
재해·재난 대비 개인정보처리시스템 위기 대응 지침

2026. 7.



양천구시설관리공단

제 · 개정 이력서

[illegible]

[목 차]

제 1 장 총 칙	1
1. 목적	1
2. 관련근거	1
3. 대상 및 적용범위	1
4. 용어정의	2
 제 2 장 위기대응 절차	 3
1. 절차개요	3
2. 단계별 정의	3
 제 3 장 위기대응 체계	 4
1. 위기대응 조직의 구성	4
2. 위기등급의 분류	7
3. 복구목표의 설정	8
4. 백업관리	9
5. 위기대응 훈련	10
6. 비상연락망 구성	10
 [별지 제1호] 백업 관리대장	 11
[별지 제2호] 양천구시설관리공단 개인정보보호 세부 인원 현황	12
[별지 제3호] 공단 비상연락망(별첨)	

제 1 장 총 칙

1. 목적

지진, 화재, 풍수해, 단전, 통신장애, 사이버공격 등 재해·재난으로 개인정보처리 시스템의 가용성·무결성·기밀성이 훼손되거나 훼손될 우려가 있는 경우, 양천구시설관리공단(이하 “공단”이라 한다)이 신속하게 상황을 통제하고 개인정보의 유출 등을 방지하며 핵심 서비스를 복구하기 위한 조직, 절차 및 최소 조치기준을 정하는 것을 목적으로 한다.

2. 관련근거

- 가. 개인정보보호법 제12조(개인정보 보호지침), 제29조(안전조치의무), 제31조(개인정보 보호책임자의 지정), 제34조(개인정보 유출 등의 통지·신고)
- 나. 「개인정보 보호법 시행령」 제30조(개인정보의 안전성 확보 조치), 제39조(개인정보 유출 등의 통지), 제40조(개인정보 유출 등의 신고) [2026. 5. 19. 시행]
- 다. 「개인정보의 안전성 확보조치 기준」 제4조, 제8조, 제10조 및 제11조 [개인정보보호위원회고시 제2026-9호, 2026. 7. 1. 시행]
- 라. 「표준 개인정보 보호지침」 [개인정보보호위원회고시 제2025-4호, 2025. 4. 11. 시행]

3. 대상 및 적용범위

- 가. 개인정보를 전자적으로 저장·처리·전송하는 모든 시스템, 데이터베이스, 서버, 네트워크, 클라우드, 저장장치 및 관련 보안장비
- 나. 적용범위
 - 이 지침은 재해·재난, 단전, 통신장애, 사이버공격 및 이에 준하는 사고 발생 시 개인정보처리시스템과 관련 장비의 예방·대응·복구 및 복원 업무에 적용한다.
 - 개인정보처리시스템, 데이터베이스, 영상정보 저장장치, 백업매체 및 관련 정보 보호시스템의 백업·복구와 위기대응 조치에 적용한다.
 - 비전자적 개인정보 문서는 침수·화재·도난 방지를 위한 안전한 보관, 대피 및 복구 조치를 적용한다.

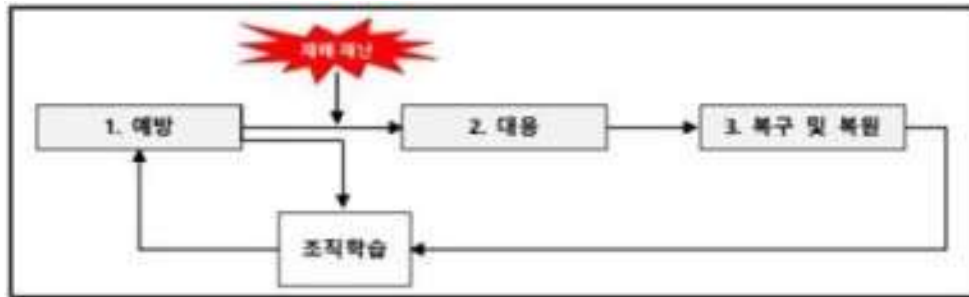
4. 용어 정의

- 가. 재해·재난 : 태풍, 홍수, 지진, 낙뢰 등 자연현상과 화재, 붕괴, 폭발, 단전, 침수, 통신두절, 사이버공격 등으로 정보시스템 또는 업무에 중대한 영향을 줄 수 있는 사고
- 나. 개인정보처리시스템 : 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템
- 다. 위기 : 개인정보처리시스템이 중단되거나 개인정보가 분실·도난·유출·위조·변조 또는 훼손되었거나, 정해진 복구목표를 초과할 가능성이 있는 상태
- 라. 재해복구(DR) : 주센터 장애 시 대체 환경에서 시스템과 데이터를 복구·운영하기 위한 체계
- 마. 백업 : 원본 데이터의 손실·훼손에 대비하여 별도 매체 또는 별도 환경에 생성한 복사본
- 바. 격리 : 감염, 공격 또는 오류의 확산을 방지하기 위하여 시스템·계정·단말기를 네트워크 또는 서비스로부터 분리하는 조치

제 2 장 위기대응 절차

1. 절차 개요

가. 개인정보처리시스템의 위기 발생 시 예방, 대응, 복구 및 복원으로 이루어지는 3가지 단계를 체계적으로 구조화해야 함



〈위기대응 절차 예시〉

2. 단계별 정의

가. 1단계 : 예방

- 위기 상황이 발생하기 전 예상되는 문제들을 미리 보완하고 대비
- 위기대응 조직, 위기등급, 복구목표 등 위기대응 체계 검토
- 주기적 백업 실시 및 위기대응 훈련 실시를 통해 위기대응 준비

나. 2단계 : 대응

- 재해·재난으로 위기 상황이 발생하여 위기대응 체계에 따라 대응 실시
- 위기대응 조직을 소집하고 위기 등급을 정의하여 위기상황 선포
- 비상연락체계를 가동하고 위기대응 조직의 역할에 따라 대응 실시

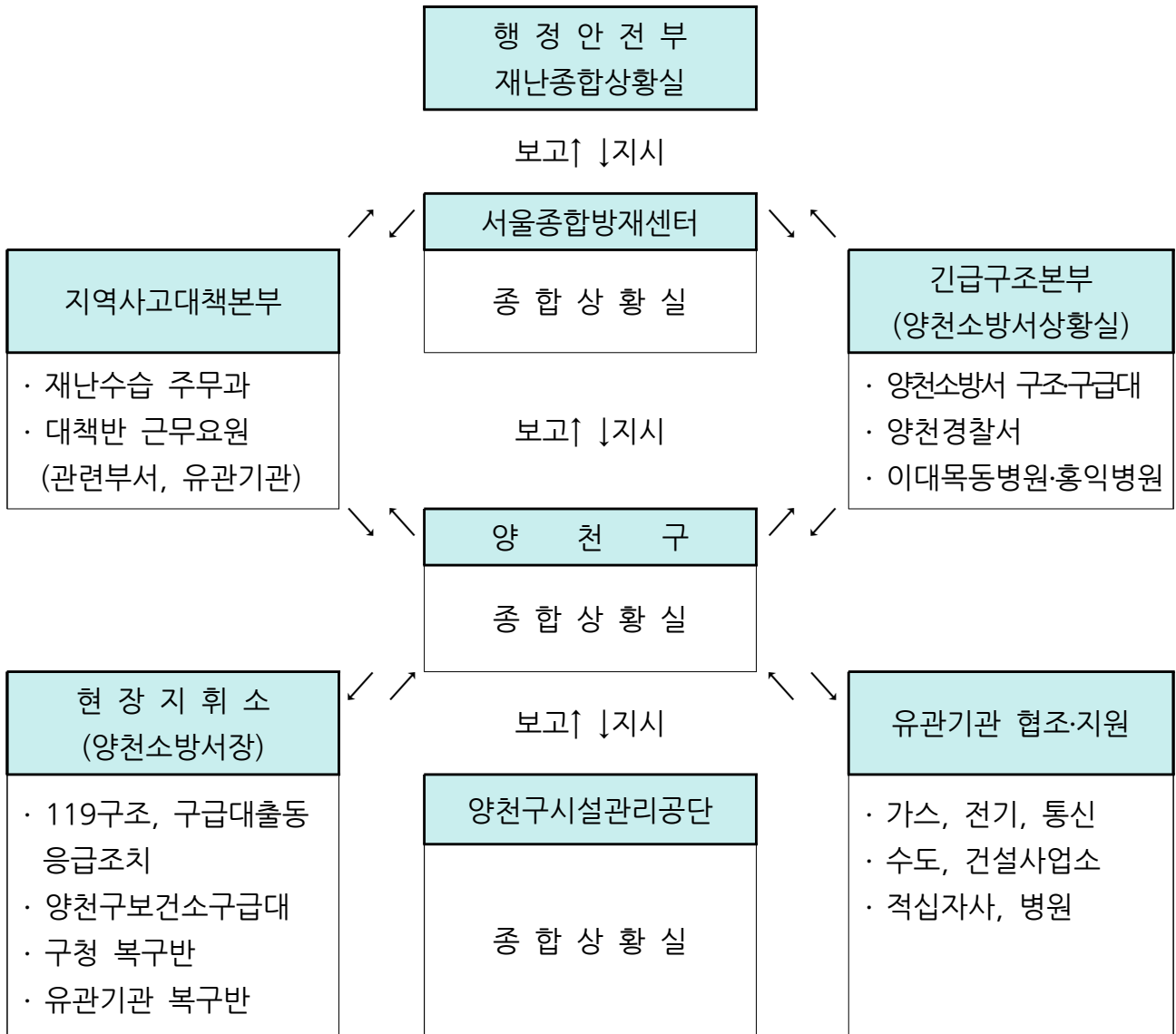
다. 3단계 : 복구 및 복원

- 복구목표에 따라 우선순위가 높은 업무부터 복구 및 복원 실시
- 복구 및 복원이 완료되면 위기 상황의 종료를 선언하고 위기대응 시 이슈사항을 위기대응 체계에 반영하여 개선
- 위기상황으로 인한 피해를 수습하고 위기내용 학습

제 3 장 위기대응 체계

1. 위기대응 조직의 구성

가. 양천구 재해·재난 종합상황관리 체계도



나. 운영시기 : 사업장 재해 발생 시 또는 개인정보 보호책임자 또는 대응총괄이

필요하다고 판단하여 소집하는 경우

다. 기 능 : 재해 상황 조사 및 재해복구에 관한 총괄 조정

- 양천구 사고대책본부, 관련기관(안전재난과 등 긴밀한 공조체제 유지 및 상호 인력장비 협조
- 관계기관 등에 대한 상황 전파 및 수습, 복구, 지원업무 수행

라. 양천구시설관리공단 개인정보처리시스템 재해·재난 대책본부의 구성



마. 조직에 따른 업무분장

구 분	담 당	행위자(직위·역할)	비 고
대책 본부장	개인정보 보호책임자(CPO)	본부장	02-2061-3413
대응 총괄	침해사고 대응 총괄	혁신성과팀장	02-2061-3414
간사	전산 및 개인정보보호 총괄 담당자	개인정보 보호실무자	02-2061-3414
침해사고 처리책임자	침해사고 발생한 팀 및 센터	팀장 및 관장	-
시스템운영자	유지보수업체	시스템 실무자/ 유지보수 업체	-
안전감사팀	개인정보보호 담당자	사업장 담당자	02-2061-3416
경영지원팀	개인정보보호 담당자	사업장 담당자	02-2061-3413
주차관리팀	개인정보보호 담당자	사업장 담당자	02-2644-1385~6
공공시설관리팀	개인정보보호 담당자	사업장 담당자	02-2061-3436
양천센터	개인정보보호 담당자	사업장 담당자	02-2652-1792
신월센터	개인정보보호 담당자	사업장 담당자	02-2605-4093
목동센터	개인정보보호 담당자	사업장 담당자	02-2062-1862

바. 업무분장 및 행동 요령

단 계	주 요 업 무	행 위 자
사고인지 및 긴급조치	■ 개인정보 유출사고 신고 접수 및 사고인지 - 유출부서는 지체 없이 개인정보보호 담당자에게 신고 - 개인정보보호 담당자는 책임자에게 사고내용 등 보고 ■ 유출사고 신속대응팀 구성 및 유관기관 협조체계 확인 ■ 피해 최소화를 위한 긴급조치 수행 - 노출 페이지 및 외부 접근경로 차단, 관련 계정 정지 또는 비밀번호 초기화 - 접속기록, 보안장비 로그, 시스템 이미지 및 사고 관련 자료의 증거보전 - 유지보수업체 및 정보보호 전문기관에 기술지원 요청 - 감염 또는 침해가 의심되는 시스템·단말기·계정을 네트워크 및 서비스로부터 격리	개인정보 유출 부서장/전직원 개인정보보호책임자 /담당자
↓		
개인정보 침해사고 대응팀 구성	■ 노출 및 제공된 정보의 종류에 따라 분야별 책임자를 처리 책임자로 지정 ■ 개인정보 침해사고 대응팀 구성 및 운영 - 개인정보 침해사고 발생 시 개인정보 보호책임자는 침해사고 처리책임자 및 대응총괄과 협의하여 사고대응팀의 구성과 대응범위를 결정한다.	개인정보 유출 부서장 개인정보보호 책임자
↓		
정보주체 유출통지 및 개인정보 유출신고	■ 1건이라도 유출 시, 정보주체에게 개인정보 유출 사실 통지 (72시간 이내) - 유출된 개인정보의 항목, 유출된 시점, 피해 구제 절차 등 ■ 다음 어느 하나에 해당하면 72시간 이내에 개인정보보호위원회 또는 한국인터넷진흥원에 신고 - 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우 - 민감정보 또는 고유식별정보가 유출등이 된 경우 - 외부의 불법적인 접근으로 개인정보가 유출된 경우	개인정보보호 책임자(CPO)
↓		
사고분석 및 대응·복구	■ 개인정보 유출 신고 등 사고 신속 대응팀의 조사 - 침해의 규모, 경위, 방법, 원인 및 관련자를 조사 - 필요 시 대응팀 및 CPO가 승인한 외부 전문가 지원 ■ 개인정보 침해사고 대응 및 복구 지원 - 접속기록, 보안장비 로그, 시스템 이미지 등 증거자료를 보존한 후 검증된 백업본을 이용하여 복구한다. - 복구 후 개인정보의 무결성, 접근권한, 보안설정 및 서비스 정상가동 여부를 확인한다.	개인정보 유출 부서장 개인정보보호 담당자
↓		
민원대응반 운영	■ 개인정보 유출사고 규모 및 성격에 따라 민원대응반 구성 ■ 2차 피해 방지를 위한 고객 민원 대응 및 고객 불안 해소 조치	(필요 시)
↓		
유출사고 결과보고	■ 개인정보 유출사고 결과보고서 작성 및 보고 - 침해사고처리 책임자는 보고서 작성 후 CPO에게 제출 - CPO는 개인정보침해 관련자에 대한 처분을 해당 부서에 요청 - 담당자는 침해사고 처리보고서를 관리하고 결과를 기록	개인정보 유출 부서장 개인정보보호책임자 /담당자
↓		
개선 및 이행점검	■ 침해사고처리 책임자는 처리보고서 제출 후 30일 이내 원인 분석 ■ 개인정보 유출사고 사례 전파 교육 및 개선 대책 시행(재발방지)	분야별 책임자 개인정보 담당자

2. 위기등급의 분류

가. 위기 등급별 판단 기준

구분	판단 기준
1등급	■ 전체 서비스가 중단되었거나 핵심 개인정보처리시스템을 사용할 수 없는 경우 ■ 예상 복구시간이 해당 시스템의 승인된 RTO를 초과하는 경우 ■ 중대한 개인정보 유출 또는 데이터 손상이 발생한 경우 ■ 주 백업 또는 대체수단으로 정상적인 복구가 곤란한 경우
2등급	■ 일부 기능 또는 일부 서비스가 중단된 경우 ■ 예상 복구시간이 승인된 RTO 이내이나 데이터 복원 또는 장비 교체가 필요한 경우 ■ 서비스는 가능하지만 성능 또는 처리품질이 현저히 저하된 경우
3등급	■ 일시적인 장애로 서비스 및 개인정보에 미치는 영향이 경미한 경우 ■ 즉시 복구 가능하고 데이터 손실이나 개인정보 유출 가능성이 없는 경우

나. 등급별 대응 방법

장애 등급	장애 범위	장애 대책
1 등급	■ 전체 서비스 및 개인정보처리시스템에 영향을 주는 장애	
	• 서비스 제공 불가 • 개인정보처리시스템 운용의 전면 중단 및 복구 불가	• 1등급 장애 지정 • 비상대책안 수립 및 시행 • 접수 및 즉시 유지보수업무 착수 • 20분 이내 비상연락망 가동 및 대응조직 소집
2 등급	■ 서비스는 가능하나 품질에 손실 발생	
	• 특정 자원의 장애 또는 고장으로 인한 심각한 속도 저하 현상 • 데이터의 일부 손상으로 복구 필요 • 일부 시스템 작동 중단	• 2등급 장애 지정 • 장애대책안 수립 및 시행 • 접수 및 즉시 유지보수업무 착수 • 30분 이내 관계자 보고 및 유지보수 대응체계 가동
3 등급	■ 구성 변경 및 정기 점검 작업 시 서비스 중단 상태	
	• 정기 점검 시 구성 변경으로 인한 서비스 중단 • 정기 점검 시 재기동으로 인한 서비스 중단	• 3등급 장애 지정 • 장애 진행 상황 모니터링 • 담당자 자체 조치 후 진행상황 기록 및 필요 시 상위보고

다. 장애 처리 절차 및 복원

- 개인정보처리시스템 및 관련 정보보호시스템에서 발생한 장애는 유지보수업체의 기술지원 인력의 기술지원을 받아 대응

연번	항목	내용	수행자
1	장애 발생	- 시스템 장애 발생을 유지보수업체에 접수	공단 전산담당자
2	1차 엔지니어 처리	- 유지보수업체 엔지니어에게 장애를 접수하고 처리	공단 전산담당자 유지보수업체 엔지니어
3	장애 유형 판단	- 장애이력, 유지보수 기록 및 기술자료를 통해 유사 장애와 조치내역 확인	공단 전산담당자 유지보수업체 엔지니어
4	2차 엔지니어 처리	- 유지보수업체 엔지니어 현장 투입	공단 전산담당자 유지보수업체 엔지니어
5	장비교체 및 시스템 점검	- 문제로 판명될 경우 장비 교체 및 시스템 점검	공단 전산담당자 유지보수업체 엔지니어
6	장애현황 파악	- 장애 원인, 영향범위, 조치내역 및 복구결과 기록	공단 전산담당자 유지보수업체 엔지니어
7	고객만족	- 고객이 만족할 수 있는 서비스를 제공	공단 전산담당자

라. 개인정보처리시스템 구성 요소

수탁업체	전화번호	개인정보처리시스템
(주)혁신정보시스템	1577-6846	공단 홈페이지
		문화체육시설 회원관리시스템
세인소프트	02-2039-8800	거주자우선주차 시스템
		공영주차장 통합관리시스템

3. 복구목표의 설정

- 가. 개인정보처리시스템의 위기 상황 발생 시 신속한 대응 및 복구를 위해 복구목표시간(RTO) 및 복구목표시점(RPO)을 정의해야 함
- 나. 복구목표시간은 장애 또는 재해가 발생한 시점과 공단이 이를 인지한 시점 중 먼저 확인되는 시점부터 산정

다. 복구목표시간 (RTO : Recovery Time Objective)

- 서비스 또는 사업 감내 목표를 초과하여 영향을 미치기 전 시점까지의 최고 중단 허용시간
- 개인정보처리시스템의 책임자는 업무 영향도를 고려하여 복구목표 시간의 정의 필요

라. 복구목표시점 (RPO : Recovery Point Objective)

- 업무를 계속적으로 수행하기 위해 손실된 데이터에 대한 유실 허용 시점
- 복구목표시점은 시스템별 업무 중요도, 백업주기, 데이터 변경량 및 유지보수 계약의 서비스 수준을 고려하여 정한다. 최종 복구 가능한 시점은 검증된 정상 백업본 중 복구목표시점에 가장 가까운 시점까지

4. 백업 관리

가. 정보시스템 장애 복구 흐름도



나. 백업관리

- 개인정보처리시스템 담당자는 신속한 업무 복구를 위해 백업 대상을 선정하고 필요한 내용을 주기적으로 백업 및 DR 구성
- 백업 대상은 DB, 개발소스 및 메일 데이터, 로그, 서버OS 그리고 기타 중요도가 높다고 판단되는 데이터를 대상으로 함
- 개인정보처리시스템 담당자는 안전한 백업 매체를 선정하고 백업의 주기 및 소산 유무를 결정
- 백업 매체는 비인가자가 접근할 수 없는 격리된 곳에 보관하여 비인가자에 의한 백업 정보 유출이 일어나지 않도록 함

다. 백업 시스템 운영현황

구분	유지관리 현황	비고
백업시스템	유지관리 계약 운영	비상시 유지보수업체현장 방문지원, 백업시스템 및 UPS 등 비상가동 실시
UPS 및 전기	정기점검 및 유지관리	

5. 위기대응 훈련

가. 개인정보처리시스템의 위기가 발생하는 경우 피해를 최소화하고 신속한 복구를 위해 상·하반기 위기대응 훈련과 정기적인 시스템 점검을 실시

나. 위기대응 훈련은 평시 서비스 운영 중에 재해·재난 복구시스템이 정상 작동되는지 확인해야 하며 위기상황 발생 시와 동일하게 위기대응 조직의 역할을 수행

다. 위기대응 훈련 시에는 다음의 사항을 유의하여 실시

- 재해·재난 복구시스템의 정상 작동
- 위기대응 조직 구성원별 역할 숙지
- 복구목표의 달성
- 운영 데이터 및 개인정보의 훼손·유출 방지
- 비상연락망 정상 가동상황
- 위기대응 체계 운용 시 이슈사항

라. 위기대응 훈련 종료 후 훈련 시 도출된 미흡사항 및 이슈사항을 위기대응 체계에 반영하여 개선

6. 비상연락망 구성

가. 개인정보처리시스템 담당자는 위기대응 조직원으로 이뤄진 비상연락망 관리

나. 개인정보처리시스템 담당자는 비상연락망을 주기적으로 검토하고 평상시에도 연락체계를 활용하여 정보를 공유

다. 위기상황 발생 시 위기상황 종료 시까지 비상연락망을 가동하여 신속한 대응 지원

양천구시설관리공단 개인정보보호 세부 인원 현황

(1) 개인정보 보호책임자

구 분	직 위 (직 급)	성 명
개인정보 보호책임자(CPO)	본부장	이 현 노

(2) 개인정보보호 분야별책임자

구 분	직 위 (직 급)	성 명
개인정보를 보유 · 처리하는 각 부서의 팀(관)장	안전감사팀장	김 성 식
	경영지원팀장	박 영 은
	혁신성과팀장	박 지 은
	공공시설관리팀장	김 준 현
	주차관리팀장	박 성 훈
	양천센터관장	이 상 주
	신월센터관장	이 영 복
	목동센터관장	조 경 만

(3) 개인정보 보호담당자

구 분	직 위 (직 급)	성 명
혁신성과팀(총괄부서)	관리6급	한 양 규(정)
	관리5급	최 상 곤(부)
	관리7급	이 현 정(부)
주차관리팀(주차관제)	관리6급	강 현 선(정)

(4) 사업장 개인정보 보호담당자

구 분	사업장/직급	성 명	비 고
혁신성과팀	관리6급	한 양 규	공단 개인정보보호 총괄(정)
	관리5급	최 상 곤	공단 개인정보보호 총괄(부)
	관리7급	이 현 정	공단 개인정보보호 총괄(부)
안전감사팀	관리7급	이 동 명	개인정보보호 담당자
경영지원팀	관리7급	윤 성 준	개인정보보호 담당자
주차관리팀	관리6급	강 현 선	개인정보보호 담당자
공공시설관리팀	관리5급	김 윤 기	개인정보보호 담당자
양천센터	기술5급	지 미 정	개인정보보호 담당자
신월센터	관리6급	위 현 주	개인정보보호 담당자
목동센터	관리5급	오 현 미	개인정보보호 담당자

(5) 개인정보 취급자

- 인사, 급여, 홈페이지, 회원관리, 주차 등 개인정보를 취급하는 전 직원
(관리직, 지도직, 접수처)