★선임주임	팀장	기획조정실장	경영전략본부장	
협 조				

문서번호	기획조정실-3466
보존기간	10년
결재일자	2016.05.23.
공개여부	공개

개인정보보호 내부관리계획

2016. 5

서울특별시 시설관리공단 | 기획조정실

목 차

제1장 총 칙

제1조(목적)

개인정보보호 내부관리계획(이하 '본 계획' 또는 '내부관리계획'이라 한다)은 개인정보보호법 제29조(안전조치의무) 내부관리계획의 수립 및 시행 의무에 따라 제정된 것으로 서울특별시시설관리공단(이하 '공단'이라 한다)이 취급하는 개인정보를 체계적으로 관리하여 개인정보가 분실, 도난, 누출, 변조, 훼손, 오·남용 등이 되지 아니하도록 함을 목적으로 한다.

제2조(적용범위)

본 계획은 홈페이지 등의 온라인을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 오프라인(서면, 전화, 팩스 등)을 통해 수집, 이용, 제공 또는 관리되는 개인정보에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부직원(계약직 등 비정규직 포함) 및 외부업체 직원에 대해 적용된다.

제3조(용어 정의)

1. "개인정보"라 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
2. "처리"란 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
3. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
5. "개인정보 보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자로서, 법 제31조에 따른 지위에 해당하는 자를 말한다.
6. "개인정보 보호담당자"란 개인정보책임자가 업무를 수행함에 있어 보조적인 역할을 하는 자를 말하며 개인정보보호 책임자가 일정 요건의 자격을 갖춘 이를 지정한다.
7. "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.
8. "개인정보처리시스템"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.

제2장 내부관리계획의 수립 및 시행

제4조(내부관리계획의 수립 및 승인)

① 개인정보 보호담당자는 공단의 개인정보보호를 위한 전반적인 사항을 포함하여 내부관리계획을 수립하여야 하며, 개인정보보호와 관련한 법령 및 관련 규정을 준수하도록 내부관리계획을 수립하여야 한다.

② 개인정보 보호책임자는 개인정보 보호담당자가 수립한 내부관리계획의 타당성을 검토하여 개인정보보호를 위한 내부관리계획을 승인하여야 한다.

③ 개인정보 보호담당자는 개인정보보호 관련 법령의 제·개정 사항 등을 반영하기 위하여 매년 11월말까지 내부관리계획의 타당성과 개정 필요성을 검토하여야 한다.

④ 개인정보 보호담당자는 모든 항목의 타당성을 검토한 후 개정할 필요가 있다고 판단되는 경우 12월말까지 내부관리계획의 개정안을 작성하여 개인정보 보호책임자에게 보고하고 개인정보 보호책임자의 승인을 받아야 한다.

제5조(내부관리계획의 공표)

① 개인정보보호책임자는 전조에 따라 승인한 내부관리계획을 매년 1월말까지 공단 내부 직원에게 공표한다.

② 내부관리계획은 내부직원(계약직 등 비정규직 포함), 외부업체 직원이 언제든지 열람할 수 있는 방법으로 비치하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제3장 개인정보보호책임자의 의무와 책임

제6조(개인정보보호책임자의 지정)

① 공단은 개인정보보호법 시행령 제32조 제2항 1호에 따라 해당하는 지위에 있는 자를 개인정보보호책임자로 임명한다.

1. 공단 개인정보 보호책임자 : 경영지원본부장
2. 분야별 보호책임자 : 개인정보 처리부서의 장

제7조(개인정보보호책임자의 의무와 책임)

① 개인정보보호책임자는 정보주체의 개인정보 보호를 위하여 다음 각 호의 업무를 수행한다.

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 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. 개인정보보호법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행

8. 개인정보 보호 관련 자료의 관리

9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

② 개인정보보호책임자는 업무를 수행함에 있어서 필요한 경우 개인정보 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.

③ 개인정보보호책임자는 개인정보 보호와 관련하여 이법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다.

제8조(개인정보취급자의 범위 및 의무와 책임)

① 개인정보취급자의 범위는 다음과 같다.

1. 공단 내에서 정보주체의 개인정보를 처리하는 업무를 수행하는 자를 말하며, 정규직 이외에 특정직, 임시직, 파견근로자, 시간제근로자 등이 포함될 수 있다.

② 개인정보취급자의 의무와 책임

1. 내부관리계획의 준수 및 이행

2. 개인정보의 기술적·관리적 보호조치 기준 이행

3. 업무상 알게 된 개인정보를 제3자에게 제공하지 않음

제4장 개인정보의 처리단계별 기술적 · 관리적 안전조치

제9조(개인정보취급자 접근권한 관리 및 인증)

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

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 하며, 또한 비밀유지의무 등에 대한 서약서를 받아야 한다.

③ 개인정보처리자는 제1항, 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

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

⑤ 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망 또는 전용선 등 안전한 접속수단을 적용하여야 한다.

제10조(비밀번호 관리)

① 개인정보처리자는 개인정보취급자 또는 정보주체가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자나 개인관련 정보를 패스워드로 이용하지 않도록 비밀번호 작성규칙을 수립하고, 이를 적용 및 운용하여야 한다.

② 개인정보처리자는 비밀번호에 적정한 기간의 유효기간(**100일**)을 설정하여야 한다.

③ 개인정보처리자는 다음의 비밀번호 설정을 반드시 해야한다.

- CMOS , 윈도우 , 화면보호기

제11조(접근통제)

① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한

2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

② 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용 컴퓨터에 조치를 취하여야 한다.

③ 개인정보처리자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하는 경우 반드시 인증을 받아야 접속가능 그렇지 않으면 접속제한 조치를 취하여야한다.

④ 별도의 개인정보처리시스템을 이용하지 않고 업무용 컴퓨터를 이용하여 개인정보를 처리하는 경우, 업무용 컴퓨터 기기의 운영체제 또는 보안프로그램 등에서 제공하는 접근통제 기능을 활용하여야 한다.

제12조(개인정보의 암호화)

① 개인정보처리자는 주민등록번호, 비밀번호, 바이오정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다. 단, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

② 개인정보처리자는 정보주체의 개인정보를 정보통신망을 통하여 송·수신하거나 보조저

장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 개인정보처리자 또는 개인정보취급자는 정보주체의 개인정보를 업무용 컴퓨터(PC)에 저장할 때에는 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장하여야 한다.

제13조(접속기록의 위·변조 방지)

① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관하여야 한다.

② 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제14조(보안프로그램 설치 및 운영)

① 개인정보처리자는 개인정보처리시스템 또는 업무용 컴퓨터에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 한다.

② 보안 프로그램은 항상 최신의 버전으로 업데이트를 해야 하며, 자동 업데이트 설정 기능을 사용하거나, 실시간 감지 기능을 반드시 적용하여야한다.(일 1회 이상 업데이트를 적용하여야 함)

③ 악성 프로그램관련 경보가 발령된 경우 또는 사용 중인 응용프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 적용하여야 한다.

제15조(물리적 접근제한)

① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 개인정보처리자는 물리적 접근방지를 위한 별도의 보호시설에 출입하거나 개인정보를 열람하는 경우, 그 출입자에 대한 출입사실 및 열람 내용에 관한 관리대장을 작성하도록 하여야 한다.

④ 개인정보처리자는 관리대장의 출입 및 열람 내용의 주기적 검토로 부적당한 출입자에 한 감시· 제재조치를 취할수 있다.

제5장 개인정보보호 교육

제16조(개인정보보호 교육 계획의 수립)

① 개인정보보호책임자는 다음 각 호의 사항을 포함하는 연간 개인정보보호 교육계획을 매년 2월말까지 수립한다.

1. 교육목적 및 대상, 내용

2. 교육 일정 및 방법

② 개인정보보호책임자는 수립한 개인정보보호 교육 계획을 실시한 이후에 교육의 성과와 개선 필요성을 검토하여 차년도 교육계획 수립에 반영하여야 한다.

제17조(개인정보보호 교육의 실시)

① 개인정보보호책임자는 정보주체정보보호에 대한 직원들의 인식제고를 위해 노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 직원을 대상으로 매년 정기적으로 연1회 이상의 개인정보보호 교육을 실시한다.

② 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시한다.

③ 개인정보보호에 대한 중요한 전파 사례가 있거나 개인정보보호 업무와 관련하여 변경된 사항이 있는 경우, 개인정보보호책임자는 부서 회의 등을 통해 수시 교육을 실시할 수 있다.

④ 추진 체계별 교육

1. 개인정보보호 책임자 / 담당자 교육

   1) 개인정보 책임자/담당자는 행정자치부 혹은 서울시에서 주관하는 개인정보보호 책임자/담당자 교육과 워크숍에 가급적 참석한다.

2. 개인정보처리자 교육

   1) 개인정보를 수집·운영하는 부서의 장은 개인정보취급자,개인정보위탁자에 대해 의무준수 사항을 주지시키고 자체적으로 개인정보보호 교육을 실시한다.

3. 개인정보수탁자 교육

   1) 위탁부서에서는 수탁자로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손 되지 않도록 교육을 실시한다.

제6장 개인정보 침해대응 및 피해구제

제18조(개인정보 유출 등의 통지)

① 개인정보보호책임자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 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 후 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. 공단의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 개인정보보호책임자는 개인정보가 유출된 경우 그 피해를 최소화하기 위하여 “침해사고 대응팀”을 구성하고 필요한 조치를 한다.

제19조(개인정보 유출 등의 신고)

개인정보보호책임자는 1만명 이상의 개인정보가 유출된 경우에는 본 계획 제18조에 따른 통지 및 조치 결과를 지체 없이 안전행정부장관 또는 전문기관(한국정보화진흥원, 한국인터넷진흥원)에 신고하여야 한다. 이 경우 안전행정부장관 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

제20조(권익침해 구제방법)

① 개인정보주체는 개인정보침해로 인한 구제를 받기 위하여 개인정보분쟁조정위원회, 한국인터넷진흥원 개인정보침해신고센터 등에 분쟁해결이나 상담 등을 신청한다.
이 밖에 기타 개인정보침해의 신고 및 상담에 대하여는 아래의 기관에 문의한다.

1. 개인정보분쟁조정위원회 : (국번없이)118
2. 대검찰청 사이버범죄수사단 : 02-3480-3571
3. 경찰청 사이버테러대응센터 : 02-1566-0112
4. 한국인터넷진흥원 개인정보침해신고센터 : http://privacy.kisa.or.kr