
개인정보 침해·유출사고 대응지침

2026. 8.



양천구시설관리공단

[제 · 개정 이력서]

[illegible]

[목 차]

제 1 장 총 칙	1
1. 목적	1
2. 관련근거	1
3. 다른 지침 등과의 관계	1
4. 용어 정의	1
제 2 장 개인정보 침해·유출사고 개요	2
1. 개인정보 침해·유출사고 분류	2
2. 개인정보 침해·유출사고 대응 방향	3
3. 개인정보 침해·유출사고 대응 업무분장	3
제 3 장 개인정보 침해·유출사고 대응절차	4
1. 개인정보 침해·유출사고 통지	4
2. 개인정보 침해·유출사고 절차	4
3. 개인정보 침해·유출사고 보고	5
4. 개인정보 침해·유출사고 통지	5
5. 개인정보 침해·유출사고 처리 및 종결	6
제 4 장 문제발생에 따른 3단계 대응절차	6
1. 심각단계	6
2. 경계단계	8
3. 주의단계	9
제 5 장 사후 대응 및 모니터링 방안	10
1. 사후 대응 및 재활동 방안	10
2. 모니터링 및 사전 대응 전략	10
[별지 제1호] 개인정보 침해·유출 통지 절차	11
[별지 제2호] 개인정보 침해·유출 통지문(안)	13
[별지 제3호] 개인정보의 침해·유출 통지내용(예시)	15
[별지 제4호] 고객의 대응방안 안내(예시)	16
[별지 제1호서식] 개인정보 침해·유출 신고서	17
[별지 제2호서식] 개인정보 침해·유출 신고 관리대장	18
[별지 제3호서식] 개인정보 침해·유출 사고 보고서	19
[별지 제4호서식] 개인정보 침해·유출 사고 관리대장	20
[별지 제5호서식] 개인정보 침해·유출 사고 처리보고서	21

제 1 장 총 칙

1. 목적

공단 내부의 과실·오남용, 분실·도난, 잘못된 전달, 외부 해킹·악성코드, 개인정보처리 시스템의 취약점 또는 수탁자의 관리상 과실 등으로 개인정보 침해·유출사고가 발생 하거나 발생 가능성이 확인된 경우, 체계적이고 신속한 대응을 통해 피해의 확산을 방지하고 정보주체의 권익을 보호하며 사고 원인을 분석하여 재발을 방지하는 것을 목적으로 한다.

2. 관련근거

- 가. 「개인정보 보호법」
- 나. 「개인정보 보호법 시행령」
- 다. 공단의 「개인정보 내부관리계획」
- 라. 「개인정보의 안전성 확보조치 기준」 (개인정보보호위원회 고시)
- 마. 기타 개인정보 보호 및 정보보안 관련 법령·고시·가이드라인

3. 다른 지침 등과의 관계

개인정보 침해·유출사고의 대응에 관하여 법령, 공단 규정 또는 다른 지침에서 특별히 정한 사항은 그 규정을 우선 적용한다. 다만 이 지침은 사고 대응의 기본 절차와 내부 보고체계를 정하는 공단의 공통 기준으로서 다른 규정과 상호 보완하여 운영한다.

4. 용어 정의

- 가. “침해·유출”이란 법령이나 공단의 자유로운 의사에 의하지 않고, 고객의 개인정보에 대하여 공단이 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 것을 말함.
- 나. “침해·유출사고”란 비 인가된 접근, 개인정보처리시스템의 오·남용, 비 인가된 시스템 사용 또는 사용자의 계정 도용, 악성코드 유입 및 실행, 정보 서비스의 방해, 해킹사고와 바이러스 사고, 보안정책에 위반되는 행위를 말한다.
- 다. “오·남용”이란 개인정보처리시스템 및 네트워크 자원을 허가받지 않은 방법으로 사용하거나 악용하는 공격 또는 스팸메일을 보낼 때 다른 사이트의 시스템을

이용하는 방법이나 다른 사람의 계정을 도용하는 행위 등을 말한다.

라. "정보수집"이란 특정 사이트나 개인정보처리시스템 및 네트워크에 대한 정보를 수집하기 위한 공격을 말한다.

마. "시스템 침입"이란 개인정보처리시스템 또는 네트워크의 취약성을 이용하여 시스템에 침입하는 공격으로, 특정 취약점을 공격하는 해킹프로그램을 이용하거나, 잘못된 서버 운영상의 문제를 이용하여 침입함을 말한다.

바. "침해·유출사고 대응팀"이란 해킹 또는 바이러스 사고 발생에 따른 사고의 분석, 처리, 사후 복구, 사후 예방 조치 등을 주요 업무로 하는 한시적으로 운영하는 조직을 말한다.

사. "초동조치"란 사고 확대를 막고 증거를 보존하기 위해 사고 발생 직후 수행하는 계정 차단, 권한 회수, 네트워크 격리, 로그 보존, 취약점 차단 등의 긴급 조치를 말한다.

※ 이외 용어의 정의는「개인정보 보호법」제2조(정의), 공단의「정보보안지침」,「개인정보 내부관리계획」참조

제 2 장 개인정보 침해·유출사고 개요

1. 개인정보 침해·유출사고 분류

분 류	사 례
분실·도난	개인정보가 포함된 문서, 노트북, 휴대전화, 이동식 저장매체 등을 분실하거나 도난당한 경우
무단접근	개인정보처리시스템 또는 데이터베이스에 권한 없는 자가 접근한 경우
오전달·오발송	이메일·문자·팩스·우편·문서·파일 등을 권한 없는 수신자에게 전달한 경우
외부 해킹	취약점 악용, 계정 탈취, 악성코드, 랜섬웨어, 웹쉘, 불법접속 등으로 개인정보에 접근한 경우
내부자 오·남용	권한을 가진 자가 업무 목적을 벗어나 개인정보를 조회·복사·반출·제공한 경우
공개·노출	홈페이지, 게시판, 클라우드, 공유폴더, 출력물 등에서 개인정보가 불특정 또는 권한 없는 자에게 공개된 경우
수탁자 사고	위탁받은 업무를 수행하는 과정에서 수탁자 또는 재수탁자의 관리 소홀로 개인정보가 분실·도난·유출된 경우
기타	시스템 오류, 백업·복구 과정의 잘못된 처리, 파기 미흡, 출력물 방치 등으로 개인정보의 통제권을 상실한 경우

2. 개인정보 침해·유출사고 대응 방향

- 가. 사고 발생 전: 개인정보보호 정책·절차 수립, 담당조직 운영, 사고대응 비상연락망 유지, 수탁자 관리, 예방점검 및 교육을 실시한다.
- 나. 사고 발생 시: 사고를 즉시 접수하고 초동조치와 증거보존을 우선 수행한 후 사실관계를 확인하여 정보주체 통지 및 관계기관 신고 여부를 신속하게 판단한다.
- 다. 사고 처리 후: 원인분석, 피해복구, 정보주체 보호조치, 재발방지 대책, 교육 및 제도개선을 완료하고 결과를 기록한다.
- 라. 대응 과정에서 정보주체의 2차 피해를 방지하기 위하여 비밀번호 변경, 사칭·피싱 주의, 금융거래 확인 등 사고 유형별 예방조치를 구체적으로 안내한다.

3. 개인정보 침해·유출사고 대응 업무분장

구 분	분 장 내 용	담 당		비 고
발생 전 (대응방안)	○ 개인정보보호 통제를 위한 정책 수립	공 단	개인정보 보호책임자	전략 수립
	○ 개인정보보호 통제를 위한 절차 수립			
	○ 개인정보보호 활동을 위한 조직 구성	혁 신 성과팀	개인정보 보호담당자	
	○ 개인정보 침해·유출사고 발생에 따른 정보 수집			
발생 후	○ 사고 발생에 따른 개별취재 등 언론대응(홍보 관련 부서 협조) - 대 고객 사과문 발표 등	혁 신 성과팀	개인정보 보호담당자	지침 이행
	○ 대응방안 취합 및 대책반 구성·개최 준비			
	○ 위험 상황 전사 공유(전 부서 협조)	공 단	개인정보 보호책임자	
	○ 대응방안 검토 결과 대응방침 결정			

제 3 장 개인정보 침해·유출사고 대응절차

1. 개인정보 침해·유출사고 통지

가. 개인정보보호 담당자는 유출 인원 등을 확인하여 [별지 제1호]의 통지방법에 따라 정보주체들에게 유출 통지한다.

- 단 1명의 정보주체에 관한 개인정보가 유출 등이 된 경우 해당
- 서면 등의 방법을 통하여 개별 통지가 원칙
- 통지 항목

- ① 유출된 개인정보의 항목
- ② 유출 시점과 및 그 경위
- ③ 정보주체가 취할 수 있는 피해 최소화 조치
- ④ 기관의 대응조치 및 피해구제 절차
- ⑤ 피해 신고 접수 담당부서 및 연락처

나. 수탁사업자가 수탁 업무를 처리하는 과정에서 개인정보가 유출된 경우 즉시 위탁자에게 보고하도록 위·수탁계약서에 명시하고, 수탁사업자로부터 보고 받은 시점에서 지체 없이 유출 통지한다.

2. 개인정보 침해·유출사고 절차

가. 1천명 이상의 고객에 관한 개인정보가 침해·유출된 경우에는 고객에 대한 통지 및 조치 결과를 72시간 이내에 공단에 보고한다.

나. 고객에 관한 개인정보가 1천명 이상의 침해·유출된 경우에는 고객에 대한 통지 및 조치결과를 72시간 이내에 공단 이사장을 경유하여 개인정보보호위원회 또는 한국인터넷진흥원 중 어느 하나에 신고한다.

다. 개인정보 침해·유출사고 보고 또는 신고는 별지 제1호 서식의 '개인정보 침해·유출 신고서'를 활용한다.

라. 전자우편, 팩스 또는 인터넷 사이트를 통하여 유출신고를 할 시간적 여유가 없거나 그 밖에 특별한 사정이 있는 때에는 먼저 전화를 통하여 신고한 후, 별지 제1호 서식의 '개인정보 침해·유출 신고서'를 제출 가능하다.

- 마. 1천명 이상의 고객에 관한 개인정보가 유출된 경우에는 통지와 함께 공단 홈페이지에 고객이 알아보기 쉽도록 7일 이상 게재할 수 있도록 개인정보 보호책임자에게 요청한다.
- 바. 개인정보 침해·유출사고 신고는 별지 제2호 서식의 '개인정보 침해·유출 신고 관리대장'에 기록·관리한다.

3. 개인정보 침해·유출사고 보고

- 가. 개인정보 침해·유출사고가 발생한 것으로 확인된 때에는 개인정보 보호담당자는 지체 없이 개인정보 보호책임자에게 침해·유출 사고에 대한 보고한다.
- 나. 사고보고는 별지 제3호 서식 '개인정보 침해·유출사고 보고서' 활용한다.

4. 개인정보 침해·유출사고 통지

- 가. 실제로 침해·유출 사고가 발생한 것으로 확인된 때에는 정당한 사유가 없는 한 72시간 이내에 해당 고객에게 아래 사항 공지한다.
 - 침해·유출된 개인정보의 항목
 - 침해·유출된 시점과 그 경위
 - 침해·유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 고객이 할 수 있는 방법 등에 관한 정보
 - 공단의 대응조치 및 피해구제절차
 - 고객에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
 - 별지 제1호 '개인정보 침해·유출 통지 절차'
 - 별지 제2호 '개인정보 침해·유출 통지문(안)'
 - 별지 제3호 '개인정보의 침해·유출 통지내용(예시)'
- 나. 침해·유출된 시점과 그 경위의 경우, 개인정보 침해·유출 사고가 최초 발생한 시점과 알게 된 시점 사이에 시간적 차이가 있는 경우에는 이에 대한 과실유무를 입증 필요하다.
- 다. 침해·유출 사고의 조치를 취한 이후에는 고객에게 다음 아래의 사실만을 일차적으로 알리고, 추후 확인되는 즉시 알릴 수 있다.
 - 고객에게 유출이 발생한 사실

- 통지항목 중 확인된 사항

라. 고객에게 통지할 때에는 서면, 전자우편, 팩스, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 72시간 이내에 고객에게 알려야 함과 동시에, 홈페이지 등을 통하여 공개 가능하다.

- 별지 제4호 ‘고객의 대응방안 안내(예시)’

5. 개인정보 침해·유출사고 처리 및 종결

가. 공단에서는 개인정보 침해·유출사고 종결처리는 문서로 기록·관리한다.

- 별지 제4호 서식의 ‘개인정보 침해·유출 사고 관리대장’
- 별지 제5호 서식의 ‘개인정보 침해·유출 사고 처리 보고서’

나. 개인정보 침해·유출사고에 대한 종결 처리되었음을 각 관련기관에 통지한다.

- 공단 이사장
- 개인정보보호위원회 또는 한국인터넷진흥원 중 어느 하나에 통지 (1천명 이상의 고객에 관한 개인정보가 유출된 경우)

제 4 장 문제발생에 따른 3단계 대응절차

1. 심각단계

가. 발생 시나리오

- 공단의 내부기밀 및 개인정보 언론보도, 고객의 부정적 인지도 확대
- 비판여론 확대, 사업 중단, 관계자 문책요구 증가

나. 대응계획 및 방향

- 「개인정보 보호법」 대처 방안에 따라 업무분장, 적극적 대응
- 유출내용 대상자 통보, 공단 이사장 보고, 유출경로 분석
- 비판여론 수용, 신속한 고객 사과조치 및 재발방지 약속, 개선방안 제시

다. 침해·유출사고 대응 업무분장

구 분	업 무 분 장
공단 이사장	· 침해·유출사고수준 발생 시 상황보고 받고 대응책 지시 · 개인정보 보호책임자에게 접수 받은 내용을 검토하고 개인정보보호위원회에 즉시 보고
개인정보 보호책임자	· 침해·유출사고수준 발생 시 대내외 홍보계획을 추진하고 침해·유출사고 대응 팀 구성 · 침해·유출사고 대응팀 구성여부를 공단 이사장에 보고 · 침해·유출사고 유형 및 수준을 판단하고 침해·유출사고수준 발생 시 개인정보 보호담당자로부터 즉시 보고를 받고 필요한 대응 강구
개인정보 보호담당자	· 침해·유출사고 발생 시 정보수집 및 유출상황을 파악하고, 침해·유출사고 관리 보고서 작성 후 개인정보 보호책임자에게 즉시 보고

라. 침해·유출사고 대응 프로세스 및 보고절차

순 서	대응 조치
침해·유출사고 발생	· 침해·유출사고 발생 징후 입수 및 정보수집 · 침해·유출사고 진행에 따라 대응절차 준비
정보수집 / 침해·유출사고 대응	· 침해·유출사고의 종류 및 정도에 따라 대응방법 선택 · 개별취재 등 언론 대응은 공단 홍보팀으로 이관 · 유출경로 추적 및 로그분석
리스크관리팀 가동	· 리스크 발생 시 예상피해 산출 및 대응방안 마련
대응방침 결정 및 발표	· 조속한 대응방침 결정 · 정확한 피해 확인 및 피해정도에 따라 홈페이지 및 기타 매체를 통한 상황전파여부 결정
조직내부 관리	· 침해·유출사고 대응 상황 전파
조기수습 / 확산방지	· 이해관계자 대책 마련, 조기수습 및 파급확산 방지 · 재발방지를 위한 조치
사후 대응 및 재활동	· 침해·유출사고 상황 종료 후 공단 이미지 재활을 위한 PR활동 전개 · 침해·유출사고 대응 내용을 매뉴얼 하여 임직원 침해·유출사고 의식 교육 활용

2. 경계단계

가. 발생 시나리오

- 공단의 내부기밀 및 특정 개인정보 언론 노출
 - 전문자·일간지 및 방송 등 일부 비판여론 형성에 대한 사업추진 방향 선회 필요

나. 대응계획 및 방향

- 침해·유출사고 대응 발효 시 개인정보 보호책임자의 침해·유출사고 대응

다. 침해·유출사고 대응 업무분장

구 분	업 무 분 장
공단 이사장	· 침해·유출사고수준 발생 시 개인정보 보호책임자로부터 보고를 받고 필요한 대응책 지시 · 개인정보 보호책임자에게 접수 받은 내용을 검토하고 교육부장관에게 즉시 보고
개인정보 보호책임자	· 침해·유출사고 유형 및 수준을 판단하고 침해·유출사고수준 발생 시 공단 이사장에게 즉시 보고 또는 통보
개인정보 보호담당자	· 침해·유출사고 발생 시 정보수집 및 유출상황을 파악하고, 침해·유출사고 관리 보고서 작성 후 개인정보 보호책임자에게 즉시 보고

라. 침해·유출사고 대응 프로세스 및 보고절차

순 서	대응 조치
침해·유출사고 발생	· 침해·유출사고 발생 직후 입수 및 정보수집 · 침해·유출사고 진행에 따라 대응절차 준비
정보수집 / 침해·유출사고대응	· 침해·유출사고의 종류 및 정도에 따라 대응방법 선택 · 개별취재 등 언론 대응은 공단 홍보팀으로 이관 · 유출경로 추적 및 로그분석
사후 대응 및 재활활동	· 침해·유출사고 상황 종료 후 공단 이미지 재활을 위한 PR활동 전개 · 침해·유출사고대응 내용을 매뉴얼 하여 임직원 침해·유출사고의식 교육 활용

3. 주의단계

가. 발생 시나리오

- 공단 내부갈등의 외부 노출
- 언론, 유관기관 등을 통해 공단 내부갈등 상황이 일부 노출

나. 대응계획 및 방향

- 침해·유출사고 대응 발효 시 개인정보 보호책임자의 통제 하에 침해·유출사고 대응

다. 침해·유출사고 대응 업무분장

구 분	업 무 분 장
공단 이사장	· 개인정보 보호책임자로부터 보고 받은 내용을 검토하고 필요한 대응책 지시
개인정보 보호책임자	· 침해·유출사고 유형 및 수준을 판단하고 침해·유출사고수준 발생 시 공단 이사장에게 즉시 보고 또는 통보
개인정보 보호담당자	· 침해·유출사고 발생 시 정보수집 및 유출상황을 파악하고, 침해·유출사고관리 보고서 작성 후 개인정보 보호책임자에게 즉시 보고

라. 침해·유출사고 대응 프로세스 및 보고절차

순 서	대응 조치
침해·유출사고 발생	· 침해·유출사고 발생 직후 입수 및 정보수집 · 침해·유출사고 진행에 따라 대응절차 준비
정보수집 / 침해·유출사고대응	· 침해·유출사고의 종류 및 정도에 따라 대응방법 선택 · 개별취재 등 언론 대응은 공단 홍보팀으로 이관 · 유출경로 추적 및 로그분석
사후 대응 및 재활활동	· 침해·유출사고 상황 종료 후 공단 이미지 재활을 위한 PR활동 전개 · 침해·유출사고대응 내용을 매뉴얼 하여 임직원 침해·유출사고의식 교육 활용

제 5 장 사후 대응 및 모니터링 방안

1. 사후 대응 및 재활동 방안

가. 비판여론 수용, 신속한 대 고객 사과조치 및 재발방지 약속

- 공단 홍보팀 홍보담당자 협조에 따른 조치
- 보도자료 및 대내외 홍보 활동

나. 사이버 침해·유출사고 처리 절차 및 대응 요령 따른 업무수행

- 개인정보보호 사고 발생 시의 사고대응절차와 공식적인 보고절차 정의
 - 사고인지 → 초동대응 및 신고 → 사고원인 조사 → 피해복구 → 후속조치
- 개인정보처리시스템 사용자는 시스템이나 관련 장비에 취약점을 인식했거나 의심스러운 요소를 발견 시, 반드시 부서별 개인정보책임자에게 보고

2. 모니터링 및 사전 대응 전략

가. 추진방향

- 개인정보보호 통제를 위한 정책 수립
- 효율적인 개인정보보호 활동을 위한 조직 구축
- 지속적인 개인정보보호 활동 수행 관리를 통해 체계적인 개인정보보호 운영

나. 세부추진전략

- 장애처리
 - 시스템 모니터링을 통하거나 장애 발견자로부터 장애사항 접수
 - 장애등록 및 장애내용을 분석
 - 복구대책에 따라 장애복구조치 수행 및 조치결과를 보고
 - 장애복구내용 및 향후대책을 개인정보 보호책임자에게 보고
- 예방점검
 - 매년 예방점검 계획을 수립하여 관련부서와 협의 후, 개인정보 보호책임자에게 보고(유지보수 계약 체결 등)
 - 정기 예방점검 및 예방점검 결과 보고(매월 유지보수 결과 보고 등)

개인정보 침해·유출 통지 절차

구분	세 부 내 용	법적근거
침해·유출 통지방법	공단은 개인정보 유출이 발생했을 경우 지체 없이 정보주체에게 개인정보 유출 관련 사항을 통지	법 제34조 시행령 제40조
통지방법	1. 서면, 전자우편, 팩스, 전화, 휴대전화 문자전송 또는 이와 유사한 방법 2. 1번의 통지방법과 동시에 홈페이지 등을 통하여도 공개 - 단, 통지 및 조치 후에도 1천명 이상의 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알기 쉽도록 7일 이상 통지내용을 게재 - 인터넷 홈페이지를 운영하지 않는 공단의 경우 사업장 등의 보기 쉬운 장소에 통지내용을 게시	시행령 제40조
통지내용	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 피해구제절차 ⑤ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처	법 제34조 제1항
통지시기	72시간 이내(유출사고 최초발생 시점과 확인된 시점 사이에 시간적 차이가 있는 경우 이에 대한 과실유무를 입증해야 함)	시행령 제40조
통지연기	1. 개인정보 유출확산방지를 위해 조치가 필요한 경우 유출 통지를 연기 ① 개인정보가 유출되었을 것으로 의심되는 개인정보처리시스템의 접속권한 삭제·변경 또는 폐쇄 조치 ② 네트워크, 방화벽 등 대·내외 시스템 보안점검 및 취약점 보완 조치 ③ 향후 수사에 필요한 외부의 접속기록 등 증거 보존 조치 ④ 정보주체에게 유출 관련 사실을 통지하기 위한 유출확인 웹페이지 제작 등의 통지방법 마련 조치 ⑤ 기타 개인정보의 유출확산 방지를 위해 필요한 기술적·관리적 조치 2. 공단은 1번 각 항목의 조치를 취한 이후, 정보주체에게 다음 각 항목의 사실만 일차적으로 알리고, 추후 확인되는 즉시 알릴 수 있음 ① 정보주체에게 유출이 발생한 사실 ② 통지내용 중 확인된 사항	시행령 제40조

구분	세 부 내 용	법적근거
침해·유출통지 신고방법		
신고대상	1천명 이상의 정보주체에 관한 개인정보가 유출된 경우	법 제34조 제3항
신고기관	http://www.privacy.go.kr	시행령 제39조 제2항
신고시기	72시간 이내(정보주체에 대한 통지 및 조치결과 신고)	
신고방법	① 전자우편, 팩스, 인터넷 사이트를 통해 유출사고 신고 및 신고서 제출 ② 시간적 여유가 없거나 특별한 사정이 있는 경우 : 전화를 통하여 통지내용을 신고한 후, 유출신고서를 제출할 수 있음	
신고내용	기관명, 통지여부, 유출된 개인정보 항목·규모, 유출 시점·경위, 유출피해 최소화 대책·조치 및 결과, 정보주체가 할 수 있는 피해 최소화 방법 및 구제절차, 담당부서·담당자 연락처 등	
신고접수 기록	개인정보보호위원회 또는 한국인터넷진흥원에 신고접수사실 확인(신고자 전자우편, 팩스)	

기술지원		
지원요청	피해 확산방지, 피해복구 등을 위한 기술지원 - 개인정보보호위원회 또는 한국인터넷진흥원과 공동으로 조사·지원팀 구성	법 제34조 제3항
결과보고	유출신고 처리결과 보고서를 유출신고 업무종결한 날로부터 10일 이내 개인정보보호위원회에 제출	

벌칙		
벌칙조항	개인정보 유출신고(72시간이내) 위반시 과태료 3천만원이하	법 제75조 제2항 제9호

개인정보 침해·유출 표준 통지문(안)

※ 부가설명 란에 필수사항은 < >, 참고사항은 ()로 표기

※ 필수사항이 확인되지 않아 통지문에 포함하지 않은 경우 추후 확인되면 반드시 추가 통지

※ 아래 (안)을 참고하여 유출 상황에 적합하게 내용을 변경하여 활용

표준 통지문(안) 예시	부가 설명
개인정보 유출 사실을 통지해 드리며, 깊이 사과드립니다.	<제목> - ‘유출 통지’ 문구 포함
귀하의 개인정보 보호를 위해 최우선으로 노력하여 왔으나, 불의의 사고로 귀하의 소중한 개인정보가 유출되었음을 알려 드리며, 이에 대하여 진심으로 사과를 드립니다.	(사과문) - 유출 통지 사실 알림 - 사과문을 먼저 표현
귀하의 개인정보는 ○○○○년 ○○월 ○○일 ○○○시스템 장애 처리를 위한 데이터 분석 과정에서 유지관리업체로 전달되었고, 유지관리업체는 자체 서버에 저장·보관하다가 안전 조치를 다하지 못해 ○○○○년 ○○월경 해커에 의한 해킹으로 유출되었습니다. 유출된 정확한 일시는 ○○○○○에서 현재 수사가 진행 중이며, 확인되면 추가로 알려 드리도록 하겠습니다.	<유출된 시점과 경위> - 유출된 시점과 경위를 누구나 이해할 수 있게 상세하게 설명 - ‘귀하’, ‘고객님’ 등으로 유출된 정보주체 명시 ※ 부적합한 표현 : 일부 고객, 회원정보의 일부 - 추가 확인된 사항은 반드시 추가로 통지
유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 주민등록번호, 이메일, 연락처 등 총 6개입니다.	<유출된 항목> - 유출된 항목을 누락 없이 모두 나열 ※ ‘등’으로 생략하거나, ‘회사 전화번호’ 및 ‘집 전화번호’를 합쳐서 ‘전화번호’로 표시 안 됨
유출 사실을 인지한 후 즉시 해당 IP와 불법접속 경로를 차단하고, 취약점 점검과 보완 조치를 하였습니다. 또한, 유지보수업체 서버에 있던 귀하의 개인정보는 즉시 삭제 조치하였습니다.	<공단의 대응조치> - 접속경로 차단 등 예시된 항목 외에도 망 분리, 방화벽 설치, 개인정보 암호화, 인증 등 접근 통제, 시스템 모니터링 강화 등 조치한 내용 설명
○○○○○이 발표한 수사 결과에 따르면 현재 해커는 검거되었고, 해커가 불법 수집한 개인정보는 2차 유출하거나 판매하지는 않은 것으로 확인되었습니다.	<피해 최소화를 위한 정보주체의 조치방법> - 유출 경위에 따라 정보

표준 통지문(안) 예시	부가 설명
따라서 현재로서는 이번 사고로 인한 2차 피해가 발생할 가능성이 높지 않아 보이나, 혹시 모를 피해를 최소화하기 위하여 귀하의 비밀번호를 변경하여 주시기 바랍니다. 그리고 개인정보 악용으로 의심되는 전화, 메일 등을 받으시거나 기타 궁금하신 사항은 연락주시면 친절하게 안내해드리고, 신속하게 대응하도록 하겠습니다.	주체가 할 수 있는 방법을 안내 - 사건에 따라 다양한 피해를 추정하여 예방 가능한 방법을 모두 안내 (보이스 피싱, 피싱 메일, 불법 TM, 스팸문자 등)
아울러, 피해가 발생하였거나 예상되는 경우에는 아래 담당부서에 신고하시면 성실하게 안내와 상담을 해드리고, 필요한 조사를 거쳐 손실보상이나 손해배상 등의 구제절차를 진행하도록 하겠습니다. 개인정보분쟁조정위원회의 분쟁조정 제도나 신고 접수 전문기관인 한국인터넷진흥원의 개인정보침해신고센터를 통해 피해를 구제받고자 하실 경우에도 연락주시면 그 절차를 안내하고 필요한 제반 지원을 아끼지 않도록 하겠습니다.	<공단의 피해 구제절차> - 보상이나 배상이 결정된 경우에는 그 내용을 상세히 기재 - 보상이나 배상이 결정되지 않은 경우 계획과 절차를 안내 - 감독기관 등을 통한 구제절차도 안내
앞으로 장애처리 과정에 대한 개인정보 보호 조치 강화 등 내부 개인정보 보호 관리체계를 개선하고, 관계 직원 교육을 통해 인식을 제고하여, 향후 다시는 이와 유사한 사례가 발생하지 않도록 최선의 노력을 다하겠습니다.	(공단의 향후 대응계획) - 추가적인 향후 대응계획을 포함
항상 믿고 사랑해 주시는 귀하께 심려를 끼쳐 드리게 되어 거듭 진심으로 사과드립니다.	(사과문)
▶ 피해 등 접수 담당부서 : 혁신성과팀 ▶ 피해 등 접수 전화번호 : 02-2061-3414 ▶ 피해 등 접수 e-메일주소 : ykhan@ycs.or.kr	<피해 등 신고 접수 담당부서 및 연락처> - 전담처리부서 안내를 원칙으로 하되, 대량 유출로 일시적으로 콜센터 등 다른 부서를 지정한 경우 해당 부서를 안내
<양천구시설관리공단> 직원 일동	

개인정보 침해·유출 통지내용(예시)

고객 여러분의 개인정보가 유출되어 심려를 끼치게 된 점 진심으로 사과드립니다.

고객 여러분께 알려드립니다.

당 공단에서는 내부 모니터링을 통해 고객의 일부 정보가 ○○월 ○○일 해킹에 의해 유출된 사실을 ○○월 ○○일 확인하였으며 고객 여러분의 피해예방 및 조속한 범인검거를 위하여 수사기관 및 관계기관에 즉시 조사를 의뢰하였음을 알려드립니다.

현재까지 파악된 바는 유출된 개인정보는 암호화된 비밀번호 등이며, 비밀번호는 최고 수준의 기술로 암호화되어 있어 안전합니다.

이는 중국발 IP로부터의 악성코드를 통해 해킹된 것으로 추정하고 있으며 자세한 상황은 수사기관 및 관계기관의 사실 확인을 바탕으로 추가 공지해 드리겠습니다.

고객 여러분의 서비스 사용에는 아무런 문제가 없습니다만, 보이스 피싱 및 스팸 메일 예방을 위하여 고객 여러분의 세심한 주의를 부탁드립니다.

고객의 피해예방을 위한 안내 및 당 공단의 조치

1. 보이스 피싱 주의 : 공공기관 및 기타 기관의 직원을 사칭하여 전화 등으로 금융정보를 묻는 경우에는 전화를 일단 끊고 반드시 해당 기관에 확인해 주시기 바랍니다.
2. 스팸 메일 주의 : 광고, 홍보성 메일이 증가할 수 있으니 각 메일에서 제공하고 있는 스팸 설정, 수신거부 기능 등을 참고하여 차단해 주시면 스팸 수신을 줄일 수 있습니다.
당 공단에서는 중국 등 위험 지역 특정 IP로부터의 대량 메일 발송에 대하여서는 자동 차단 기능 등 스팸에 대한 필터를 강화할 것입니다.
3. 비밀번호 변경 : 비밀번호는 암호화되어 있어 안전합니다만 생년월일, 휴대폰번호, 단순한 숫자의 나열 등 예측하기 쉬운 방식으로 설정하신 비밀번호는 만일의 경우를 대비해서 변경해 주시기 바랍니다.

아이디/비밀번호 찾기

당 공단에서는 비밀번호 변경 캠페인을 정기적으로 진행하고 있으며 무작위 조합을 통한 비정상 로그인 시도를 차단하기 위하여 틀린 비밀번호 입력 시 인증을 강화하였습니다.

당 공단은 조속한 범인 검거와 고객정보의 회수를 위하여 수사기관 및 관계기관에 적극 협조할 것이며, 업계 전문가 및 관련 정부 기관들과 함께 유출 정보의 유포 방지 및 2차 피해예방을 위하여 최선의 노력을 다할 것입니다. 관련하여 궁금한 점이 있으시면 아래 핫라인으로 연락주시기 바랍니다.

핫라인: 02-2061-3414 메일주소: ykhan@yys.or.kr

해킹으로 인해 고객 여러분께 불편을 끼쳐드린 점 다시한번 고개 숙여 사과드리며, 이번 일을 계기로 최고 수준의 보안으로 한층 강화하여 신뢰를 줄 수 있는 공단이 되도록 노력하겠습니다.

개인정보 유출여부 확인을 위한 기능은 빠른 시간 내에 제공할 예정입니다.

고객의 대응방안 안내(예시)

개인정보 유출 2차 피해 예방 4대 핵심 수칙

 **주의:** 공단을 사칭한 안내나 문자를 받으시면 절대 링크나 첨부파일을 열지 마시고, 공식 홈페이지 및 대표전화로 먼저 확인하십시오!

✓ 즉시 실행해야 할 4가지

1 비밀번호 즉시 변경

유출 의심 서비스는 물론, 동일/유사한 비밀번호를 사용하는 타 사이트 비밀번호도 함께 변경합니다.

2 2단계 인증 및 로그인 보안 강화

문자·앱 인증 등 추가 인증 수단을 설정하고, 로그인 알림 및 최근 접속기록을 점검합니다.

3 금융·통신 거래 내역 점검

신청하지 않은 결제, 계좌이체, 휴대전화 개통, 소액결제 및 인증서 발급 내역이 있는지 확인합니다.

4 의심 연락 증거 화면 캡처

의심스러운 문자, 메일, 전화번호, URL 및 접속기록은 삭제하기 전 화면을 캡처하여 보관합니다.

⊘ 절대 하지 말아야 할 4가지

1 불분명한 링크·첨부파일 열기 금지

출처가 확실하지 않은 URL, 앱 설치 파일(.apk), 문서 첨부파일은 절대로 실행하지 마십시오.

2 민감 개인정보 및 인증번호 전달 금지

주요 개인식별정보, 계좌·카드번호, 비밀번호, OTP/인증번호를 전화·문자·메신저로 절대 전달하지 않습니다.

3 원격제어 및 앱 설치 요구 거절

피해 확인이나 보상/환불을 이유로 원격제어 앱이나 보안 앱 설치를 요구하면 즉시 통화를 종료합니다.

4 확인되지 않은 정보 온라인 확산 금지

유출 규모나 원인, 피해 여부가 공식 확인되지 않은 사실을 온라인이나 SNS에 전달하지 않습니다.

⚠ 특히 이런 연락(사기/스미싱)을 주의하세요!

- **보상 및 환불 신청 빙자:** 유출 피해 보상금을 받으라며 특정 링크 접속이나 앱 설치를 유도하는 경우
- **본인 확인 빙자:** 유출 여부를 조회해주겠다며 아이디, 비밀번호, OTP 인증번호 입력을 요구하는 경우
- **기관 사칭 송금 요구:** 공단·경찰·금융감독원 직원을 사칭하여 계좌이체나 '안전계좌' 송금을 요구하는 경우

피해 발생 또는 의심 시 대처 단계

1단계: 금융/통신 차단

지급정지 & 계정보호

해당 금융사 및 통신사에 즉시 연락하여 계좌 지급정지, 소액결제 차단, 휴대폰 개통 정지를 요청하세요.

2단계: 신고 & 상담

주요 신고기관 연결

- 경찰청: 112
- 금융감독원: 1332
- 개인정보침해신고센터: 118

3단계: 스미싱 검증

보호나라 카카오톡

의심스러운 URL 문자 수신 시 카카오톡 '보호나라' 채널의 '스미싱·피싱 확인서 비스'를 이용하세요.

[별지 제1호 서식]

표준 개인정보 보호지침 [별지 제1호 서식]

개인정보 침해·유출 신고서

기 관 명					
고객에의 통지 여부					
유출된 개인정보의 항목 및 규모					
유출된 시점과 그 경위					
유출피해 최소화 대책·조치 및 결과					
고객이 할 수 있는 피해 최소화 방법 및 구제절차					
담당부서·담당자 및 연락처	구분	성명	부서	직위	연락처
	개인정보 보호책임자				
	개인정보 보호담당자				

유출신고 접수기관	기관명	담당자명	연락처

개인정보 침해·유출 사고 보고서

개인정보 보호담당자	개인정보 보호책임자

침해·유출사고 처리 담당자		침해·유출사고 번호	
신고자 정보			
소 속			
신고자 이름			
전화번호			
E-mail			
피해 시스템 정보			
IP 주소			
호스트 명			
운영체제			
추정 피해 시간			
시스템 운영 환경			
공격 시스템 정보			
IP 주소			
호스트 명			
사고에 대한 설명(간단히 작성)			
사고발견 경위, 피해현황 등			
관련 기관(부서) 통지			
기관(부서)명	통지 내용		

개인정보 침해·유출 사고 처리 보고서

보고일자	20 년 월 일	문서번호	
침해·유출 신고/접수번호			
침해·유출 대상정보	☐ 일반 개인정보 ☐ 주민등록번호 ☐ 외국인등록번호 ☐ 민감정보 ☐ 계좌번호 ☐ 신용카드번호		
접수일시		신고자	
침해·유출사고 처리책임자		신고자 연락처	
신고내용			
대응과정	일시	대응활동	
침해·유출 내용	※ 확인된 침해 정보의 세부사항, 규모 및 유출방법 - 침해·유출방법 : 유출, 외부자 제공, 수집, 접근, 분석, 이용, 내부자 제공, 불법 저장, 불안정한 저장, 파기, 비파기 등 세부사항		
침해·유출 발생 경위			
관련자			
침해·유출 발생 원인			
증거자료			
복구 및 재발 방지 조치			
처분			