경징계	5. 감봉	개인정보 무단조회·열람 및 관리소홀 중 비위의 정도가 심하고 경과실이거나, 비위의 정도가 약하고 중과실인 경우	
	6. 감봉-견책	개인정보 부정이용, 무단유출 중 비위의 정도가 약하고 경과실인 경우	
	7. 견책	개인정보 무단조회·열람 및 관리소홀 중 비위의 정도가 약하고 경과실인 경우	
기타 처분	8. 경고	개인정보 부정이용, 무단유출, 무단·조회열람 및 관리 소홀 중 위법 또는 부당한 행위라고 인정되나, 징계 또는 문책 사유에 이르지 아니하는 경미한 경우	기관 내 감사규 정
	9. 주의	개인정보 부정이용, 무단유출, 무단·조회열람 및 관리 소홀 중 위법 또는 부당한 행위라고 인정되나, 그 정도가 경고에 이르지 아니할 정도로 경미한 경우	
	10. 기관경고	개인정보가 유출되거나 무단 조회·열람이 발생되어 그 책임이 기관 전체에 귀속된다고 판단되는 경우	
고발	11. 고발	개인정보 보호와 관련된 법규의 위반에 따른 범죄 혐의가 있다고 인정되는 경우	개인정 보 보호법 제65조

[별지 제1호 서식]

보조기억매체(전산장비 포함) 반출·입 대장

<관리책임자: >

[illegible]

[별지 제2호 서식]

개인정보의 목적 외 이용 및 제3자 제공 대장

개인정보 또는 개인정보파일 명칭			
이용 또는 제공 구분	[] 목적 외 이용 [] 제3자 제공		
목적 외 이용기관의 명칭 (목적 외 이용의 경우)		담당자	소속
			성명
			전화번호
제공받는 기관의 명칭 (제3자 제공의 경우)		담당자	소속
			성명
			전화번호
이용하거나 제공한 날짜, 주기 또는 기간			
이용하거나 제공한 형태			
이용 또는 제공의 법적 근거			
이용 목적 또는 제공받는 목적			
이용하거나 제공한 개인정보의 항목			
「개인정보보호법」 제18조 5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청하는 경우에는 그 내용			

[별지 제3호 서식]

개인정보파일 파기 관리대장

[illegible]

[별지 제4호 서식]

확 약 서

000 회계업체는(는) 보육통합정보시스템과 어린이집 회계보고시스템간 회계업무 처리를 위한 시스템 연계시, 개인정보 취급에 대한 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본사는 어린이집으로부터 위탁받은 회계업무 처리를 위해, 계약기간 중은 물론 계약 종료 후에도 업무상 취득한 정보를 일체 누설하거나 개인의 영리목적 등 사적으로 이용하지 않을 것을 서약합니다.
2. 본사는 해당 어린이집과 회계처리 업무 위탁계약 종료시, 업무상 취득한 모든 정보를 삭제 조치하며, 복사본 등 관련 자료 일체를 보유하지 않을 것을 서약합니다.
3. 본사는 회계처리 업무를 위탁한 해당 어린이집과 개인정보보호법 제26조에 의거하여 ‘개인정보처리위탁 계약서’를 작성 날인하였음을 확인합니다.
4. 본사는 보육통합정보시스템과 어린이집 회계보고시스템간 연계시 ‘(붙임) 개인정보안전성 확보조치 체크리스트’등의 보안조치를 이행하였음을 확인합니다.
5. 본사는 위 사항을 위반하였을 시에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수할 것을 서약합니다.

년 월 일

업체명 :

직위 :

서약자(대표자) :

(서명 또는 인)

[별지 제5호 서식]

개인정보안전성 확보 조치 체크리스트

회계업체명		대 표 자	(서명 또는 인)
소 재 지		작 성 일 시	20 . .
구분	세부 내용		준수여부 (○, X)

<접근 권한의 관리 및 통제>

1	어린이집 회계처리 관련 업무 담당자에게 업무 수행에 필요한 최소한의 범위로 접근권한 차등 부여하고 담당자의 업무 변경 또는 퇴직시 접근권한 즉시 변경(말소) 및 그 기록을 3년간 보관	
2	회계처리시스템의 개인정보취급자 별로 사용자계정 발급(1인 1계정)	
3	회계처리시스템 이용시 사용자가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용	
4	개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 회계처리시스템, 업무용 컴퓨터 등에 조치	

<개인정보 암호화>

5	보육통합정보시스템과 회계처리시스템간 정보 연계시 구간 암호화	
6	로그인 비밀번호를 DB에 저장시 복호화되지 않도록 일방향 암호화하여 저장하며, 안전한 알고리즘으로 암호화	

<접속기록의 보관 등 기타>

7	접속 기록을 1년 이상 보관·관리하며 접속기록 등을 월 1회 이상 점검 접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관	
8	업무담당자 개인 pc에 개인정보 저장 불가 및 악성프로그램 등을 방지·치료할 수 있도록 보안 프로그램 설치·운영	
9	개인정보를 파기할 경우 복구 및 재생되지 않도록 파기하고 관리·감독	
10	개인정보의 안전한 처리를 위하여 '개인정보의 안전성 확보조치기준(개인정보보호위원회 고시 제2020-2호)' 제4조에 의거 내부관리계획 수립 및 시행	

* 동 붙임자료는 해당 회계업체에서 별도 보관

* 보육통합정보시스템 연계 승인기관은 필요시 위 항목들에 대한 준수여부를 확인·점검할 수 있으며, 점검결과에 따라 시스템 연계 승인이 취소될 수 있으니 참고하시기 바랍니다.

[별지 제6호 서식]

소명 요청서

구 분		내 용		
소명 요청 정보	관계대상 시스템	보육통합정보시스템		소명 순번
	소명기관 구분	<input checked="" type="checkbox"/> 개인정보보호센터 <input type="checkbox"/> 자체기관		
	소명요청일		답변 제출기한일	
	소명추출조건 및 요청사유			
	2차소명	요청일		
		답변제출기한일		
사유				
조회자 정보	이름		ID	
	소속지원명		IP	
	소속명		소속코드	
조회 내용	발생일시			
	고객명			
	생년월일			
	사용프로그램	프로그램ID	프로그램명	
비고				

[별지 제7호 서식]

소명 답변서

구 분		내 용		
소명 답변 내용	답변자		답변일	
	기 관		부 서	
	소명연기여부	<input type="checkbox"/> 정상 <input type="checkbox"/> 연기	소명연기 사유1)	
	답변내용	※ 개인정보 조회목적과 사유를 명확하고 상세하게 기록 합니다.		
	첨부자료	※ 필요시 근거 자료를 첨부 합니다.		
	답변지연사유	※ 답변제출기한일을 경과하여 답변시 입력합니다.		
2차 소명 답변 내용	답변자		답변일	
	기 관		부서	
	답변내용	※ 개인정보 조회목적과 사유를 명확하고 상세하게 기록 합니다.		
	첨부자료	※ 필요시 근거 자료를 첨부 합니다.		

[별지 제8호 서식]

암호 키 관리대장

일련 번호	일자		키 사용 용도	암호 키	담당자 서명	부서장 서명
	키 생성					
	키 폐기					
	키 생성					
	키 폐기					
	키 생성					
	키 폐기					
	키 생성					
	키 폐기					
	키 생성					
	키 폐기					
	키 생성					
	키 폐기					
	키 생성					
	키 폐기					
	키 생성					
	키 폐기					
	키 생성					
	키 폐기					
	키 생성					
	키 폐기					
	키 생성					
	키 폐기					

※ 응용 프로그램, 네트워크, 서버 보안을 위해 각 담당부서에서는 암호 키 관리 대장을 작성하여 보관