양천구시설관리공단
개인정보 내부 관리계획

2026. 10.

양천구시설관리공단

[제 · 개정 이력]

개정 번호	구분	시행일자	주 요 내 용	작성자
1	제정	2005. 2.	○ 개인정보보호방침(이사장 방침) 제정	송재성
2	일부개정	2011. 7.	○ 개인정보보호 기술적조치 추가 ○ 개인정보보호법 의무사항 반영	송재성
3	일부개정	2012. 4.	○ 행정안전부 공공기관 표준 개인정보처리방침 준용	송재성
4	제정	2013. 10.	○ 양천구시설관리공단 개인정보보호 내부관리계획 제정 - 개인정보보호법 제정에 따른 내부관리계획 작성	유경용
5	일부개정	2016. 6.	○ 개인정보보호 담당자 변경	최상곤
6	일부개정	2017. 1.	○ 개인정보보호 담당자 변경 ○ 공영 및 거주자주차 시스템 수탁자 변경	강현선
7	일부개정	2020. 4.	○ 개인정보 관리 조직의 역할 및 책임 구체화 - 부서별 담당자, 취급자 등 추가 ○ 개인정보 보호교육 내용 구체화 ○ 영상정보처리기기 관리사항 추가 ○ 개인정보의 기술적 보호조치 및 보안관리 추가	강현선
8	일부개정	2021. 6.	○ 가명처리 등의 방법과 절차 등 추가	강현선
9	일부개정	2023. 9.	○ 개인정보 보호책임자의 역할 수행 중 필수업무 추가	강현선
10	일부개정	2024. 7.	○ 공단 내부관리계획 표준 지침으로 수정 - 용어의 정의 추가, 개인정보보호 담당자 변경 등 ○ 개인정보 보호책임자의 역할 및 책임 수정 ○ 개인정보의 기술적 안전조치 내용 수정 - 개인정보 다운로드 항목, 취약점 점검 등 추가 ○ 개인영상정보처리에 관한사항 수정 ○ 그 밖의 개인정보보호조치 항목 추가	유경용
11	일부개정	2025. 5.	○ 내부관리계획의 수립·변경 및 승인 내용 수정 ○ 개인정보 관리조직 변경(신규사업장 추가 등) ○ 접근 통제 관련 항목 수정 ○ 개인정보의 암호화 관련 항목 수정 ○ 접속기록의 보관 및 점검 관련 항목 수정 ○ 재해·재난 대비 안전조치 관련 항목 수정	유경용

[제 · 개정 이력]

개정 번호	구분	시행일자	주 요 내 용	작성자
12	일부개정	2026. 6	○ 「개인정보의 안전성 확보조치 기준」(고시 제2025-9호) 반영 ○ 공단 내부관리계획 표준 지침으로 수정 - 용어의 정의 추가 , 내용 수정 등 ○ 적용 범위 이동형 영상정보처리기기 처리 개인영상정보 적용 대상 명시 ○ 분야별 책임자 업무에 이동형 영상정보처리기기 운영·관리 방침 수립 추가 ○ 개인정보보호협의회 구성·운영 추가 ○ 고정형·이동형 영상정보처리기기 관련 조항 분리 및 이동형 조항(제36조) 추가 ○ 조문 신설에 따른 조문 체계 현행화	한양규
13	일부개정	2026. 10.	○ 「연계정보 생성·처리 등에 관한 기준」 [별표4] 반영 ○ 연계정보 관련 용어 정의 및 적용 범위 신설 ○ 제10장 연계정보의 안전조치 신설(제42조~제48조) ○ 개인정보 침해 분류에 연계정보 추가, 자체점검 항목 추가 ○ 조문 신설에 따른 조문 체계 현행화	한양규

목 차

제1장 총 칙 1

제1조 목 적 1
제2조 용어 정의 1
제3조 적용 범위 5

제2장 내부관리계획의 수립·시행 및 점검 7

제4조 내부관리계획의 수립·변경 및 승인 7
제5조 내부관리계획의 공표 및 시행 7

제3장 개인정보 보호책임자 등 지정 및 업무 8

제6조 개인정보 보호조직의 구성 및 운영 8
제7조 개인정보 관리조직의 구성 9
제8조 개인정보보호 담당 분야별 업무와 역할 9
제9조 개인정보 보호책임자의 지정 10
제10조 개인정보 보호책임자의 역할 및 책임 11
제11조 개인정보 분야별 책임자 지정 및 업무 11
제12조 개인정보 취급자 지정 및 업무 12

제4장 개인정보 보호교육 13

제13조 개인정보 보호책임자의 교육 13
제14조 개인정보 취급자 관리·감독 13
제15조 개인정보 취급자의 교육 14

제5장 개인정보의 기술적 안전조치 15

제16조 접근 권한 관리 15
제17조 접근 통제 16
제18조 개인정보 암호화 18
제19조 접속기록 보관 및 점검 19
제20조 악성프로그램 등 방지 20
제21조 관리용 단말기의 안전조치 20
제22조 홈페이지 개인정보 노출방지 조치 21
제23조 취약점 점검 21

목 차

제6장 개인정보의 관리적 안전조치 ····· 22
제24조 개인정보보호협의회 구성·운영 ····· 22
제25조 개인정보 유출사고 대응 계획 수립·시행 ····· 22
제26조 위탁계약 및 위탁업무의 공개 ····· 24
제27조 수탁자에 대한 관리·감독 ····· 25
제28조 개인정보 위험도 분석 및 관리 ····· 25

제7장 개인정보의 물리적 안전조치 ····· 26
제29조 물리적 접근 제한 ····· 26
제30조 재해·재난 대비 안전조치 ····· 27
제31조 개인정보파일 등록 및 변경 ····· 27
제32조 개인정보의 파기 ····· 28
제33조 개인정보 처리실태 조사 ····· 29

제8장 영상정보처리기기 관리 계획 ····· 30
제34조 고정형 영상정보처리기기 설치 및 운영 ····· 30
제35조 고정형 영상정보처리기기 운영·관리 방침 수립 및 공개 ····· 31
제36조 이동형 영상정보처리기기 운영 ····· 31
제37조 개인영상정보의 보호 조치 ····· 32
제38조 목적 외 및 제3자 제공 ····· 33
제39조 보관 및 파기 ····· 33

제9장 가명정보 처리에 관한 사항 ····· 34
제40조 가명정보 처리 ····· 34
제41조 가명정보의 결합과 반출 등 ····· 34

제10장 연계정보의 안전조치 ····· 35
제42조 연계정보 보호책임자 지정 등 ····· 35
제43조 연계정보의 취급·관리 절차 ····· 35
제44조 주민등록번호와 연계정보의 분리 보관 ····· 36
제45조 연계정보의 안전한 저장·전송 ····· 36
제46조 연계정보 유출·도난 방지를 위한 취약점 점검 ····· 37
제47조 연계정보 침해사고 대응 ····· 37
제48조 연계정보 수집 현황의 기록·보관 및 실태점검 ····· 38

목 차

제11장 그 밖에 개인정보 보호를 위하여 필요한 사항 39
제49조 개인정보 보호 자체점검 주기 및 절차 39
제50조 자체점검 결과 관리 39
제51조 타 법령과의 관계 40

목 차

[붙 임]

[붙임 1] 수탁업체 교육자료 ····· 41
[붙임 2] 표준 개인정보처리위탁 계약서(안) ····· 42
[붙임 3] 보안서약서(대표자용) ····· 45
[붙임 4] 보안서약서(직원용) ····· 47
[붙임 5] 개인정보처리 업무위탁 시 점검사항 ····· 49
[붙임 6] 개인정보파일 보유기간 책정 기준표 ····· 50
[붙임 7] 개인정보파일 관리대장 ····· 51
[붙임 8] 개인정보파일 등록·변경 신청서 ····· 52
[붙임 9] 개인정보의 목적 외 이용 및 제3자 제공 대장 ····· 53
[붙임 10] 개인정보 파기요청서 ····· 54
[붙임 11] 개인정보파일 파기 관리대장 ····· 55
[붙임 12] 통제구역 출입자 명부 ····· 56
[붙임 13] 보조기억매체 반·출입 대장 ····· 57
[붙임 14] 개인영상정보 관리대장 ····· 58
[붙임 15] 개인영상정보 청구서 ····· 59
[붙임 16] 개인정보 열람/정정·삭제/처리정지 요구서 ····· 60
[붙임 17] 위임장 ····· 61
[붙임 18] 개인정보 열람/일부열람/열람연기/열람거절 통지서 ····· 62
[붙임 19] 개인정보 정정·삭제/처리정지 요구에 대한 결과 통지서 ·· 63
[붙임 20] 개인정보 유출신고서 ····· 64
[붙임 21] 개인정보 침해신고 처리대장 ····· 65
[붙임 22] 연계정보 수집 현황 기록대장 ····· 66
[붙임 23] 연계정보취급자 지정 현황 ····· 67

제 1 장 총 칙

제1조 목 적

① 양천구시설관리공단 개인정보 내부 관리계획은 「개인정보 보호법」 제29조와 같은 법 시행령 제16조제2항, 제30조 및 제30조2, 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2025-9호)에 따라 공단에서 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 사항을 정하는 것을 목적으로 한다.

제2조 용어 정의

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

1. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보로 다음과 같은 내용 등이 포함됨

▸ 개인정보 : 성명, 주소, 연락처, 소득, 학력, 성적, 직업, 전자우편, 영상, 통화내용, 신용, 부채, 인터넷 접속IP 등 객관적 사실에 관한 정보와 개인에 대한 제3자의 의견이나 평가 등 주관적 정보 포함
▸ 고유식별정보 : 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호
▸ 민감정보 : 사상, 신념, 노동조합, 정당의 가입·탈퇴, 정치적 견해, 건강, 유전정보 등

2. 단일 정보만으로 특정개인을 알아볼 수 없더라도, 다른 정보와 결합하여 개인을 알아볼 수 있다면 개인정보에 포함

② "**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.

③ "**가명처리**"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가정보가 없이는 특정 개인을 알아볼 수

없도록 처리하는 것을 말한다.

④ "**추가정보**"란 개인정보의 전부 또는 일부를 대체하는 데 이용된 수단이나 방식(알고리즘 등), 가명정보와의 비교·대조 등을 통해 삭제 또는 대체된 개인정보 부분을 복원할 수 있는 정보를 말한다.

⑤ "**익명정보**"란 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보를 말한다.

⑥ "**정보주체**"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

⑦ "**개인정보파일**"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

⑧ "**개인정보처리자**"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

⑨ "**개인정보 보호책임자**"란 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.

⑩ "**개인정보 보호 분야별 책임자**"(이하 "분야별 책임자"라 한다)란 업무를 위하여 개인정보를 처리하는 부서의 장(팀·관장)을 말한다.

⑪ "**개인정보 보호담당자**"란 개인정보 보호책임자를 보좌하여 개인정보 보호업무에 대한 실무를 담당하는 자로서 개인정보처리자가 지정한 자를 말한다.

⑫ "**개인정보취급자**"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 직원, 파견근로자, 시간제근로자 등을 말한다.

⑬ **"가명정보처리자"**란 업무를 목적으로 개인정보를 가명처리하여 활용 또는 제공하는 공공기관, 법인, 단체 및 개인 등을 말한다.

⑭ "**가명정보취급자**"란 가명정보를 처리하는 가명정보처리자의

지휘·감독을 받아 가명정보를 처리하는 업무담당자를 말한다.

⑮ “**재식별**”이란 추가정보 또는 행위자가 달리 보유하고 있는 다른 정보나 공개된 정보와의 결합 또는 대조·비교 등을 통해 특정 개인을 알게 되거나, 알아보려 하는 상태 또는 행위를 말한다.

⑯ “**정보통신망**”이란「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조제1항제1호의「전기통신사업법」제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.

⑰ “**개인정보처리시스템**”이란 데이터베이스 시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.

⑱ “**비밀번호**”란 정보주체 및 개인정보취급자 등이 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 인증할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

⑲ “**접속기록**”이란 개인정보처리시스템에 접속하는 자가 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.

⑳ “**고유식별정보**”란 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 주민등록번호, 여권번호, 운전면허의 면허번호, 외국인등록번호를 말한다.

㉑ “**민감정보**”란 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 유전자검사 등의 결과로 얻어진 유전정보, 범죄경력자료, 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정

개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보, 인종이나 민족에 관한 정보를 말한다.

㉒ "**생체정보**"란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징(연령·성별·감정 등)을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보를 말한다.

㉓ "**생체인식정보**"란 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.

㉔ "**인증정보**"란 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속을 요청하는 자의 신원을 검증하는데 사용되는 정보를 말한다.

㉕ "**P2P(Peer to Peer)**"란 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.

㉖ "**공유설정**"이란 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것을 말한다.

㉗ "**보조저장매체**"란 이동형 하드디스크(HDD), 유에스비(USB)메모리 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 쉽게 연결·분리할 수 있는 저장 매체를 말한다.

㉘ "**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.

㉙ "**모바일 기기**"란 무선망을 이용할 수 있는 스마트폰, 태블릿 컴퓨터 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.

㉚ "**내부망**"이란 인터넷망 차단, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

㉛ "**관리용 단말기**"란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 접속하는 단말기를 말한다.

㉜ "**고정형 영상정보처리기기**"란 일정한 공간에 설치되어 지속적 또는 주기적으로 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을

통하여 전송하는 장치로서 영 제3조제1항에 따른 폐쇄회로 텔레비전(CCTV) 및 네트워크 카메라를 말한다.

㉝ "**이동형 영상정보처리기기**"란 사람이 신체에 착용 또는 휴대하거나 이동 가능한 물체에 부착 또는 거치(据置)하여 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 영 제3조제2항에 따른 착용형, 휴대형, 부착·거치형 장치를 말한다.

㉞ "**개인영상정보**"란 법 제2조제1호에 따른 개인정보 중 영상정보처리기기에 의하여 촬영 · 처리되는 영상 형태의 개인정보를 말한다.

㉟ "**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 제26조제2항에 따른 수탁자는 제외한다.

㊱ "**연계정보**"란 본인확인기관이 서비스 연계를 위하여 이용자의 주민등록번호를 비가역적으로 암호화하여 생성한 정보(CI : Connecting Information)를 말하며, 공단은 연계정보를 개인정보에 포함하여 관리한다.

㊲ "**본인확인기관**"이란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정보통신망법"이라 한다) 제23조의3에 따라 본인확인기관으로 지정받은 자를 말한다.

㊳ "**연계정보 처리시스템**"이란 본인확인기관으로부터 연계정보를 제공받아 처리하는 홈페이지 회원가입 본인인증 연동 기능 등 정보시스템을 말한다.

㊴ "**연계정보취급자**"란 연계정보 처리시스템의 운영·관리 업무를 수행하는 개인정보취급자(수탁자의 직원을 포함한다)를 말한다.

제3조 적용 범위

① 본 계획은 공단에서 전자적 처리를 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 서면 등 전자적 처리 이외의 수단을 통해서 수집,

이용, 제공 또는 관리되는 개인정보와 공개된 장소에 설치·운영하는 고정형 영상정보처리기기 및 업무 목적으로 운영하는 이동형 영상정보처리기기를 통하여 처리되는 개인영상정보에 대해서도 적용되며, 개인정보를 처리하거나 개인정보 처리 업무를 위탁받아 처리하는 수탁자에게도 본 개인정보 내부관리 계획이 적용된다.

② 본 계획은 공단이 본인확인기관으로부터 제공받아 처리하는 연계정보에 대해서도 적용한다.

제 2장 내부 관리계획의 수립·시행 및 점검

제4조 내부 관리계획의 수립·변경 및 승인

① 개인정보 보호책임자는 공단에서 처리하는 개인정보 및 영상정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 내부관리계획을 수립 또는 개정하여야 하며, 영상정보 담당자는 필요한 경우 개인정보처리시스템 또는 영상정보처리기기별로 자체 실정에 맞게 내부관리계획을 수립하여 시행하여야 한다. 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있다.

② 개인정보보호 담당자는 개인정보보호 관련 법령의 제·개정 사항 반영 등 내부 관리계획에 중요한 변경이 있을 경우 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

③ 개인정보 보호담당자는 내부관리계획의 타당성과 개정 필요성을 검토하고 개정이 필요할 경우, 개정안을 작성하여 개인정보 보호책임자에게 보고하고 승인을 받아야 한다.

④ 개인정보 보호책임자는 내부 관리계획의 이행실태를 연 1회 이상 점검·관리 하여야 한다.

⑤ 개인정보처리자는 내부 관리계획의 세부 이행을 위한 각종 지침 등을 마련하여 시행할 수 있다.

제5조 내부 관리계획의 공표 및 시행

① 개인정보 보호책임자는 내부 관리계획을 승인한 후 전 직원에게 공표하고, 언제든지 열람 할 수 있는 방법으로 비치하여 전 직원이 이를 준수할 수 있도록 하여야 한다.

② 내부관리계획은 각 부서에 공문으로 발송하여 전 직원들이 공람할 수 있도록 하고, 사내·외부에 고시한다. 변경사항이 있는 경우에는 이를

공지하여야 한다.

③ 동 계획에 명시되지 않은 사항은 아래 관련 법규에 따른다.

<개인정보보호 관련 법규>

1. 개인정보 보호법, 같은 법 시행령
2. 개인정보 처리 방법에 관한 고시
3. 표준 개인정보 보호지침
4. 개인정보의 안전성 확보조치 기준
5. 개인정보 영향평가에 관한 고시
6. 양천구시설관리공단 개인정보보호 업무지침
7. 그 밖의 관계 법규

제 3 장 개인정보 보호책임자 등 지정 및 업무

제6조 개인정보 보호조직의 구성 및 운영

① 개인정보 보호책임자는 개인정보의 안전한 처리를 위하여 다음 각 호의 사항을 포함하는 개인정보 보호조직을 구성하고 운영하여야 한다.

1. 개인정보 보호책임자의 지정
2. 개인정보 보호책임자의 지휘 · 감독 하에 개인정보 보호책임자의 업무를 지원하는 담당자의 지정
3. 개인정보를 처리하는 개인정보취급부서의 지정

② 개인정보 보호조직의 설치, 변경 및 폐지는 이사장(본부장)으로부터 승인을 받아 정한다.

③ 개인정보취급부서에서는 개인정보 보호조직과 충분히 협의, 조정 하여 개인정보를 처리하여야 한다.

④ 개인정보 보호조직은 제7조에 따른 업무를 수행하여야 하며, 그 밖에 개인정보의 안전성 확보를 위하여 개인정보 보호책임자가 필 요하다고 판단되는 사항을 수행할 수 있다.

제7조 개인정보 관리조직의 구성



제8조 개인정보보호 담당 분야별 업무와 역할

직책	역할 및 책임	담당자
개인정보 보호책임자 (CPO)	<개인정보관리 분야> • 개인정보보호 내부관리계획의 수립 및 시행 • 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 • 개인정보 처리와 관련한 불만의 처리 및 피해 구제 • 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축 • 개인정보보호 교육 계획의 수립 및 시행 • 개인정보 침해사고 예방, 처리 및 재발 방지 관리 총괄 • 개인정보파일의 보호 및 관리·감독 등 <영상정보처리기기 관리 분야> • 영상정보처리기기 관련 개인정보보호 총괄 • 개인영상정보 이용·제공 총괄 관리 • 영상정보처리기기 위탁업체 보안 총괄 관리 • 개인영상정보 안전성 확보 총괄 • 영상정보처리기기 운영·관리 방침 수립 총괄 • 영상정보처리기기 설치 현황 관리 총괄 등	본부장
개인정보보호 분야별 책임자	<개인정보관리 분야> • 부서별 개인정보파일 및 개인정보처리시스템에 대한 관리적·물리적·기술적 안전성 확보 • 개인정보 취급자에 대한 교육과 관리 감독 • 개인정보보호 업무 관련 사항 CPO에게 수시 보고 • 처리정보 취급내역에 대한 로그기록 의무화 • 해당 부서의 침해사고 발생에 대한 처리 및 관리 감독	팀·관장

	• 기타 소관 분야별 개인정보 보호를 위해 필요한 사항 등 <영상정보처리기기 관리 분야> • 당해 부서의 영상정보처리기기 설치·운영 • 영상정보처리기기 안전성 확보 조치 • 영상정보처리기기 및 화상정보 취급자에 대한 관리·감독 등	
개인정보 보호 담당자	<개인정보관리 및 영상정보처리기기 관리 분야> • 개인정보보호 계획 및 방침 운영 • 개인정보 침해 대응 • 개인정보처리 실태 관리 및 각종 자료 취합 • 개인정보보호 교육 관련 행정업무 • 개인정보보호 관련 각종 행정업무 • 개인정보 처리와 관련된 시스템 운영 감독 등 • 영상정보처리기기 관리 분야 전반 계획, 방침운영, 감독, 대응 등 각종 업무	성과팀 개인정보 담당자
전산실 정보보호담당자	<개인정보관리 분야> • 침입차단, 침입탐지, 방화벽 운영, 접속기록 관리 등 개인정보처리시스템 정보보호에 대한 물리적, 기술적, 관리적 전산실 보안관리 • 기타 전산실 및 개인정보처리시스템 정보보호관련 전반 업무	
부서별 개인정보 보호 담당자	<개인정보관리 및 영상정보처리기기 관리 분야> • 사업장별 개인정보보호 계획의 준수 및 이행 • 개인정보보호를 위한 기술적, 관리적, 물리적 보호조치 • 개인정보보호 관련 관련서식 및 대장 작성·유지 • 부서 내 열람청구, 정정·삭제, 처리정지 등 정보주체의 권리 보장 • 유효기간이 지난 파일의 삭제, 최소 정보 수집 및 동의 절차 수행 • 기타 팀 내 개인정보보호와 관련된 전반 업무 • CCTV 시스템의 안전성 확보 조치 이행 등	해당 부서 담당자
개인정보 취급자	<개인정보관리 분야> • 개인정보보호 활동 참여 • 개인정보보호 내부관리계획의 준수 및 이행 • 개인정보의 기술적·관리적 보호조치 기준 이행	업무직 수탁업체
부서별 영상정보처리기기 담당자	<영상정보처리기기 관리 분야> • CCTV시스템의 안전성 확보 조치 이행 등	해당부서 시설담당

제9조 개인정보 보호책임자의 지정

① 양천구시설관리공단의 본부장은「개인정보 보호법」제31조와 같은 법 시행령 제32조에 따라 개인정보 보호책임자(CPO : Chief Privacy Officer)로 지정하고 개인정보의 처리에 관한 업무를 총괄해서 책임진다.

제10조 개인정보 보호책임자의 역할 및 책임

① 개인정보 보호책임자는 다음 각 호의 임무를 수행하여야 한다.

1. 개인정보보호 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 오·남용 방지를 위한 내부통제 시스템의 구축
5. 개인정보보호 교육 계획의 수립과 시행
6. 개인정보파일의 보호 및 관리·감독
7. 「개인정보보호법」 제30조에 따른 개인정보 처리방침의 수립 ·변경 및 시행
8. 개인정보보호 관련 자료의 관리
9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기
10. 시행령 제14조의2 제1항 각 호의 고려사항에 대한 판단 기준에 따른 개인정보의 추가적인 이용 또는 제공 여부의 점검
11. 개인정보 보호지침 등의 제·개정
12. 영상정보처리기기 운영·관리 방침 수립·시행
13. 그 밖에 개인정보의 적절한 처리를 위한 업무

② 개인정보 보호책임자는 제1항의 업무를 수행하면서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사 하거나 관계 당사자로부터 보고를 받을 수 있다.

③ 개인정보 보호책임자는 담당자 및 취급자로부터 개인정보의 처리 현황과 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로 부터 보고 받을 수 있으며, 이를 수시로 관리·감독하여야 한다.

제11조 개인정보 분야별 책임자 지정 및 업무

① 개인정보 보호책임자를 지원하기 위하여 개인정보를 처리하는 부서의 장(팀·관장)을 분야별 책임자로 지정한다.

② 분야별 책임자가 결원, 출장, 사고, 그 밖의 사유로 그 직무를 수행할 수 없을 때에는 차하위자가 업무를 대행한다.

③ 분야별 책임자는 아래와 같은 업무를 수행한다.

1. 개인정보 수집, 이용·제공, 파기 등 전 단계에서의 안전성 확보 조치
2. 개인정보취급자 지정·관리·감독·교육
3. 개인정보파일의 지정·관리·보호·파기
4. 공개 대상 개인정보파일 등록·공개
5. 공개 대상 개인정보파일의 개인정보 처리방침의 수립·시행 및 공개
6. 고정형·이동형 영상정보처리기기 운영·관리 방침 수립·시행
7. 개인정보 보호 관련 자료 관리 및 제출
8. 개인정보 처리와 관련한 요구 처리 및 피해구제
9. 개인정보 유출 통지 및 피해 확산 방지
10. 개인정보처리 관련 개선 권고 및 시정 조치사항 이행
11. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 감독
12. 개인정보 보호책임자가 위임·요청한 개인정보 보호와 관련된 업무
13. 그 밖에 개인정보의 적절한 처리를 위해 필요한 사항

제12조 개인정보 취급자 지정 및 업무

① 개인정보취급자는 공단 주요 업무를 수행함에 있어 개인정보를 취급하는 담당자로 아래와 같은 임무를 수행한다.

1. 업무를 수행함에 있어 처리되는 개인정보에 대한 보호관리
(개인정보의 수집・보유・이용 및 제공・파기 단계에서의 관리)
2. 개인정보 보호법령 및 관련 규정의 준수
3. 내부 관리계획의 준수 및 이행
4. 개인정보의 안전성 확보조치 기준 이행
5. 소속 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검 등

② 개인영상정보취급자는 개인영상정보 보호와 관련하여 다음과 같은 역할 및 책임을 이행하여야 한다.

1. 개인영상정보 보호 활동 참여와 내부관리계획의 준수 및 이행
2. 개인영상정보의 보호조치 기준 이행
3. 직원 또는 제3자에 의한 위법・부당한 개인영상정보 침해행위에 대한 점검
4. 기타 개인영상정보 보호를 위해 필요한 사항의 이행

제 4 장 개인정보 보호교육

제13조 개인정보 보호책임자의 교육

① 개인정보 보호책임자는 대상별 개인정보보호 교육계획을 수립하여 연 1회 이상 전 직원을 대상으로 개인정보 보호 교육을 실시한 후 교육의 성과와 개선 필요성 등을 검토하여 다음 년도 교육계획 수립에 반영하여야 한다.

② 개인정보 보호책임자는 개인정보 취급 업무를 처음 시작하는 자에게 의무사항을 주지시키고, 수시 또는 정기적으로 보안교육을 실시하여야 한다.

③ 개인정보 보호책임자는 소관 개인정보의 처리업무를 위탁한 경우 수탁자의 개인정보취급자에 대한 개인정보 보호 교육 이행여부를 점검하여야 한다.

④ 교육 방법은 집합교육뿐만 아니라, 사이버 교육, 외부 전문기관이나 전문요원 위탁교육 등 다양한 방법으로 실시할 수 있다.

⑤ 구체적인 교육일정, 교육방법, 교육내용 등은 매년 수립하는 개인정보 보호 교육계획을 따른다.

제14조 개인정보 취급자 관리·감독

① 분야별 책임자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 개인정보취급자에 대하여 관리·감독하여야 한다.

② 분야별 책임자는 개인정보취급자를 업무상 필요한 한도 내에서 최소한으로 두어야 하며, 개인정보취급자의 개인정보 처리범위를 업무상 필요한 한도 내에서 최소한으로 제한하여야 한다.

③ 분야별 책임자는 개인정보처리시스템에 대한 접근권한을 해당 업무수행에 필요한 최소한의 범위로 업무담당자에게 차등 부여하고 접근권한 부여 이력을 기록·관리해야 한다.

④ 분야별 책임자는「개인정보 보안서약서」를 활용하여 개인정보 취급자에게 보안서약서를 제출하도록 하는 등 적절한 관리·감독을 해야하며, 인사

이동 등에 따라 개인정보취급자 또는 개인정보 취급자의 업무가 변경되는 경우에는 개인정보에 대한 접근권한을 지체없이 변경·말소하고 그 사항을 기록·관리하여야 한다.

⑤ 분야별 책임자는 각 개인정보처리시스템 별로 개인정보취급자의 접속기록을 보관·관리하고 점검하여야 한다.

⑥ 분야별 책임자는 그 외 안전성 확보에 필요한 사항을 이행하고 있는지 관리·감독하여야 한다.

제15조 개인정보 취급자의 교육

① 개인정보 보호책임자는 다음 각 호의 사항을 포함하여 정기적으로 교육을 실시하여야 한다.

1. 교육대상 : 개인정보 보호담당자, 개인정보 취급자 등
2. 교육내용 : 대상별로 차별화
   - 개인정보보호의 중요성
   - 기관의 개인정보보호 정책·지침 및 위험관리
   - 개인정보의 안전성 확보조치 기준 이행
   - 개인정보보호 업무의 절차 및 책임
   - 개인정보보호 유출사고 사례 및 대응절차 등
3. 교육 방법 : 사내교육(내·외부 강사활용), 외부교육, 위탁교육, 온라인교육 등

② 개인정보 보호책임자는 제4장에 따라 개인정보보호 교육을 실시한 결과 또는 이를 입증할 수 있는 관련 자료 등을 기록 · 보관하여야 한다.

③ 개인정보 보호책임자는 개인정보보호에 대한 중요한 전파 사례가 있거나 개인정보보호 업무와 관련하여 변경된 사항이 있는 경우 부서 회의 등을 통해 수시로 교육을 실시할 수 있다.

④ 개인정보 보호책임자는 내부관리계획에 따라 자체적인 교육을 실시할 수 있다.

제 5 장 개인정보의 기술적 안전조치

제16조 접근 권한 관리

① 개인정보 보호책임자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 차등 부여하여야 한다. 이 경우 접근 권한은 개인정보취급자뿐만 아니라 업무 수행을 위하여 개인정보처리시스템에 접근하는 자 전체를 대상으로 한다.

구분	역할 및 책임
접근권한 총책임자	- 개인정보보호 책임관(본부장) - 접근권한 관리 총괄
접근권한 관리자	- 혁신성과팀장 - 접근권한 부여·삭제·수정 등 권한 관리 - 접근권한 부여·삭제·수정 등 권한 설정에 대한 적절성 점검
접근권한 담당자	- 개인정보보호 총괄담당자 - 접근권한 부여·삭제·수정 등 권한 운영 수행 - 접근권한 부여·삭제·수정 등 권한 설정에 대한 적절성 점검 수행

② 개인정보 보호책임자는 개인정보취급자가 전보, 퇴직 등 인사이동으로 변경 되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 부여, 변경 또는 말소하여야 한다.

③ 개인정보 보호책임자는 제1항 내지 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 최소 3년간 보관하여야 한다.

④ 개인정보 보호책임자는 개인정보취급자별로 한 개의 사용자 계정을 발급하여야 하며, 다른 개인정보취급자와 공유하지 않도록 하여야 한다.

⑤ 개인정보 보호책임자는 개인정보처리시스템, 인터넷 홈페이지 등에 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 다음 각 호의 사항을 적용하여야 한다.

1. 사용자 계정(ID)과 동일하지 않은 비밀번호 설정 사용
2. 비밀번호 최소길이는 다음과 같이 적용

- 최소 10자리 : 영대문자, 영소문자, 숫자, 특수문자 중 2종류 이상으로 구성
- 최소 8자리 : 영대문자, 영소문자, 숫자, 특수문자 중 3종류 이상으로 구성

3. 개인의 신상 및 부서 명칭 등과 관계가 없는 비밀번호 설정 사용
4. 일반 사전에 등록된 단어 설정 금지
5. 동일 단어 또는 숫자 반복 설정 금지
6. 한 번 이상 사용한 비밀번호 재사용 금지
7. 비밀번호 공유 사용 금지
8. 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지
9. 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않음
10. 초기 할당된 임시 비밀번호는 로그인 후 즉시 변경 설정
11. 비밀번호에 유효기간을 설정하여 분기별 1회 이상 변경 설정

⑥ 개인정보 보호책임자는 정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접근할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하여야 한다.

제17조 접근 통제

① 개인정보 보호책임자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 안전조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 인터넷 프로토콜(IP) 주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 인터넷 프로토콜(IP) 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응

② 개인정보 보호책임자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 한다. 다만, 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우 가상사설망 등 안전한 접속수단 또는 안전한 인증수단을 적용할 수 있다.

③ 개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.

④ 고유식별정보를 처리하는 개인정보 보호책임자는 인터넷 홈페이지 를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연1회 이상 취 약점을 점검하고 필요할 경우 보완 조치하여야 한다.

⑤ 개인정보 보호책임자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무 처리를 하지 않는 경우에는 자동으로 접속이 차단되도록 하는 등 필요한 조치를 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 이용 할 수 있다.

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

제18조 개인정보의 암호화

① 개인정보처리자는 비밀번호, 생체인식정보 등 인증 정보를 저장 또는 정보통신망을 통하여 송·수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

② 개인정보 보호책임자는 다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

1. 주민등록번호
2. 여권번호
3. 운전면허번호
4. 외국인등록번호
5. 신용카드번호
6. 계좌번호
7. 생체인식정보

③ 개인정보 보호책임자는 이용자가 아닌 정보주체의 개인정보를 다음 각 호와 같이 저장하는 경우에는 암호화하여야 한다.

1. 인터넷망 구간 및 인터넷망 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우
2. 내부망에 고유식별정보를 저장하는 경우(다만, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.)

가. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과

나. 암호화 미적용시 위험도 분석에 따른 결과

④ 개인정보 보호책임자는 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다.

⑤ 개인정보처리자는 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

⑥ 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보 보호책임자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

⑦ 이메일을 통해 개인정보를 전송하는 경우 이메일 첨부 문서를 암호화하여 전송하여야 한다.

제19조 접속기록의 보관 및 점검

① 개인정보 보호책임자는 개인정보 취급자의 개인정보처리시스템에 대한 접속기록을 1년 이상 보관·관리하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 2년 이상 보관·관리하여야 한다.

1. 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우
2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우
3. 개인정보처리자로서 「전기통신사업법」제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우

② 개인정보 보호책임자는 개인정보의 분실・도난・유출・위조・변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히, 개인정보의 다운로드가 확인된 경우에는 내부 관리계획 등으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.

③ 개인정보 보호책임자는 개인정보취급자의 접속기록이 위・변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

기록 항목	주 요 내 용
식별자	개인정보시스템에서 접속자를 식별할 수 있도록 부여된 ID 등
접속일시	개인정보 처리 일시(접속한 시점 또는 업무를 수행한 시점)
접속지 정보	접속한 자의 PC 등 단말기 정보 또는 서버의 IP 주소 등 접속 주소
정보주체 정보	누구의 개인정보를 처리하였는지를 알 수 있는 식별정보(이름, ID 등)
수행업무	개인정보취급자가 개인정보처리시스템(회원관리, 주차관리 프로그램 등)을 이용하여 정보주체의 개인정보를 처리(생성, 수정, 삭제, 검색, 저장(다운로드), 출력 등)한 내용을 알 수 있는 정보

④ 분야별 책임자는 개인정보의 다운로드가 확인된 경우에는 다음의 기준 및 개인정보처리시스템 별 접근권한 관리정책 기준에 따라 그 사유를 반드시 확인하여 개인정보의 오·남용이나 유출을 목적으로 다운로드한 것이 확인되었다면 지체 없이 다운로드한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다.

1. 다운로드 정보주체의 수 제한
2. 일정기간 내 다운로드 횟수 제한
3. 업무시간 외 다운로드 수행 제한

제20조 악성프로그램 등 방지

① 개인정보 보호책임자 및 분야별 책임자는 개인정보처리시스템 또는 업무용 컴퓨터에 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램을 설치·운영하여야 하며, 다음의 사항을 준수하여야 한다.

1. 프로그램의 자동 업데이트 기능을 사용하거나, 정당한 사유가 없는 한 일 1회 이상 업데이트를 실시하는 등 최신의 상태로 유지
2. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

② 개인정보 보호책임자 및 분야별 책임자는 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 이에 따른 업데이트 등을 실시하여야 한다.

제21조 관리용 단말기의 안전조치

① 개인정보보호 분야별 책임자는 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

4. 개인정보보호 분야별 책임자는 개인정보가 포함된 정보를 출력 또는 복사할 경우에 개인정보 유출사고를 방지하기 위한 보호조치를 취하여야 한다.
5. 개인정보보호 분야별 책임자는 민감한 개인정보 또는 다량의 개인 정보가 포함된 정보를 출력하거나 복사할 경우 출력, 복사자의 성명, 일시 등을 기재하여 개인정보 유출 등에 대한 책임소재를 확인할 수 있는 강화된 보호조치를 추가로 적용할 수 있다.
6. 개인정보 취급자는 개인정보의 이용을 위하여 출력 또는 복사한 자료는 개인정보의 이용 목적이 완료된 경우 분쇄기로 분쇄하거나 소각하는 등의 안전한 방법으로 파기하여야 한다.

제22조 홈페이지 개인정보 노출 방지 조치

① 게시판 등 글쓰기 화면에 개인정보 노출 경고메시지 안내
② 개인정보 노출 차단 점검을 연 2회 이상 실시하고 문서화
③ 홈페이지 취약점 점검을 연 2회 이상 실시하고 문서화
④ 홈페이지 회원가입 시 비밀번호 작성 안내 문구를 작성 규칙에 맞게 안내

제23조 취약점 점검

① 분야별 책임자는 사이버 공격으로 인한 개인정보의 유출, 도난 방지 등을 위해 다음의 사항을 포함한 보안대책을 수립 · 시행하고, 보안대책의 적절성을 수시 확인해야 하며, 연 1회 이상 서버 설정 정보와 저장자료의 절취 및 위 · 변조 가능성 등 보안 취약점을 점검 · 보완해야 한다.

1. 서버 내 저장자료에 대하여 업무별 · 자료별 중요도에 따라 개별사용자의 접근권한 차등 부여 및 접근통제
2. 서버 운용에 필요한 서비스 포트 이외 불필요한 서비스 포트 제거 및 관리자용 서비스와 개별사용자용 서비스 분리 · 운용
3. 관리자용 서비스 접속시 특정 IP주소가 부여된 관리용 단말기 지정 · 운용
4. 서버 설정 정보 및 저장자료에 대한 정기적 백업 시행
5. 데이터베이스는 개별사용자의 직접 접속 차단, 개인정보 등 중요정보 암호화 등 데이터베이스별 보안조치 실시

제 6 장 개인정보의 관리적 안전조치

제24조 개인정보보호협의회 구성 · 운영

① 개인정보 보호 업무의 원활하고 체계적인 수행에 필요한 정책 결정 및 지원, 점검 등을 위하여 개인정보 보호책임자, 분야별 책임자 등으로 구성된 협의회(기관협의회, 시스템협의회 등)를 구성하여 운영한다.

1. 개인정보보호협의회는 '정보보안 실무협의회'와 함께 운영할 수 있다.

② 개인정보보호협의회 기능

1. 내부 관리계획 등 개인정보 보호에 관한 정책 수립 및 개선에 관한 사항
2. 개인정보의 수집·이용 및 안전성 확보조치에 관한 사항
3. 애로사항, 우수사례 공유 및 발전방향에 관한 사항
4. 그 밖에 개인정보 보호에 관하여 위원장 또는 위원 과반수가 요청한 사항

제25조 개인정보 유출사고 대응 계획 수립 · 시행

① 개인정보보호 책임자는 개인정보 취급자의 과실 및 오·남용 또는 개인정보처리시스템의 외부 해킹 등으로 개인정보에 대한 침해·유출 사고가 발생할 경우를 대비하여 체계적이고 신속한 대응으로 피해를 최소화 할 수 있도록 대응 계획을 수립하여야 한다.

1. 개인정보 침해 분류

등급	조합 수준	개인정보 항목	영향도 설명
1	개인을 식별할 수 있으며, 악용할 경우 위험이 매우 높은 정보	주민등록, 여권번호, 외국인등록번호, 운전면허번호, 계좌번호, 아이디, 비밀번호, 연계정보(CI)	개인의 신분 및 신상 정보에 대해 알 수 있으며, 악용할 경우위험이 매우 높은 정보
2	개인을 식별할 수 있으며, 악용할 경우 위험이 높은 정보	이름, 주소, 전화번호, 핸드폰번호, 이메일주소, 종교, 병역, 장애등급, 기초수급생활자 정보 등	개인 식별 및 신상정보에 대해 알 수 있으며, 악용할 경우 위험이 높은 정보
3	개인을 식별할 수 있으며, 악용할 수 있는 정보	이름, 주소, 전화번호, 핸드폰번호, 이메일 주소 등	개인의 신분과 신상정보에 대한추정이 가능하여 노출 시, 악용할 수 있는 정보
4	개인을 식별할 수 없으나, 개인을 식별할 수 있는 정보와 같이 노출 시 위험이 높은 정보	인종, 종교, 병역, 장애등급, 기초생활 수급자 정보, 자동차 번호 등	개인의 신분과 신상정보를 파악하기 어려우나 신상정보와 같이 노출 시 매우 민감한 정보

2. 침해사고 대응절차

단 계	구 분	처 리 내 용	주관 · 대상
1단계	침해사고 신고	① 혁신성과팀 유선 · 방문, 공단 홈페이지를 통해침해사고 신고 [개인정보유출신고서] -붙임20	정보주체, 내부직원 외부기관 등
2단계	신고 접수	① 사고내용접수 [개인정보 침해신고 처리대장] -붙임21 ② 이사장 및 개인정보보호 책임자에게 보고 ③ 긴급조치 실시	개인정보보호 담당자 전산실 정보보호 담당자
3단계	침해사고 대응팀 구성	① 개인정보보호 담당자, 분야별책임관, 정보보안전문가, 유지보수 업체 등 참여	개인정보보호 책임관
4단계	침해사고 처리	① 조사(침해규모·경위·방법), 분석조치 및 해결(회수 · 삭제 · 복구 · 보호 · 수사의뢰 등) ② 정보주체 통지 및 관련기관 신고 ③ 관련자 조사 및 징계	침해사고 대응팀
5단계	침해사고 결과보고	① 사건현황, 사건분석, 사건 처리 및 조치현황, 피해규모 및 재발방지대책	침해사고 처리 책임자
6단계	개선 및 이행점검	① 개선안 수립, 개선이행, 이행점검	개인정보보호 책임관

3. 침해사고 유출통지, 신고방법 및 개인정보 침해구제

구 분	조 치 사 항
개인정보 유출 통지 시기	① 개인정보보호 담당자는 개인정보 유출 사실을 인지하였을 경우 즉시 해당 정보주체에게 알림 ② 개인정보보호 담당자는 긴급조치가 필요한 경우에는 해당 조치를 취한 후 정보주체에게 알림 1. 접속경로 차단, 취약점 점검 · 보완, 유출된 정보 삭제 및 외부 접근기록 등 증거 확보 조치 등
유출 통지 항목	① 정보주체에게 통지 항목 ▸ 유출된 개인정보의 항목, 유출된 시점과 경위 ▸ 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보 ▸ 대응조치 및 피해구제절차 ▸ 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처 ② 통지항목에 대하여 구체적인 내용을 확인하지 못할 경우 1. 유출이 발생한 사실과 통지항목 중 확인된 사항을 먼저 알리고 나중에 확인되는 사항을 추가로 알림
유출 통지 방법	① 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 등 ② 연락처가 없어 개별통지가 어려운 경우, 인터넷 홈페이지에 지속 게재 ③ 정보주체에 관한 개인정보가 유출된 경우, 정보주체에게 통지하는 동시에, 인터넷 홈페이지에 유출 통지 항목을 7일 이상 게재
유출신고	① 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우 양천구청 및 행정안전부에 5일 이내에 신고 [개인정보유출신고서] - 붙임20
유출 신고 방법	① 전자우편, 팩스, 개인정보포털(www.privacy.go.kr)로 신고 ② 시간적 여유가 없거나 특별한 사정이 있는 경우, 전화로 사전 신고 후 제출 [개인정보유출신고서] - 붙임20
개인정보보호 위반 직원 징계	① 양천구시설관리공단 인사규정 시행내규 - 징계양정 기준에 의거 처리

② 제1항에 따른 개인정보 유출사고 대응 계획에는 긴급조치, 유출통지· 조회 및 신고 절차, 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다. 또한 개인정보 보호책임자는 개인정보 유출사고 대응 계획을 각 부서에 공문으로 발송하고 전 직원이 언제든지 열람할 수 있도록 내부 행정업무시스템의 게시판에 게시하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

③ 개인정보 보호책임자는 개인정보 유출에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

제26조 위탁계약 및 위탁업무의 공개

① 개인정보보호 관리 책임자가 개인정보의 처리업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 관리적·기술적·물리적 조치에 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 등에 관한 사항

② 부서별 개인정보 처리업무 위탁 시 계약서에 포함하여 계약을 체결해야한다.「표준 개인정보처리위탁 계약서(붙임1-첨부2)」

③ 위탁자가 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 인터넷 홈페이지 등을 통해 지속적으로 공개하여야 한다.

제27조 수탁자에 대한 관리 · 감독

① 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 위탁자가 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

1. 수탁자의 개인정보 처리현황 및 실태, 목적 외 이용제공 여부, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 관리·감독하여야 한다.

② 개인정보처리 업무를 위탁하는 경우에 위탁자는 아래의 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 등에 관한 사항

제28조 개인정보 위험도 분석 및 관리

① 분야별 책임자는 개인정보파일(개인정보처리시스템 포함)을 운용하고자 하는 경우 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 사전에 식별 · 평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안을 마련하기 위해 위험 분석을 하고 필요한 조치를 하여야 한다.

② 개인정보 수집·이용체계 변경, 개인정보처리시스템 구성 변경, 내·외부망 연계, 기타 운용 체계가 변경되는 경우 위험 분석을 재실시하여야 한다.

③ 위험 분석은 개인정보 위험도 분석 기준을 활용하거나 위험요소를 식별 및 평가하는 등의 방법으로 수행할 수 있다.

※ 구체적인 위험도 분석 및 대응방안은「개인정보 위험도 분석 기준 및 해설서」에 따름

제 7 장 개인정보의 물리적 안전조치

제29조 물리적 접근 제한

① 개인정보 보호책임자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 장소를 별도로 두고 있는 경우에는 이에 대한 출 입통제 절차를 수립·운영하여야 하며 물리적 접근제한을 위한 잠금장치, 지문인식장치, CCTV 등을 설치하고 출입자 관리대장을 비치하여야 한다.

② 개인정보 보호책임자는 개인정보 취급자 또는 정보시스템의 유지관리 수행을 위한 용역업체 직원 등 상시출입자로 지정되지 않은 자가 제1항의 장소에 출입하거나 그 곳에 보관하고 있는 개인정보를 열람할 경우 출입 사실 및 열람 내용을 출입자 관리대장에 기록하고 관리하여야 한다.

③ 개인정보 보호책임자는 제2항의 출입자 관리대장의 출입 및 열람 내용을 주기적으로 검토하여 정당하지 않은 권한으로 출입하거나 열람하는 경우가 있는지를 점검·확인하여야 한다.

④ 개인정보 취급자는 민감한 개인정보 또는 다량의 개인정보가 포함된 정보를 출력하거나 복사하여 보관할 경우 장금장치가 되어 있는 안전한 곳에 보관하여야 한다.

⑤ 개인정보 취급자는 개인정보가 포함된 보조저장매체 사용 시 안전한 저장매체를 이용하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

⑥ 공단 홈페이지 내 개인정보 유출 방지를 위하여 다음 각 호를 조치하여야 한다.

1. 홈페이지 취약점 점검을 연 1회 이상 실시하고 문서화
2. 홈페이지 회원가입 시 비밀번호 작성 안내 문구를 작성규칙에 맞게 안내
3. 게시판 등 글쓰기 화면에 개인정보 노출 주의 안내

제30조 재해 · 재난 대비 안전조치

① 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 다음 각 호의 조치를 하여야 한다.

1. 위기대응 매뉴얼 등 대응 절차를 마련하고 정기적으로 점검
2. 개인정보처리시스템 백업 및 복구를 위한 계획을 마련

※ 세부사항은 「재해·재난 대비 개인정보처리시스템 위기대응 지침」참고

제31조 개인정보파일 등록 및 변경

① 개인정보 취급자는 개인정보파일을 보유할 경우 보유를 시작(변경)한 날로부터 60일 이내에 개인정보파일명, 수집근거, 보유목적, 보유 기간 등을 행정안전부에서 운영하는 개인정보보호 종합지원시스템(http://intra.privacy.go.kr)에 등록(변경)하여야 하며, 개인정보보호 책임자는 개인정보 취급자가 등록(변경) 신청한 개인정보파일에 대하여 검토하고 승인 또는 반려처리 하여야 한다. 다만, 생성 변경이 상시적으로 이루어지는 경우에는 1년 1회 변경 등록이 가능하다.

② 개인정보파일을 등록할 시에는 다음의 각 호를 입력해야 한다.

1. 개인정보파일을 운용하는 기관의 명칭/개인정보파일의 명칭
2. 개인정보파일의 운영 근거 및 목적, 개인정보파일에 기록되는 개인정보의 항목
3. 개인정보파일로 보유하고 있는 개인정보의 보유 건수
4. 개인정보의 처리방법, 개인정보의 보유기간
5. 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
6. 개인정보 처리 관련 업무를 담당하는 부서 및 열람 요구를 접수 및 처리하는 부서
7. 개인정보파일의 개인정보 중 영 제35조제4항에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유
8. 개인정보 영향평가를받은 개인정보파일의 경우 그 영향평가의 결과

제32조 개인정보의 파기

① 개인정보 취급자는 보유기간 종료일 또는 개인정보처리가 불필요한 것으로 인정되는 날로부터 5일 이내에 개인정보를 파기하여야 하며, 개인정보파일을 파기하기 전에 개인정보파일 파기 요청서 작성하여 개인정보보호담당자에게 제출하여야 한다.

② 개인정보보호 담당자는 개인정보파일 파기 요청 시 파기 결과를 확인한 후, 개인정보파일 파기 관리대장을 작성하고 행정안전부에서 운영하는 개인정보보호 종합지원시스템에 등록된 개인정보파일 현황을 삭제하여야 한다.

③ 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각·파쇄 등)
2. 전용 소자 장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

④ 개인정보처리자가 개인정보의 일부만을 파기하는 경우 “완전파괴, 전용 소자 장비를 이용하여 삭제, 데이터가 복원되지 않도록 초기화 또는 덮어쓰기” 방법으로 파기하는 것이 어려운 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

⑤ 그 밖에 파기 절차에 대한 기준은 영 제21조 및 동법 시행령 제 16조를 따른다. 단,「공공기록물 관리에 관한 법률」등 다른 법령에서 보존해야하는 경우에는 예외를 둔다.

제33조 개인정보 처리실태 조사

① 개인정보 보호책임자는 개인정보보호를 위한 내부관리 계획 및 관련 법령에서 정하는 개인정보보호 규정을 성실히 이행하는지에 대한 실태조사를 할 수 있다.

② 개인정보 보호책임자는 개인정보의 처리에 대한 실태조사를 위해 조사 대상, 일정, 절차 및 방법 등을 포함하는 실태조사 계획을 별도로 수립·시행할 수 있다.

③ 개인정보보호 분야별 책임자는 수시로 개인정보 취급자 및 개인정보 처리시스템에 대해 개인정보처리실태 점검, 관리·감독을 통하여 개선 조치하고, 개인정보의 처리 실태조사에 적극 협조하여야 한다.

제 8 장 영상정보처리기기 관리 계획

제34조 고정형 영상정보처리기기 설치 및 운영

① 고정형 영상정보처리기기를 공개된 장소에 설치·운영하고자 하는 경우 법 제25조에서 정하는 경우를 제외하고는 불가하며, 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 설치·운영할 수 없다.

② 공개된 장소에 고정형 영상정보처리기기를 설치·운영하려는 경우 행정예고, 설명회, 설문조사 등을 통해 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

③ 고정형 영상정보처리기기 도입시 「국가 정보보안 기본지침」 제23조 제1항에 따라 보안기능확인서 또는 한국정보통신기술협회(TTA)의 공공기관용 보안 성능품질 인증 등 일정한 보안성능이 확인된 제품 도입하여야 하며, 구축 시 “보안성 검토”를 수행하여야 한다.

④ 고정형 영상정보처리기기를 설치·운영하는 경우 영 제25조제1항 각 호의 사항이 포함된 「고정형 영상정보처리기기 운영·관리 방침」을 수립하고, 인터넷 홈페이지에 게재하여 정보주체에게 공개하여야 한다.

※ 고정형 영상정보처리기기 운영·관리에 관한 사항을 개인정보 처리방침에 포함하여 공개 가능

⑤ 고정형 영상정보처리기기를 설치·운영하고자 하는 경우 정보주체가 쉽게 알아 볼 수 있도록 법 제25조제4항 각 호의 사항이 포함된 안내판을 설치하여야 한다.

※ 영 제24조제2항 각 호에 해당하는 경우 안내판 설치를 갈음하여 인터넷 홈페이지에 게재 가능

제35조 고정형 영상정보처리기기 운영·관리 방침 수립 및 공개

① 개인정보 보호책임자는 다음 각 호의 사항을 모두 포함한 영상정보처리기기 운영·관리 방침을 수립하여 공단 대표 홈페이지를 통하여 공개하여야 한다.

1. 고정형 영상정보처리기기의 설치 근거 및 설치 목적
2. 고정형 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위
3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람
4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법
5. 영상정보처리기기 운영자의 영상정보 확인 방법 및 장소
6. 정보주체의 영상정보 열람 등 요구에 대한 조치
7. 영상정보 보호를 위한 기술적·관리적 및 물리적 조치
8. 그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항

제36조 이동형 영상정보처리기기 운영

① 업무를 목적으로 이동형 영상정보처리기기를 공개된 장소에서 운영하고자 하는 경우 법 제25조의2에서 정하는 경우를 제외하고는 불가하며, 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 촬영할 수 없다.

② 이동형 영상정보처리기기를 설치·운영하는 경우 영 제25조제1항 각 호의 사항이 포함된 「이동형 영상정보처리기기 운영·관리 방침」을 수립하고, 인터넷 홈페이지에 게재하여 정보주체에게 공개하여야 한다.

※ 이동형 영상정보처리기기 운영·관리에 관한 사항을 개인정보 처리방침에 포함하여 공개 가능

③ 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하는 경우 불빛, 소리, 안내판, 안내서면, 안내방송 등의 방법으로 정보주체가 촬영 사실을 쉽게 알 수 있도록 표시하고 알려야 한다.

※ 드론을 이용한 항공촬영 등 정보주체에게 촬영 사실을 알리기 어려운 경우에는 보호위원회가 구축·운영하는 인터넷 사이트에 공지하는 방법으로 알릴 수 있음

제37조 개인영상정보의 보호 조치

① 개인영상정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 법 제29조 및 영 제30조제1항에 따라 안전성 확보를 위하여 다음의 조치를 하여야 한다.

단 계	주 요 내 용
관리적보안	▪ 처리기록의 보관 및 위조·변조 방지를 위한 조치 - 개인영상정보의 생성 일시 및 열람할 경우에 열람 목적·열람자·열람 일시 등 기록·관리 조치 ▪ 영상정보처리기기 또는 관리서버가 아닌 곳에 영상기록 또는 음성기록 저장·전송 금지 ▪ 저장된 개인영상정보의 임의 편집·삭제 금지 ▪ 정상작동여부 및 보안관리 상태에 대하여 주기적인 점검 실시 ▪ 분실, 피탈 등의 사고발생 시 즉시 관리책임자에게 보고
기술적보안	▪ 관리서버의 접근권한은 업무수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여 ▪ 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용 - 네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일 저장 시 비밀번호 설정 등 ▪ 영상정보처리기기 및 관리서버는 업무망 및 인터넷망과 분리하여 별도의 단독망 구성을 원칙 ▪ 부득이한 사유로 관리서버의 업무망 연결 시에는 Telnet 등 원격접근 서비스 차단 설정, 침입차단 시스템을 활용하여 IP·포트 접근 제한, 디폴트 패스워드 변경, 카메라IP 외부 공개 금지 ▪ 영상정보처리기기 및 관리서버는 계정·비밀번호나 생체인식 등을 통해 접근통제가 되어야 하며, 최신 백신 설치 및 비인가 휴대용 저장장치 사용금지 등 보안조치 철저
물리적보안	▪ 영상정보처리기기 및 관리서버는 비인가자의 임의 조작이 물리적으로 불가능하도록 위치하거나 잠금장치를 설치 ▪ 개인영상정보의 목적을 달성하였을 경우 지체없이 복구불가 하도록 완전 삭제

② 개인영상정보 보호담당자는 “표준 개인정보보호지침“의 준수 여부에 대한 다음 각 호의 사항에 대해 자체점검하고 그 결과를 개인정보보호 종합지원시스템에 등록하여야 하며, 공단 홈페이지에 공개하여야 한다.

제38조 목적 외 및 제3자 제공

① 개인정보보호 분야별 책임자는 개인영상정보를 관련 근거에 의해 제 3자에게 제공할 경우나 수집 목적 이외로 이용할 경우 개인정보의 목적 외 이용 및 제3자 제공대장을 작성하여 관리하여야 한다.

제39조 보관 및 파기

① 개인정보보호 분야별 책임자는 수집한 개인영상정보를 영상정보처리기기 운영·관리 방침에 명시한 보관 기간이 만료한 때에는 다른법령에 특별한 규정이 없는 한 지체 없이 파기하고 개인영상정보 관리대장을 작성하여 관리하여야 한다.

② 개인정보보호 분야별 책임자가 그 사정에 따라 보유 목적의 달성을 한 최소한의 기간을 산정하기 곤란한 때에는 보관 기간을 개인영상정보수집 후 30일 이내로 한다.

③ 개인영상정보의 파기 방법은 다음 각 호의 어느 하나와 같다.

1. 개인영상정보가 기록된 출력물(사진 등) 등은 파쇄 또는 소각
2. 전자기적 파일 형태의 개인영상정보는 복원이 불가능한 기술적 방법으로 영구 삭제

제 9 장 가명정보 처리에 관한 사항

제40조 가명정보 처리 [양천구시설관리공단은 가명정보 처리를 하지 않음]

① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

② 개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니 된다.

③ 개인정보처리자가 개인정보를 가명처리하여 활용하고자 하는 경우 가명처리에 관한 절차 및 방법 등은 보호위원회가 정한 「가명처리 가이드라인」을 준수하여야 한다.

제41조 가명정보의 결합과 반출 등

① 제28조의2에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 보호위원회 또는 관계 중앙행정기관의장이 지정하는 전문기관에서 수행한다.

② 결합을 수행한 기관 외부로 결합된 정보를 반출하려는 개인정보 처리자는 가명정보 또는 제58조의2에 해당하는 정보로 처리한 뒤 전문기관 장의 승인을 받아야한다.

③ 제1항에 따른 결합절차와 방법, 제2항에 따른 반출 및 승인 기준·절차 등 필요한 사항은 보호위원회의 「가명처리의 결합 및 반출 등에 관한 고시」가 정하는 바에 따른다.

제10장 연계정보의 안전조치

제42조 연계정보 보호책임자 지정 등

① 공단은 정보통신망법 제23조의6 및 「연계정보 생성·처리 등에 관한 기준」제11조에 따라 연계정보의 안전조치를 총괄하는 연계정보 보호책임자로 제9조에 따른 개인정보 보호책임자(본부장)를 지정한다.

② 연계정보 보호책임자를 보좌하여 연계정보 안전조치 실무를 담당하는 연계정보 보호담당자는 개인정보 보호담당자로 한다.

③ 연계정보 보호책임자는 다음 각 호의 업무를 수행한다.

1. 연계정보 안전조치에 관한 내부 규정의 수립·시행 및 개정
2. 연계정보취급자의 지정·관리 및 교육
3. 연계정보 처리 실태의 정기 점검(연 1회 이상) 및 개선
4. 연계정보 침해사고 대응 계획의 수립·시행
5. 연계정보 수집 근거 및 현황의 기록·보관 관리
6. 그 밖에 연계정보의 안전한 처리를 위하여 필요한 사항

제43조 연계정보의 취급 · 관리 절차

① 공단은 홈페이지 회원가입 시 휴대폰 본인인증 과정에서 본인확인기관으로부터 연계정보를 제공받을 수 있으며, 연계정보를 목적 외로 이용하거나 제3자에게 제공하지 아니한다.

② 공단은 본인인증 과정에서 연계정보가 제공되는 경우에도 이를 이용하지 아니하며, 데이터베이스·로그·파일 등에 저장하지 아니한다.

③ 연계정보 처리시스템을 변경하여 연계정보를 저장하려는 경우에는 사전에 연계정보 보호책임자의 승인을 받아야 하며, 저장 전에 제44조 및 제45조에 따른 안전조치를 적용하여야 한다.

④ 연계정보 보호책임자는 연계정보 처리시스템을 운영·관리하는 연계정보취급자를 업무상 필요한 최소한의 인원으로 지정하고, 「연계정보취급자

지정 현황」(붙임 23)으로 관리하여야 한다.

⑤ 연계정보 처리시스템에 대한 접근권한의 신청·승인·변경·말소는 제16조 및「개인정보처리시스템 접근권한 관리 지침」에 따르며, 퇴직·전보 등으로 업무가 변경된 경우 지체 없이 권한을 말소하고 그 내역을 기록하여야 한다.

⑥ 연계정보 보호담당자는 분기 1회 이상 연계정보취급자 목록과 담당업무의 적정성을 검토하고 그 결과를 기록하여야 한다.

⑦ 연계정보 보호책임자는 연계정보취급자를 대상으로 연 1회 이상 연계정보의 안전한 처리에 관한 교육을 실시하여야 하며, 제4장에 따른 개인정보 보호교육에 연계정보 관련 내용을 포함하여 실시할 수 있다.

제44조 주민등록번호와 연계정보의 분리 보관

① 공단은 법령에 근거가 있는 경우를 제외하고는 정보주체의 주민등록번호를 수집·보관하지 아니한다.

② 제43조제3항에 따라 연계정보를 저장하는 경우로서 법령에 따라 주민등록번호를 보관하는 경우에는 비인가자의 접근 등에 의해 연계정보와 주민등록번호가 함께 유출되지 않도록 다음 각 호의 어느 하나의 방법으로 분리하여 보관·관리하여야 한다.

1. 물리적 분리 : 서버 또는 DBMS를 달리하여 보관
2. 논리적 분리 : DBMS의 인스턴스 또는 테이블을 달리하여 보관하고, 각각에 대한 접근권한을 업무 특성에 따라 최소한으로 차등 부여

제45조 연계정보의 안전한 저장 · 전송

① 연계정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 SSL/TLS 등 안전한 암호 알고리즘을 적용한 보안 기술을 사용하여 암호화하여야 한다.

② 제43조제3항에 따라 연계정보를 저장하는 경우에는 안전한 암호 알고리즘으로 암호화하여 저장하여야 하며, 연계정보 처리 과정에서 로그 형태로

저장되는 연계정보도 또한 같다.

③ 제2항에 따른 암호화에 사용하는 암호 키의 생성·이용·보관·배포 및 파기는 제18조제6항에 따른 절차를 준용한다.

④ 연계정보는 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장하여서는 아니 된다.

제46조 연계정보 유출 · 도난 방지를 위한 취약점 점검

① 연계정보 보호책임자는 연계정보의 유출·도난을 방지하기 위하여 연 1회 이상 연계정보 처리시스템(홈페이지 본인인증 연동 기능 등)에 대한 보안 취약점 점검을 실시하여야 한다.

② 제1항의 취약점 점검은 제23조에 따른 취약점 점검 및 웹 취약점 진단과 병행하여 실시할 수 있으며, 점검 결과 발견된 취약점은 지체 없이 조치하고 그 결과를 기록·보관하여야 한다.

제47조 연계정보 침해사고 대응

① 공단은 연계정보의 수집 출처, 처리 목적, 처리 방법, 이용·보유 여부(이용·저장하지 않음) 및 안전조치 등 연계정보 처리에 관한 사항을 개인정보 처리방침에 포함하여 인터넷 홈페이지에 공개하여야 한다.

② 연계정보 침해사고의 접수 및 처리는 다음 각 호에 따른다.

1. 접수 창구 : 개인정보 고충처리부서(혁신성과팀) 유선·방문, 공단 홈페이지 민원센터, 전자우편
2. 대응 절차 : 사고 접수·인지 → 연계정보 보호책임자 보고 → 피해 확산 방지(접근 차단, 계정 잠금 등) → 원인 분석 및 증거 보존 → 정보주체 통지 및 관계 법령에 따른 신고 → 피해 복구 및 재발방지 대책 수립
3. 대응 담당 : 연계정보 보호책임자(총괄), 연계정보 보호담당자(실무), 분야별 책임자 및 수탁자(협조)
4. 그 밖의 세부 절차는 제25조 및 「개인정보 침해·유출사고 대응 지침」을 준용한다.

③ 정보주체는 연계정보 이용내역 등 연계정보 처리에 관한 사항의 열람, 정정·삭제, 처리정지, 동의 철회를 요구할 수 있으며, 공단은 개인정보 처리 방침 제11조 및 「개인정보 정보주체 권리행사 절차서」에 따라 지체 없이 처리한다. 이 경우 요구 방법과 절차는 연계정보 수집 방법과 절차보다 어렵지 않도록 하여야 한다.

제48조 연계정보 수집 현황의 기록 · 보관 및 실태점검

① 연계정보 보호담당자는 연계정보 수집의 근거 및 현황을 확인할 수 있도록 다음 각 호의 사항을 분기별로 「연계정보 수집 현황 기록대장」에 기록하여야 한다. 이 경우 연계정보 값 자체는 기록하지 아니한다.

1. 수집 출처(연계정보를 제공한 본인확인기관의 명칭)
2. 수집 시기(본인인증 기간 및 건수)
3. 수집 목적
4. 수집 대상(본인인증을 거쳐 가입한 회원) 및 건별 세부 기록 위치

② 건별 세부 기록은 홈페이지 회원 데이터베이스의 본인인증 이력(본인인증 일시·회원번호)으로 갈음하며, 제1항의 기록대장은 1년 이상 보관하여야 한다. 이 경우 해당 기록은 제30조 및 「재해·재난 대비 개인정보처리 시스템 위기 대응 지침」에 따른 정기 백업 대상에 포함하여 관리한다.

③ 연계정보 보호책임자는 연계정보가 이 장에 따라 안전하게 처리되고 있는지 연 1회 이상 실태점검을 실시하고, 점검 결과 미흡사항은 개선 조치하여야 한다.

제11장 그 밖에 개인정보 보호를 위하여 필요한 사항

제49조 개인정보보호 자체점검 주기 및 절차

① 개인정보 보호책임자는 본부 및 소속기관이 「개인정보 보호법」 등에서 규정하고 있는 사항을 성실히 이행하고 있는지 여부를 다음과 같은 절차에 따라 관리·감독한다.

분 류	내 용	점검주기
개인정보 보호 관리실태 점검	개인정보 보호 법령 및 개인정보 내부 관리계획에 따른 보호조치의 적정성 점검	연1회
개인정보 처리업무 위·수탁 실태 점검	법적 요구사항 준수 및 안전조치를 위한 개인정보 처리업무 위수탁 실태점검	반기
접근권한 관리실태 점검	개인정보의 오·남용 및 불법 유출을 사전에 예방하기 위한 접근권한 관리실태 점검	반기
접속기록 관리실태 점검	DB접근제어 시스템을 및 로그 솔루션 활용	월1회
PC 보안 점검	개인정보취급자 PC의 안전성 점검	반기
정보화시스템	백업, 그룹웨어, 주차, 회원관리 등 보안점검	월1회
영상정보처리시스템	운영부서 주관으로 점검 실시	연1회
연계정보 처리실태 점검	「연계정보 생성·처리 등에 관한 기준」[별표4]에 따른 연계정보 안전조치 이행 여부 점검	연1회

② 자체점검을 위한 점검대상, 점검절차 등에 관한 사항을 포함하여 별도의 계획을 수립할 수 있다.

제50조 자체점검 결과 관리

① 자체점검 결과 미흡한 사항에 대해서는 매회 이행점검을 수행해야 하며, 이행계획을 수립하지 않는 경우에는 개인정보 보호책임자 또는 개인정보 보호 담당자를 통해 시정·개선 등의 필요한 조치를 지시할 수 있다.

② 개인정보 보호책임자는 개인정보보호법령 미준수 사항에 대한 시정·개선 조치가 이행되지 않거나, 개인정보 보호에 심각한 영향이 발생할 우려가 있는 경우 개인정보취급자 등에 대한 징계조치를 취할 수 있다.

제51조 타 법령과의 관계

① 이 내부관리계획에 명시되지 않은 사항은 다음 각 호에 따른다.

1. 「개인정보보호법」 및 같은 법 시행령 및 시행규칙
2. 「표준 개인정보보호지침」(개인정보보호위원회 고시)
3. 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2025-9호)
4. 「개인정보 영향평가에 관한 고시」(개인정보보호위원회 고시)
5. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 같은 법 시행령
6. 「연계정보 생성·처리 등에 관한 기준」

붙임1 수탁업체 교육자료

수탁업체 교육자료

○ 수탁자의 책임 및 의무(개인정보보호법 제5항, 제6항, 제7항)

가. 수탁업무 목적 외 개인정보 이용·제공 금지(제5항)

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

나. 수탁자의 불법행위로 인한 손해배상책임(제6항)

- 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반 하여 발생한 손해배상책임에 대하여는 수탁자가 모든 책임을 져야 한다.

다. 개인정보처리자의 의무 등 준용(제7항)

- 개인정보 처리 업무를 위탁받아 처리하는 수탁자는 개인정보를 보호하기 위하여 “개인정보의 안전성 확보조치 기준 고시”(이하 “안전성 확보조치 기준 고시”라 한다.)가 정하고 있는 기술적 · 물리적 · 관리적 조치를 하여야 한다

라. 수탁자의 누출금지 대상 정보

- 전산시스템의 내·외부 IP주소 현황
- 전산시스템 구성현황 및 전산망구성도
- 사용자계정 및 패스워드 등 시스템 접근권한 정보
- 전산시스템 취약점 및 보안시스템 취약점
- 용역사업 결과물 및 프로그램 소스코드
- 보안시스템 및 정보보호시스템 도입현황
- 방화벽·IPS 등 정보보호제품 및 라우터·스위치 등 네트워크장비 설정 정보
- ‘개인정보보호법’에 따른 개인정보
- 기타 양천구시설관리공단에서 공개가 불가하다고 판단한 자료

교육일자			
교육자 소속		수탁업체명	
교육자 성명	(인)	수탁업체 직원 성명	(인)

붙임2 표준 개인정보처리위탁 계약서(안)

표준 개인정보처리위탁 계약서(안)

OOO(이하 “위탁자”라 한다)과 △△△(이하 “수탁자”라 한다)는 “위탁자”의 개인정보 처리업무를 “수탁자”에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제1조 (목적) 이 계약은 “위탁자”가 개인정보 처리업무를 “수탁자”에게 위탁하고, “수탁자”는 이를 승낙하여 “수탁자”의 책임 아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는 개인정보 보호법, 같은 법 시행령, 개인정보의 안전성 확보조치 기준(개인정보보호위원회 고시), 표준 개인정보 보호지침(개인정보보호위원회 고시) 등에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) “수탁자”는 계약이 정하는 바에 따라 (_____) 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.[1)]

1. (위탁하는 개인정보 처리 업무 내용을 기재)
2. (위탁하는 개인정보 처리 업무 내용을 기재)

제4조 (위탁업무 기간) 이 위탁 계약서에 의한 개인정보 처리업무의 기간은 다음과 같다.

계약 기간 : 20 년 월 일 ~ 20 년 월 일

제5조 (재위탁 제한) ① “수탁자”는 “위탁자”의 동의를 얻은 경우를 제외하고 위탁받은 개인정보 처리 업무를 제3자에게 재위탁할 수 없다.

② “수탁자”가 “위탁자”의 동의를 받아 개인정보 처리 업무의 전부 또는 일부를 제3자에게 다시 위탁하는 경우에는 “위탁자”에게 재위탁받는 자 및 재위탁 업무의 범위를 알려야 한다. 다만, “수탁자”가 사전에 재위탁의 범위와 재위탁자를 정하여 “위탁자”에게 알리고 동의를 받았을 때에는 그러하지 아니하다.

③ “수탁자”는 이 규정에 따른 재위탁을 문서로 하여야 한다.

④ “수탁자”는 재위탁받는 자의 명칭과 그 업무 범위를 개인정보처리방침으로 공개하여야 한다.

1) 각호의 업무 예시 : 고객만족도 조사 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 이름, 주소, 연락처 처리 등

제6조 (개인정보의 안전성 확보조치 등) “수탁자”는「개인정보 보호법」제29조, 같은 법 시행령 제30조 및 개인정보의 안전성 확보조치 기준(개인정보보호위원회 고시)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 및 물리적 안전조치를 하여야 한다.

제7조 (개인정보의 처리 제한) “수탁자”는 계약 기간 동안은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

제8조 (수탁자에 대한 관리·감독 등) ① “위탁자”는 “수탁자”에 대하여 개인정보의 처리 위탁과 관련하여 다음 각 호의 사항을 관리하도록 요구할 수 있으며, “수탁자”는 특별한 사유가 없는 한 이에 응해야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속기록
3. 개인정보 접근 또는 접속 대상자
4. 목적 외 이용·제공 및 재위탁 제한 사항 준수 여부
5. 암호화 등 안전성 확보조치 이행 여부
6. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② “위탁자”는 “수탁자”에 대하여 제1항 각 호의 사항에 대한 현황을 점검하거나 “수탁자” 또는 제3자에 의한 현황 점검을 요구할 수 있고, 점검 사항에 대하여 시정을 요구할 수 있다. “수탁자”는 특별한 사유가 없는 한 “위탁자”의 요구를 이행해야 한다.

③ “수탁자”가 다음 각 호 중 어느 하나에 해당하는 경우에는 그러한 사정을 “위탁자”에게 알리고 위탁받은 개인정보의 처리 업무에 대한 점검 결과를 “위탁자”에게 [ ] 개월의 단위로 정기적으로 보고하는 것으로 위 각 항에 따른 “위탁자”와 “수탁자”의 의무 이행에 갈음할 수 있다. “위탁자”에 대한 “수탁자”의 보고의 시기 등에 대하여는 “위탁자”와 “수탁자”가 협의하여 정할 수 있다.

1. 개인정보 보호법 제32조의2에 따른 개인정보 보호 인증(ISMS-P)을 취득하여 주기적으로 점검을 받고 있는 경우
2. 그 외 위 1호에 준하는 경우로서, “위탁자”와 “수탁자”가 합의하여 개인정보 보호법 제31조 제7항의 개인정보 보호책임자 협의회 등에 의한 점검 등을 주기적으로 받고 있는 경우

④ 제3항에 경우에도 “수탁자”는 “수탁자”의 처리위탁 업무와 관련하여 개인정보 보호법 위반 또는 본 계약 위반의 사항이 발생한 경우에는 즉시 이를 “위탁자”에게 통지하여야 하고, “위탁자”의 지시에 따라야 한다.

제9조 (수탁자에 대한 교육) ① “위탁자”는 개인정보 보호법 제26조 제4항에 따라 개인정보 처리 업무의 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또

는 훼손되지 아니하도록 “수탁자”를 교육할 수 있으며, “수탁자”는 이에 응하여야 한다. “수탁자”는 “위탁자”와 협의하여 “수탁자”의 책임 하에 그의 개인정보 취급자 등에게 교육을 실시할 수 있다.

② 제1항에 따른 교육은 집합교육, 온라인 교육 등의 방식 등 교육 목적을 달성할 수 있는 범위 내에서 다양한 방식으로 진행될 수 있으며, 구체적인 방식에 대하여는 “위탁자”와 “수탁자”는 별도로 협의하여 정할 수 있다, 다만, “수탁자”가 자체적으로 또는 제3자인 전문업체를 통해 교육을 실시하는 경우에는 “수탁자”는 교육의 시행 여부 및 결과 등을 “위탁자”에게 증빙자료와 함께 보고하여야 하고, “위탁자”는 보고 내용을 주기적으로 점검할 수 있다.

③ 그 밖에 구체적으로 교육의 시기와 방법 등에 대해서는 “위탁자”는 “수탁자”와 협의하여 시행한다.

제10조 (정보주체 권리보장) “수탁자”는 정보주체의 개인정보 열람, 정정·삭제, 처리 정지 요청 등에 대응하기 위한 연락처 등 민원 창구를 마련해야 한다.

제11조 (개인정보의 파기) ① “수탁자”는 계약이 해지되거나 계약 기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 개인정보 보호법 시행령 제16조에 따라 즉시 파기하거나 “위탁자”에게 반환하여야 한다.

② 제1항에 따라 “수탁자”가 개인정보를 파기한 경우에는 지체없이 “위탁자”에게 그 결과를 통보해야 한다.

제12조 (손해배상) ① “수탁자”가 이 계약에 따른 의무를 위반하여 정보주체 또는 제3자에게 손해가 발생할 경우 “위탁자”와 “수탁자”는 공동으로 정보주체 또는 제3자의 손해를 배상하기로 한다.

② 제1항과 관련하여 정보주체 또는 제3자의 손해를 배상한 당사자는 상대방에게 자신의 부담 비율을 초과하는 부분에 대하여 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, “위탁자”와 “수탁자”가 서명 또는 날인한 후 각 1부씩 보관한다.

20 . . .

위탁자	수탁자
주 소 :	주 소 :
기관(회사)명 :	기관(회사)명 :
대표자 성명 : (인)	대표자 성명 : (인)

붙임3 보안서약서(대표자용)

(앞면)

보 안 서 약 서
(대표자용)

주식회사 ○○○○○○○은 양천구시설관리공단 ○○○○○○○○와 관련된 업무가 기밀사항임을 인정하고, 공단의 알게 된 모든 기밀사항을 일체타인에게 누설하지 아니한다. 또한, 기밀을 누설한 때에는 어떠한 엄중한 처벌과 모든 손해배상을 변상할 것을 서약한다.

【누출금지 대상 정보】

1. 전산시스템의 내·외부 IP주소 현황
2. 전산시스템 구성현황 및 전산망구성도
3. 사용자계정 및 패스워드 등 시스템 접근권한 정보
4. 전산시스템 취약점 및 보안시스템 취약점
5. 용역사업 결과물 및 프로그램 소스코드
6. 보안시스템 및 정보보호시스템 도입현황
7. 방화벽·IPS 등 정보보호제품 및 라우터·스위치 등 네트워크장비 설정 정보
8. '개인정보보호법'에 따른 개인정보
9. 양천구시설관리공단의 대외비 등
10. 기타 양천구시설관리공단에서 공개가 불가하다고 판단한 자료

※ 위의 모든 항목은 양천구시설관리공단에서 취급하는 모든 정보를 말한다.

※ 사업기간 중 공개불가 자료가 발생 시, 공단에서 추가 할 수 있음

※ 본 계약과 관련하여 이면 기재사항의 보안정책에 충실하며, 위반하였을 경우 관련자의 엄중한 처벌과 모든 손해배상을 변상한다.

20 년 월 일

주 소 :

상 호 :

성 명 : 대 표 (인)

(뒷면)

사업자 보안정책

(대표자용)

1. 비밀 및 대외비 급 정보 등 유출금지
   (정보시스템 구조, 데이터베이스, 개인정보 및 비공개 정보 등 유출금지)

2. 정보시스템에 대한 불법적 행위 금지
   (관련 시스템의 해킹, 시스템 구축 결과물의 유출 및 시스템 내 인위적인 악성코드 유포 금지)
   ※ 용역업무 수행 목적 외 개인정보의 처리 및 접근 금지

3. 비공개 정보 관리 강화
   (비공개 정보, 개인정보를 책상 위 등에 방치 및 휴지통·폐지함 등에 유기 또는 이면지 활용 금지)

4. 사무실·보호구역 보안관리 강화
   (통제구역 출입문을 개방한 채 퇴근, 인가되지 않은 작업자의 내부 시스템 접근, 통제구역 내 장비·시설 등 무단 사진촬영 금지 및 용역관련 사전승인을 받지 않은 하도급 금지 등)

5. 전산정보 보호대책 강화
   - 업무망 인터넷망 혼용사용, 보안 USB 사용규정 위반 및 보안관련 프로그램 강제 삭제 금지
   - 웹하드·P2P 등 인터넷 자료공유사이트를 활용하여 용역사업 관련 자료 수발신 금지
   - 개발·유지보수 시 원격작업 사용 및 저장된 비공개 정보 패스워드 미부여 금지
   - 인터넷망 연결 PC 하드디스크에 비공개 정보 저장 및 외부용 PC를 업무망에 무단연결사용 금지
   - 사용자 계정관리 미흡 및 오남용 금지(시스템 불법접근 시도 등)
   - 개인정보에 대한 접근제한 등 안전성 확보 조치
   - 비인가 메신저 무단 사용 및 비인가 보조기억매체 무단 사용 금지
   - PC내 보안성이 검증되지 않은 프로그램 사용 금지
   - 보안관련 소프트웨어의 주기적 점검

6. 주기적 보안점검 실시
   (보안관리자를 지정하여 용역관련 별도의 물리적·관리적·기술적 보안점검 실시)

붙임4 보안서약서(직원용)

(앞면)

보 안 서 약 서
(직원용)

주식회사 ○○○○○○○은 양천구시설관리공단 ○○○○○○○○와 관련된 업무가 기밀사항임을 인정하고, 공단의 알게 된 모든 기밀사항을 일체타인에게 누설하지 아니한다.

또한, 기밀을 누설한 때에는 어떠한 엄중한 처벌과 모든 손해배상을 변상할 것을 서약한다.

【누출금지 대상 정보】

1. 전산시스템의 내·외부 IP주소 현황
2. 전산시스템 구성현황 및 전산망구성도
3. 사용자계정 및 패스워드 등 시스템 접근권한 정보
4. 전산시스템 취약점 및 보안시스템 취약점
5. 용역사업 결과물 및 프로그램 소스코드
6. 보안시스템 및 정보보호시스템 도입현황
7. 방화벽·IPS 등 정보보호제품 및 라우터·스위치 등 네트워크장비 설정 정보
8. '개인정보보호법'에 따른 개인정보
9. 양천구시설관리공단의 대외비 등
10. 기타 양천구시설관리공단에서 공개가 불가하다고 판단한 자료

※ 위의 모든 항목은 양천구시설관리공단에서 취급하는 모든 정보를 말한다.

※ 사업기간 중 공개불가 자료가 발생 시, 공단에서 추가 할 수 있음

※ 본 계약과 관련하여 이면 기재사항의 보안정책에 충실하며, 위반하였을 경우 관련자의 엄중한 처벌과 모든 손해배상을 변상한다.

20 년 월 일

주 소 :

상 호 :

성 명 : (인)

(뒷면)

사업자 보안정책

(직원용)

1. 비밀 및 대외비 급 정보 등 유출금지

(정보시스템 구조, 데이터베이스, 개인정보 및 비공개 정보 등 유출금지)

2. 정보시스템에 대한 불법적 행위 금지

(관련 시스템의 해킹, 시스템 구축 결과물의 유출 및 시스템 내 인위적인 악성코드 유포 금지)

※ 용역업무 수행 목적 외 개인정보의 처리 및 접근 금지

3. 비공개 정보 관리 강화

(비공개 정보, 개인정보를 책상 위 등에 방치 및 휴지통·폐지함 등에 유기 또는 이면지 활용 금지)

4. 사무실·보호구역 보안관리 강화

(통제구역 출입문을 개방한 채 퇴근, 인가되지 않은 작업자의 내부 시스템 접근, 통제구역 내 장비·시설 등 무단 사진촬영 금지 및 용역관련 사전승인을 받지 않은 하도급 금지 등)

5. 전산정보 보호대책 강화

- 업무망 인터넷망 혼용사용, 보안 USB 사용규정 위반 및 보안관련 프로그램 강제 삭제 금지
- 웹하드·P2P 등 인터넷 자료공유사이트를 활용하여 용역사업 관련 자료 수발신 금지
- 개발·유지보수 시 원격작업 사용 및 저장된 비공개 정보 패스워드 미부여 금지
- 인터넷망 연결 PC 하드디스크에 비공개 정보 저장 및 외부용 PC를 업무망에 무단연결사용 금지
- 사용자 계정관리 미흡 및 오남용 금지(시스템 불법접근 시도 등)
- 개인정보에 대한 접근제한 등 안전성 확보 조치
- 비인가 메신저 무단 사용 및 비인가 보조기억매체 무단 사용 금지
- PC내 보안성이 검증되지 않은 프로그램 사용 금지
- 보안관련 소프트웨어의 주기적 점검

6. 주기적 보안점검 실시

(보안관리자를 지정하여 용역관련 별도의 물리적·관리적·기술적 보안점검 실시)

붙임5 개인정보 처리 업무위탁 시 점검사항

1. 점검대상

위탁사업명			
수탁기관		연락처	
점검일자		작성자	

2. 점검사항

구분	상세내역		점검결과
개인정보처리현황	개인정보수집내역		
	개인정보보유건수		
개인정보처리시스템	개인정보처리방법		아래표 참조
	개인정보접근방법		
	개인정보보호조치		

연번	점검지표	점검항목	점검결과		
1	개인정보보호 기반마련	개인정보 보호책임자와 개인정보 보호담당자는 지정하여 운영하고 있는가?	☐ Y	☐ N	☐ 해당 없음
2	개인정보보호교육추진	연간 개인정보보호 교육계획이 수립되어 있는가?	☐ Y	☐ N	☐ 해당 없음
3		개인정보취급자, 일반직원 등에 대한 교육이 모두 이행되고 있는가?	☐ Y	☐ N	☐ 해당 없음
4	개인정보 보호책임자 역할수행	개인정보 보호책임자의 역할이 정의되어있는가?	☐ Y	☐ N	☐ 해당 없음
5		개인정보 보호책임자가 교육이수 및 관리·감독 등 역할을 수행하고 있는가?	☐ Y	☐ N	☐ 해당 없음
6	재위탁 금지	재 위탁은 하고 있지 않는가?	☐ Y	☐ N	☐ 해당 없음
7	개인정보목적외 이용 및 제3자 제공 절차	제공한 개인정보를 목적 외로 이용하거나 제3자에게 제공하고 있는가?	☐ Y	☑ N	☐ 해당 없음
8	개인정보 노출방지	개인정보 노출방지를 위해 보안시스템 및 백신 소프트웨어를 설치하고 운영(모니터링, 정기점검, 업데이트등)을 하고 있는가?	☐ Y	☐ N	☐ 해당 없음
9	개인정보 침해사고 대응절차	제공한 개인정보의 유·노출사고 및 침해사고 발생 시 대응절차를 수립하고 전파하였는가?	☐ Y	☐ N	☐ 해당 없음
10	개인정보 처리시스템 접근권한 및 접속기록	개인정보처리시스템에 접근하는 권한을 담당자별로 차등하여 부여하는가?	☐ Y	☐ N	☐ 해당 없음
11		개인정보처리시스템의 접근 권한을 부여·변경·말소한 기록을 최소 1년이상 보관하는 절차를 마련하고 이를 실행하고 있는가?	☐ Y	☐ N	☐ 해당 없음
12		개인정보처리시스템에 대한 접속기록을 점검·후속조치, 보관·관리 하는가?	☐ Y	☐ N	☐ 해당 없음
13	개인정보 파기 및 관리	제공한 개인정보 처리 목적이 달성되거나 보유기간이 경과한 경우 지체없이(5일 이내) 해당 개인정보를 복원이 불가능한 방법으로 파기하고 있는가?	☐ Y	☐ N	☐ 해당 없음
14		개인정보 취급과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는 가?	☐ Y	☐ N	☐ 해당 없음
15	업무 PC 개인정보보호	업무용 컴퓨터(PC)에 저장된 개인정보는 별도로 암호화하거나 보안 USB에 저장하는가?	☐ Y	☐ N	☐ 해당 없음
16	암호화	고유식별정보, 생체인식정보 정보, 비밀번호를 개인정보처리시스템에 저장하는 경우, 해당 개인정보를 암호화하고 있는가?	☐ Y	☐ N	☐ 해당 없음

붙임6 개인정보파일 보유기간 책정 기준표

개인정보파일 보유기간 책정 기준표

보유기간	대상 개인정보파일
영구	1. 국민의 지위, 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일 2. 국민의 건강증진과 관련된 업무를 수행하기 위해 운용하는 개인정보파일 중 영구보존이 필요한 개인정보파일
준영구	1. 국민의 신분, 재산을 증명하기 위해 운용하는 개인정보파일 중 개인이 사망, 폐지 그 밖의 사유로 소멸되기 때문에 영구 보존할 필요가 없는 개인정보파일 2. 국민의 신분증명 및 의무부과, 특정대상 관리 등을 위하여 행정기관이 구축하여 운영하는 행정정보시스템의 데이터 셋으로 구성된 개인정보파일
30년	1. 관계 법령에 따라 10년 이상 30년 미만의 기간 동안 민·형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
10년	1. 관계 법령에 따라 5년 이상 10년 미만의 기간 동안 민·형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
5년	1. 관계 법령에 따라 3년 이상 5년 미만의 기간 동안 민·형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일
3년	1. 행정업무의 참고 또는 사실 증명을 위하여 1년 이상 3년 미만의 기간 동안 보존할 필요가 있는 개인정보파일 2. 관계 법령에 따라 1년 이상 3년 미만의 기간 동안 민. 형사상 또는 행정상의 책임 또는 시효가 지속되거나, 증명자료로서의 가치가 지속되는 개인정보파일 3. 각종 증명서 발급과 관련된 개인정보파일(단 다른 법령에서 증명서 발급 관련 보유기간이 별도로 규정된 경우 해당 법령에 따름)
1년	1. 상급기관(부서)의 요구에 따라 단순 보고를 위해 생성한 개인정보파일

붙임7 개인정보파일 관리대장

■ 행정안전부 개인정보보호 지침 [별지 제2호서식]

개인정보파일대장

기관 명칭	주소	등록부서	전화번호

등록항목	등록정보
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 기관의 명칭	
개인정보파일로 보유하고 있는 개인정보의 정보주체 수	
해당기관에서 개인정보 처리 관련 업무를 담당하는 부서	
개인정보의 열람 요구를 접수·처리하는 부서	
개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유	

붙임8 개인정보파일 등록·변경 신청서

■ 개인정보 처리 방법에 관한 고시 [별지 제2호 서식]

개인정보파일 ([ ] 등록 [ ] 변경등록) 신청서

접수번호	접수일	처리기간 7일

팀명(부서명)		담 당 자	전화번호

등록항목	등 록 정 보	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」 제32조제1항과 같은 법 시행령 제34조제1항에 따라 위와 같이 개인정보파일 ([ ] 등록 [ ] 변경등록)을 신청합니다.

년 월 일

신 청 부 서

(서명 또는 인)

붙임9 개인정보의 목적 외 이용 및 제 3자 제공 대장

■ 개인정보 처리 방법에 관한 고시 [별지 제1호 서식]

개인정보의 목적 외 이용 및 제3자 제공 대장

개인정보 또는 개인정보파일 명칭			
이용 또는 제공 구분	[ ] 목적외 이용 [ ] 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」 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용			

붙임10 개인정보파일 파기 요청서

표준개인정보보호지침 [별지 제4호서식]

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	
폐기 확인 방법			
백업 조치 유무			
매체 폐기 여부			

붙임11 개인정보파일 파기 관리대장

표준개인정보보호지침 [별지 제5호서식]

개인정보파일 파기 관리대장

번호	개인정보 파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장

붙임12 **통제구역 출입자 명부**

통제구역 출입자 명부

일 자	출입 시간	퇴실 시간	방문목적	출입자		입 회 자		비 고
				소속(주소)	성 명	직 급	성명	

보조기억매체 반 · 출입 대장

일 자	목 적	반 · 출입 세부내역	소 지 자		정보보호담당		관 리 자	
			소속(주소)	성 명	직 급	성명	직 급	성명

붙임14 개인영상정보 관리대장

표준개인정보보호지침 [별지 제3호서식]

개인영상정보 관리대장

번호	구분	일시	파일명/형태	담당자	목적/사유	이용·제공받는 제3자/열람등 요구자	이용·제공 근거	이용·제공 형태	기간 및 파기예정일자	파기 등 결과 및 처리일자	안전관리 요청 및 결과
1	□ 이용 □ 제공 □ 열람 □ 파기										
2	□ 이용 □ 제공 □ 열람 □ 파기										
3	□ 이용 □ 제공 □ 열람 □ 파기										
4	□ 이용 □ 제공 □ 열람 □ 파기										
5	□ 이용 □ 제공 □ 열람 □ 파기										
6	□ 이용 □ 제공 □ 열람 □ 파기										

붙임15 개인영상정보 청구서

표준개인정보보호지침 [별지 제2호서식]

개인영상정보(☐ 존재확인 ☐ 열람) 청구서 ※ 아래 유의사항을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다.				처리기한 10일 이내
청구인	성명		전화번호	
	생년월일		정보주체와의 관계	
	주소			
정보주체의 인적사항	성명		전화번호	
	생년월일			
	주소			
청구내용 (구체적으로 요청하지 않으면 처리가 곤란할 수 있음)	영상정보 기록기간	(예 : 2026.01.01 18:30 ~ 2026.01.01 19:00)		
	영상정보 처리기기 설치장소	(예 : 00시 00구 00대로 0 인근 CCTV)		
	청구 목적 및 사유			

「표준 개인정보 보호지침」 제44조에 따라 위와 같이 개인영상정보의 존재확인, 열람을 청구합니다.

년 월 일

청구인 (서명 또는 인)

서울특별시양천구시설관리공단이사장 귀하

담당자의 청구인에 대한 확인 서명	

붙임16 개인정보 열람 / 정정·삭제 / 처리정지 요구서

■ 개인정보 보호법 시행규칙 [별지 제8호서식]

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」 제35조제1항·제2항, 제36조제1항 또는 제37조제1항과 같은 법 시행령 제41조제1항, 제43조제1항 또는 제44조제1항에 따라 위와 같이 요구합니다.

년 월 일

요구인 (서명 또는 인)

서울특별시양천구시설관리공단이사장 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.

210㎜×297㎜[일반용지 70g/㎡(재활용품)]

붙임17 위 임 장

■ 개인정보 처리 방법에 관한 고시 [별지 제11호서식]

위 임 장

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

「개인정보 보호법」 제38조제1항에 따라 위와 같이 개인정보의 (☐ 열람, ☐ 정정 · 삭제, ☐ 처리정지)의 요구를 위의 자에게 위임합니다.

년 월 일

위임자

(서명 또는 인)

서울특별시양천구시설관리공단이사장 귀하

붙임18 개인정보 열람 / 일부열람 / 열람연기 / 열람거절 통지서

■ 개인정보 보호법 시행규칙 [별지 제9호서식]

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

<table>
<tr><td colspan="4">수신자 (우편번호: , 주소:)</td></tr>
<tr><td>요구 내용</td><td colspan="3"></td></tr>
<tr><td>열람 일시</td><td colspan="2"></td><td>열람 장소</td></tr>
<tr><td>통지 내용
[ ] 열람
[ ] 일부열람
[ ] 열람연기
[ ] 열람거절</td><td colspan="3"></td></tr>
<tr><td rowspan="2">열람 형태 및 방법</td><td>열람 형태</td><td colspan="2">[ ]열람・시청 [ ]사본・출력물 [ ]전자파일 [ ]복제물・인화물 [ ]기타</td></tr>
<tr><td>열람 방법</td><td colspan="2">[ ]직접방문 [ ]우편 [ ]팩스 [ ]전자우편 [ ]기타</td></tr>
<tr><td rowspan="2">납부 금액</td><td>①수수료 원</td><td>②우송료 원</td><td>계(①+②) 원</td></tr>
<tr><td colspan="3">수수료 산정 명세</td></tr>
<tr><td>사 유</td><td colspan="3"></td></tr>
<tr><td>이의제기방법</td><td colspan="3">※ 개인정보처리자는 이의제기방법을 적습니다.</td></tr>
</table>

「개인정보 보호법」 제35조제3항・제4항 또는 제5항과 같은 법 시행령 제41조제4항 또는 제42조제2항에 따라 귀하의 개인정보 열람 요구에 대하여 위와 같이 통지합니다.

년 월 일

서울특별시양천구시설관리공단이사장 직인

붙임19 개인정보 정정·삭제 / 처리정지 요구에 대한 결과 통지서

■ 개인정보 보호법 시행규칙 [별지 제4호서식]

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」 제36조제6항 및 같은 법 시행령 제43조제3항 또는 같은 법 제37조제5항 및 같은 법 시행령 제44조제2항에 따라 귀하의 요구에 대한 결과를 위와 같이 통지합니다.

년 월 일

서울특별시양천구시설관리공단이사장 직인

유의사항

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

붙임20 개인정보 유출신고서

표준개인정보보호지침 [별지 제8호서식]

개인정보 유출신고서

<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 colspan="6"></td></tr>
<tr><td rowspan="2">유출신고접수기관</td><td colspan="2">기관명</td><td colspan="2">담당자명</td><td>연락처</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td></td></tr>
</table>

붙임21 **개인정보 침해신고 처리대장**

개인정보 침해신고 처리대장

접 수		신 고 개 요	처리결과	결 재	
일 시	신 고 인 인적사항			담당자	부서장

붙임22 연계정보 수집 현황 기록대장

연계정보 수집 현황 기록대장

(분기별 작성 / 연계정보 값은 기록하지 않음 / 보관기간 1년 이상)

연번	기 간	수집 출처 (본인확인기관)	건수	수집 목적	수집 대상 / 세부 기록 위치	연계정보 처리	확인자 (확인일)
예시	2026. 1. 1. ~ 3. 31.	한국모바일인증㈜ (KMC)	○○○건	회원가입 본인인증	신규 가입 회원 / 회원 DB MEMBER	이용·저장 하지 않음	한양규 (26.10.○)
1							
2							
3							
4							
5							

※ 작성 방법

- 분기 종료 후 유지보수 업체에 해당 분기 본인인증 건수 조회를 요청하여 1줄씩 기록
  (분기별 연계정보취급자 검토 시 함께 작성)
- 건수 : 해당 기간 홈페이지 회원가입 휴대폰 본인인증 건수(회원 DB 기준, 조회 시점 탈퇴 회원 제외)
- 회원별 상세 내역(본인인증 일시·회원번호)은 회원 DB에 회원 탈퇴 시까지 보관되므로 대장에는 합계만 기재

붙임23 연계정보취급자 지정 현황

연계정보취급자 지정 현황

연번	구분	소속	직급	성명	담당업무	지정일	분기 검토일 (확인)
예시	*보호책임자*				*연계정보 안전조치 총괄*	*개정안 결재일*	
예시	*보호담당자*				*연계정보 안전조치 실무, 홈페이지 관리*		
예시	*취급자 (수탁자)*				*홈페이지 본인인증 연동 기능 유지보수*		

※ 작성 방법

- 구분 : 보호책임자(본부장), 보호담당자(개인정보 보호담당자), 취급자(홈페이지 본인인증 연동 기능을 운영·관리 하는 직원 및 수탁업체 담당자)
- 공단은 연계정보를 저장하지 않아 연계정보를 조회하는 직원은 없으며, 시스템 관리자만 취급자로 지정
- 분기 검토일 : 분기마다 인사이동·퇴직·업체 담당자 변경 여부를 확인하고 날짜와 확인자 서명 기재, 변경 시행 추가·삭제(제43조⑤⑥)