
개인정보 처리시스템 접근권한 관리지침

2026. 9.



양천구시설관리공단

제 · 개정 이력서

[illegible]

[목 차]

제 1 장 총 칙	1
1. 목적	1
2. 적용 범위	1
3. 관련 근거	1
4. 용어 정의	1
5. 기본 원칙	2
제 2 장 접근권한 관리 조직	2
1. 접근권한 관리 조직구성	2
2. 권한관리 책임자의 역할	2
3. 권한관리 담당자의 역할	3
4. 권한관리 부서책임자의 역할	3
5. 권한관리 부서담당자의 역할	3
제 3 장 접근권한 부여 기준 및 관리절차	4
1. 접근권한 부여 원칙 및 기준	4
2. 접근권한 신청	4
3. 접근권한 심사	4
제 4 장 개인정보취급자 계정 발급기준, 공유금지, 부여·말소 절차	5
1. 개인정보 취급자 계정 발급기준	5
2. 계정 공유금지	5
3. 계정 부여·말소 절차	5
제 5 장 이용자 권한관리의 안전성·보안성 확보	6
1. 이용자 정보 관리	6
2. 접근권한 점검 및 관리	6
3. 이용내역 기록	6
4. 이용기록의 보관	7
5. 보안조치	7
6. 준용	8
[별표 제1호] 개인정보보호 조직구성 및 개인정보처리시스템 접근권한 부여 기준	8
[별지 제1호 서식] 정보보안 서약서	9
[별지 제2호 서식] 사용자 권한 생성/변경 신청서	10
[별지 제3호 서식] 개인정보처리시스템 접근권한 관리 대장	11
[별지 제4호 서식] 개인정보취급자·시스템관리자 보안 서약서	12

제 1 장 총 칙

1. 목 적

이 지침은 양천구시설관리공단(이하 “공단”이라 한다)에서 운영 중인 개인정보처리시스템을 구축·운영 또는 이용함에 있어 접근권한의 오·남용을 통한 개인정보의 유·노출을 방지하고 개인정보를 보호하는데 필요한 사항을 규정하여 정보주체 등의 권리를 보호하려는데 목적이 있다.

2. 적용 범위

이 지침은 공단 임직원 및 관련 법령 등에 따라 공단 사무의 일부 또는 전부를 위탁 또는 대행하여 운영하는 자를 적용 대상으로 한다.

3. 관련 근거

가. 「개인정보보호법」 및 「개인정보보호법 시행령」

나. 「표준 개인정보 보호지침」(개인정보보호위원회 고시 제2025-4호)

다. 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회고시 제2026-9호, 2026.7.1. 시행)

4. 용어 정의

가. “개인정보처리시스템”이란 개인정보의 수집, 가공, 저장, 검색, 송신, 수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 말한다.

나. “개인정보처리시스템 이용자(이하 ”이용자“라 한다)”란 전자적 행정업무를 하는 업무담당자, 서비스를 이용하는 서비스 이용자 및 시스템 관리자를 말한다.

다. “업무담당자”란 개인정보처리시스템을 통하여 행정업무를 담당하는 사람을 말함.

라. “서비스이용자”란 개인정보처리시스템을 이용하는 주체로서 행정업무를 다루지 않는 사람을 말한다.

마. “시스템관리자”란 개인정보처리시스템의 원활한 수행을 위하여 개인정보처리시스템을 운영·관리하는 사람을 말한다.

바. “본인확인”이란 개인정보처리시스템을 통하여 업무담당자 또는 시스템 관리자가 가지고 있거나 알고 있는 정보를 이용하여 본인임을 확인하는 것을 말한다.

사. “접근권한”이란 개인정보처리시스템에 접속하여 개인정보를 활용할 수 있는 권한과 개인정보를 판독(read), 기록(write), 실행(execution) 등 디렉토리나 파일에 대해 사용자가 접근 및 수행할 수 있는 작업 권한을 말한다.

아. “행정정보”란 직무상 작성 또는 취득하여 관리하고 있는 자료를 말한다.

자. “개인정보”란 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.

차. “안전한 인증수단”이란 인증서, 보안토큰, 일회용 비밀번호(OTP) 등 아이디·비밀번호 외에 정당한 권한을 가진 자임을 추가로 확인할 수 있는 인증수단을 말한다.

※ 이외 용어의 정의는 「개인정보 보호법」 제2조(정의) 참조

5. 기본 원칙

- 가. 공단은 개인정보처리시스템을 통하여 행정정보 처리업무 등을 진행하는 과정에서 얻은 개인정보는 적절한 절차를 통해 보호하여야 한다.
- 나. 공단은 개인정보처리시스템에 보유 중인 행정정보를 서비스 제공 목적과 이에 수반되는 지원 업무에 한해 사용하여야 한다.
- 다. 공단은 고유 목적 외에 개인정보처리시스템에 보유 중인 행정정보를 사용하기 위해서는 정보주체의 동의를 얻거나 법률에서 허용하는 근거가 있는 경우에 한해 사용할 수 있다.
- 라. 공단은 개인정보처리시스템을 통한 업무 수행을 위하여 개인정보처리시스템에 접근하고자 하는 이용자에게 본인확인 및 접근권한 확인 절차를 반드시 거치도록 하여야 한다.

제 2 장 접근권한 관리 조직

1. 접근권한 관리 조직구성

공단의 효율적이고 체계적인 접근권한 관리를 위하여 접근권한 관리 조직체계를 구성 및 운영하며, 다음 각 호에 임명된 자는 보직에 임명과 동시에 접근권한 관리 조직 구성원으로 임명된 것으로 간주한다.

- 가. 권한관리 책임자 : 개인정보보호 책임자(CPO)
- 나. 권한관리 담당자 : 개인정보보호 담당자
- 다. 권한관리 부서책임자 : 각 팀(관)장(중간관리자)
- 라. 권한관리 부서담당자 : 각 팀의 개인정보보호담당자

2. 권한관리 책임자의 역할

공단 개인정보처리시스템의 사용자 계정 등록, 권한 부여, 계정 권한의 적정 관

리에 대해 다음 각 호를 업무를 수행하여야 한다.

- 가. 이용자 접근권한 관리 업무의 총괄
- 나. 이용자 접근권한 관리와 관련된 기능의 구현
- 다. 이용자 접근권한 부여의 기준 및 절차 수립
- 라. 이용자 등록·관리 및 접근부여 여부의 관리·감독 등

3. 권한관리 담당자의 역할

공단 개인정보처리시스템의 사용자 계정 등록, 권한 부여, 계정 권한의 적정성 수행을 위하여 다음 각 호를 업무를 수행하여야 한다.

- 가. 권한관리 책임자의 위임 업무 수행
- 나. 권한관리 부서책임자 및 부서의 개인정보처리시스템 운영 실태 관리 감독
- 다. 개인정보처리시스템 기술적·관리적·물리적 안전성 확보 조치 수행
- 라. 개인정보처리시스템 이용 내역에 대한 기록의 사후 점검 및 확인
- 마. 개인정보처리시스템 이용 내역과 관련된 자료의 보관 및 주기적 백업 등 관리 등

4. 권한관리 부서책임자의 역할

공단 개인정보처리시스템의 행정정보의 등록, 권한 부여, 계정 권한의 적정성 확인을 위하여 다음 각 호를 업무를 수행하여야 한다.

- 가. 행정정보의 사용권한 부여, 관리 및 감독
- 나. 행정정보의 타 부서 사용자 권한 부여 모니터링 실시
- 다. 행정정보의 등록, 변경, 파기처리 관리 및 감독
- 라. 부서 개인정보처리시스템 이용 내역에 대한 사후 점검 및 확인
- 마. 기타 권한관리를 위해 필요한 사항 등

5. 권한관리 부서담당자의 역할

공단 개인정보처리시스템의 관장업무 행정정보의 권한 부여, 계정 권한의 적정성 확인을 위하여 다음 각 호를 업무를 수행하여야 한다.

- 가. 개인정보 취급자의 권한관리 지도·감독
- 나. 부서 이용자 권한관리 규정 준수 점검
- 다. 부서 이용자 권한관리 위법·부당한 권한 부여 점검
- 라. 부서 개인정보처리시스템 이용 의견 수렴 및 불만사항 접수
- 마. 기타 권한관리를 위해 필요한 사항 등

제 3 장 접근권한 부여 기준 및 관리절차

1. 접근권한 부여 원칙 및 기준

가. 개인정보처리시스템의 접근, 개인정보 열람 등 모든 접근권한은 규정에 따라 허용된 자에 한하여 업무수행에 필요한 최소한의 범위로 부여하여야 한다.

구분	개인정보처리시스템 명	내 용	유지보수 업체
1	문화·체육 회원관리 시스템	문화체육 회원관리프로그램	혁신정보시스템
2	주차관리 시스템	주차 및 견인 관련 프로그램	세인소프트

나. 사용자 계정 발급 시 사용자별 한 개의 계정을 발급하여야 한다.

다. 접근권한을 부여받은 이용자는 접근권한을 임의로 양도, 대여해서는 안 되며, 접근권한 책임자는 이를 수시로 확인 및 지도·감독하여야 한다.

라. 책임자는 [별표 제1호]에 따라 **이용자별 업무 특성에 따른** 접근권한 차등 및 부여 기준을 마련하여야 한다.

마. **정당한 권한을 가진 개인정보처리시스템 이용자(서비스이용자는 제외한다)가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서·보안토큰·일회용 비밀번호(OTP) 등 안전한 인증수단을 적용하여야 한다.**

2. 접근권한 신청

가. 개인정보처리시스템을 이용하고자 하는 업무담당자, 시스템 관리자 및 외주 직원 등은 다음 각 호를 기재한 [별지 제2호 서식]의 “사용자 권한 생성/변경 신청서” 및 [별지 제1호 서식]의 “보안서약서”를 작성하여 해당 권한관리 부서 책임자의 결재를 받아 접근권한을 부여하여야 한다.

- ① 개인정보처리시스템 또는 행정정보의 이용 또는 활용 목적 및 근거(신청사유)
- ② 이용 또는 활용하고자 하는 개인정보처리시스템 또는 행정정보의 활용범위 (접근권한)

나. 각 팀(관)장은 다른 부서에서 보유 중인 행정정보를 이용하는 경우, 이용하고자 하는 정보의 범위를 명시하여 행정정보를 보유부서의 권한관리 부서책임자에게 다음 각 호의 사항을 작성하여 문서로 요청하여야 한다.

- ① 개인정보처리시스템 또는 행정정보의 이용 또는 활용 목적 및 근거(신청사유)
- ② 이용 또는 활용하고자 하는 개인정보처리시스템 또는 행정정보의 활용범위 (접근권한)
- ③ 행정정보의 제공방식, 보관기간 및 안전관리대책 등

3. 접근권한 심사

가. 접근권한 부서책임자는 접근권한 부여 기준에 따라 다음 각 호의 사항을 심

사하여 최소한의 접근권한을 부여하여야 하며, 개인정보처리시스템의 주요 행정정보에 대한 접근권한은 접근권한 심사위원회를 구성하여 접근권한을 심사할 수 있다.

- ① 개인정보처리시스템 또는 행정정보의 이용 또는 활용목적의 정당성
- ② 개인정보처리시스템 또는 행정정보의 이용 범위의 적정성
- ③ 신청내용의 타당성, 적합성, 공익성

나. 행정정보 보유 부서책임자는 보유하고 있는 행정정보를 그 부서의 내부 또는 다른 부서에서 이용하게 하고자 하는 경우에는 업무수행에 필요한 최소한의 범위로 이용하게 하여야 한다.

다. 권한관리 책임자는 접근권한 부서책임자가 이용자의 접근권한 부여 승인 내역을 관리·감독하여야 한다.

제 4 장 개인정보취급자 계정 발급기준, 공유금지, 부여·말소 절차

1. 개인정보 취급자 계정 발급기준

가. 개인정보처리시스템의 접근, 개인정보 열람 등 모든 접근권한은 규정에 따라 업무수행에 필요한 최소한의 범위로 부여하여야 한다.

구분	개인정보처리시스템 명	내 용	유지보수 업체
1	문화·체육 회원관리 시스템	문화체육 회원관리프로그램	혁신정보시스템
2	주차관리 시스템	주차 및 견인 관련 프로그램	세인소프트

나. 취급자 계정 발급 시 사용자별 한 개의 계정을 발급하여야 한다.

다. 접근권한을 부여받은 취급자는 접근권한을 임의로 양도, 대여해서는 안 되며, 접근권한 책임자는 이를 수시로 확인 및 지도·감독하여야 한다.

라. 책임자는 [별표 제1호]에 따라 **이용자별 업무 특성에 따른** 접근권한 차등 및 부여 기준을 마련하여야 한다.

2. 계정 공유금지

취급자는 개인정보처리시스템 또는 행정정보에 접근할 때 사용하는 사용자계정(ID) 등 이용자 본인확인에 필요한 정보를 타인과 공유하지 않고 안전하게 관리하여야 한다.

3. 계정 부여·말소 절차

가. 개인정보취급자는 [별지 제2호 서식] “사용자 권한 생성/변경 신청서” 및 [별지

제1호 서식]의 “보안서약서”를 작성하여 해당 권한관리 부서책임자의 결재를 받아 접근권한을 부여·말소하여야 한다.

나. 접근권한 부서책임자는 접근권한 부여·말소기준에 따라 다음 각 호의 사항을 심사하여 최소한의 접근권한을 부여하여야 하며, 개인정보처리시스템의 주요 행정정보에 대한 접근권한은 접근권한 심사위원회를 구성하여 접근권한을 심사할 수 있다.

- ① 개인정보처리시스템 또는 행정정보의 이용 또는 활용 목적의 정당성
- ② 개인정보처리시스템 또는 행정정보의 이용 범위의 적정성
- ③ 신청내용의 타당성, 적합성, 공익성

제 5 장 이용자 권한관리의 안전성·보안성 확보

1. 이용자 정보 관리

가. 권한관리 책임자는 이용자 등록 내역을 주기적으로 점검하여 부적절한 이용자의 접근권한을 삭제하는 등 필요한 조치를 하여야 한다.

나. 이용자는 개인정보처리시스템 또는 행정정보에 접근할 때 사용하는 사용자계정(ID) 등 이용자 본인확인에 필요한 정보를 타인과 공유하지 않고 안전하게 관리하여야 한다.

2. 접근권한 점검 및 관리

가. 조직개편·인사발령·업무분장의 변경 등으로 업무담당자의 접근권한을 변경해야 할 경우, 권한관리 책임자는 그 변경된 인사 내용에 따라 지체 없이 접근권한을 변경하여야 한다.

나. 권한관리 책임자는 소관 개인정보처리시스템 및 행정정보에 대해서 접근권한 관리의 적절성 및 접근권한의 오·남용 여부를 주기적으로 점검하여야 한다.

다. 권한관리 책임자는 접근권한 및 접속기록에 대한 점검을 월 1회 이상 실시함을 원칙으로 하되, 개인정보처리시스템의 위험도·처리량 등을 고려하여 권한관리 책임자의 승인을 받아 점검 주기를 달리 정할 수 있다.

3. 이용내역 기록

가. 개인정보를 생성·수정·삭제·열람 등을 하고자 하는 경우 다음 사항을 포함하는 정보이용 내역을 기록하고 남길 수 있도록 개인정보처리시스템 구축·운영하여야 한다.

- ① 이용자 접근 기록 및 이용 시간

- ② 이용자 식별 정보
- ③ 이용자가 생성·변경·열람·삭제한 행정정보의 내용 및 사유
- ④ 시스템 관리자가 생성·변경·열람·삭제한 정보의 내용 및 사유
- ⑤ 그 밖에 접근권한의 오·남용 및 정보 유출 여부를 검증하기 위해 필요하다고 판단되는 정보

4. 이용기록의 보관

- 가. 공단은 권한 부여, 변경 또는 말소에 대한 내역을 [별지 제3호 서식] “개인정보처리시스템 접근권한 관리 대장”에 기록하고 그 기록을 최소 3년간 보관하여야 한다.
- 나. 공단은 이용내역에 대한 기록이 변경되거나 삭제될 수 없도록 시스템을 구축하고 책임자의 사전 승인 없이 시스템 관리자 외에는 접근할 수 없도록 하여야 한다.

5. 보안조치

- 가. 공단은 사용자가 개인정보처리시스템 등에 접속한 기록을 최소 2년 이상 보관·관리하여야 한다.
 - ① 시스템사용자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관
- 나. 공단은 개인정보처리시스템 등에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 한다.
 - ① 보안 프로그램의 자동 업데이트 기능을 사용하거나 또는 일 1회 이상 업데이트 실시
 - 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
- 다. 공단은 업무용 컴퓨터 등에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램 설치·운영토록 관리하여야 한다.
 - ① 보안 프로그램의 자동 업데이트 기능을 사용하거나 또는 일 1회 이상 업데이트 실시 및 윈도우 주기적인 업데이트 실시
- 라. 공단은 이용자가 일정 횟수 이상 인증에 실패하는 경우 해당 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하여야 한다.
- 마. 공단은 개인정보를 출력·복사하는 경우 출력·복사물에 대한 관리(관리대장 작성, 마스킹, 수량 제한 등)로 안전하게 관리하여야 하며, 보유기간이 경과하거나 처리 목적을 달성한 개인정보는 지체 없이 파기하여야 한다.

6. 준용

동 지침에 기술되지 않은 사항에 대해서는 「개인정보 보호법」, 개인정보보호위원회 「표준 개인정보 보호 지침」 및 「개인정보의 안전성 확보조치 기준」을 준용한다.

[별표 제1호] 개인정보보호 조직구성 및 개인정보처리시스템 접근권한 부여 기준(개정 2026.09.)



개인정보처리 시스템명		권한관리 책임자	권한관리 담당자	분야별 책임자	업무	접근권한
문화·체육 회원관리 시스템	문화·체육 회원관리 시스템	본부장 (CPO)	개인정보보호 담당자	팀(관)장	회원관리 업무 총괄	회원관리업무 (생성, 읽기, 정정, 삭제) 타 부서 접근권한 판단 및 점검
	홈페이지 관리자 페이지				홈페이지 관리자 페이지 업무 총괄	홈페이지 관리자 페이지 업무 (생성, 읽기, 정정, 삭제) 타 부서 접근권한 판단 및 점검
주차관리 시스템						주차관리팀장

정보보안 서약서

양천시설관리공단의 직원은 본 서약서가 근무기간뿐 아니라 퇴직 후에도 일정기간 적용될 수 있음을 인식하고 숙독하신 후 서명하여 주시기 바랍니다.

1. 본인은 업무 중에 알게 된 개인정보에 대하여 공단에 재직 중 또는 퇴직 후에도 비밀을 지킬 것이다.
(‘개인정보’와 관련한 용어의 정의는 개인정보보호법에서 정의된 바에 따름)
2. 본인은 정당한 절차 없이 공단의 개인정보가 포함된 파일을 무단으로 소유·출력 또는 제3자에게 유출하지 않을 것이다.
3. 본인은 공단로부터 제공받은 정보자산(서류, 사진, 전자파일, 저장매체(HDD 등), 전산 장비 등)을 무단변조, 복사, 훼손, 정보유실 등으로부터 안전하게 관리할 것이다.
4. 본인은 명백히 허가받지 않은 정보나 시설에 접근하지 않으며, 공단 관련 업무를 수행 할 때만 데이터 처리 시설을 이용하고, 이 시설 내에 사적 정보를 보관치 않겠다.
5. 관련법과 공단 규정에서 정하는 개인정보보호 및 보안에 관한 내용을 준수할 것이다.

본인은 상기사항을 숙지하여 이를 성실히 준수할 것에 동의하며, 위 사항을 위배하였을 경우에는 관련 법령 및 규정에 의거하여 어떠한 책임도 감수할 것이며 공단에 끼친 손해에 대해 변상·복구할 것을 서약합니다.

20 년 월 일

상기 서약자

소 속 :

직 급 :

성 명 : (인)

양천구시설관리공단 이사장 귀하

※ 본 서약서는 부서에서 보관 및 관리합니다.

※ 본 서약서를 첨부해서 공문으로 혁신성과팀으로 통보합니다.

사용자 권한 생성/변경 신청서

부서명			
이 름		직 급	
전화번호	(0) -	이메일	
접근권한 (별첨1 참조)	※ 해당 업무의 상세 프로그램에 대한 필요한 권한(생성, 읽기, 정정, 삭제권한)을 명기해 주시기 바랍니다.		
신청사유			
위와 같이 정보시스템 사용자 권한의 ☐ 생성, ☐ 변경, ☐ 삭제를 신청합니다. 년 월 일 신청자 : 부서책임자 : (인) 또는 서명 (인) 또는 서명			

※ 본 권한신청서는 사용자 권한관리 부서에서 보관 및 관리합니다.

※ 본 권한신청서를 첨부해서 공문으로 혁신성과팀으로 통보 합니다.

