

□ **신구조문 대비표**

현행	개정안
제 1 장 총 칙 1. 목 적 공단 내부의 과실 및 오·남용 또는 외부 해킹 등으로 개인정보 침해·유출 사고가 발생할 경우, 체계적이고 신속한 대응이 이루어져 피해를 최소화하려는데 목적이 있음.	제 1 장 총 칙 1. 목 적 공단 내부의 과실·오남용, 분실·도난, 잘못된 전달, 외부 해킹·악성 코드, 개인정보처리시스템의 취약점 또는 수탁자의 관리상 과실 등으로 개인정보 침해·유출사고가 발생하거나 발생 가능성이 확인된 경우, 체계적이고 신속한 대응을 통해 피해의 확산을 방지하고 정보주체의 권익을 보호하며 사고 원인을 분석하여 재발을 방지하는 것을 목적으로 한다.
제 1 장 총 칙 2. 관련근거 가. 「개인정보 보호법」(이하 ‘법’이라 함) 나. 「개인정보 보호법 시행령」 다. 공단의 「개인정보 내부관리계획」	제 1 장 총 칙 2. 관련근거 가. 「개인정보 보호법」 나. 「개인정보 보호법 시행령」 다. 공단의 「개인정보 내부관리계획」 라. 「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시)(신설) 마. 기타 개인정보 보호 및 정보보안 관련 법령·고시·가이드라인(신설)
제 1 장 총 칙 3. 다른 지침 등과의 관계 개인정보 침해·유출사고 대응 등에 관하여 다른 규정 또는 지침에서 특별히 정한 것을 제외하고는 이 지침에 의함.	제 1 장 총 칙 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.

현행	개정안
제 1 장 총 칙 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 말함. 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 말함. 라. “정보수집”이란 특정 사이트나 개인정보처리시스템 및 네트워크에 대한 정보를 수집하기 위한 공격을 말함. 마. “시스템 침입”이란 개인정보처리시스템 또는 네트워크의 취약성을 이용하여 시스템에 침입하는 공격으로, 특정 취약점을 공격하는 해킹프로그램을 이용하거나, 잘못된 서버 운영상의 문제를 이용하여 침입함을 말함. 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 말함.	제 1 장 총 칙 4. 용어 정의 가. (현행과 동일) 나.~바. (내용은 현행과 동일하며, 문장 종결어미를 “~말함”에서 “~말한다”로 변경) 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.(신설)

현행	개정안																		
제 2 장 개인정보 침해·유출사고 개요 1. 개인정보 침해·유출사고 분류 가. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우 나. 개인정보가 저장된 DB 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우 다. 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우 라. 기타 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우	제 2 장 개인정보 침해·유출사고 개요 1. 개인정보 침해·유출사고 분류 <table><tr><th>분류</th><th>사 례</th></tr><tr><td>분실·도난</td><td>개인정보가 포함된 문서, 노트북, 휴대전화, 이동식 저장매체 등을 분실하거나 도난당한 경우</td></tr><tr><td>무단접근</td><td>개인정보처리시스템 또는 데이터베이스에 권한 없는 자가 접근한 경우</td></tr><tr><td>오전달·오발송</td><td>이메일·문자·팩스·우편·문서·파일 등을 권한 없는 수신자에게 전달한 경우</td></tr><tr><td>외부 해킹</td><td>취약점 악용, 계정 탈취, 악성코드, 랜섬웨어, 웹쉘, 불법접속 등으로 개인정보에 접근한 경우</td></tr><tr><td>내부자 오·남용</td><td>권한을 가진 자가 업무 목적을 벗어나 개인정보를 조회·복사·반출·제공한 경우</td></tr><tr><td>공개·노출</td><td>홈페이지, 게시판, 클라우드, 공유폴더, 출력물 등에서 개인정보가 불특정 또는 권한 없는 자에게 공개된 경우</td></tr><tr><td>수탁자 사고</td><td>위탁받은 업무를 수행하는 과정에서 수탁자 또는 재수탁자의 관리 소홀로 개인정보가 분실·도난·유출된 경우</td></tr><tr><td>기타</td><td>시스템 오류, 백업·복구 과정의 잘못된 처리, 파기 미흡, 출력물 방치 등으로 개인정보의 통제권을 상실한 경우</td></tr></table>	분류	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
분류	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																		
제 2 장 개인정보 침해·유출사고 개요 2. 개인정보 침해·유출사고 대응 방향 가. 개인정보 침해·유출사고 상황의 전반적인 개인정보보호 통제 수행	제 2 장 개인정보 침해·유출사고 개요 2. 개인정보 침해·유출사고 대응 방향 가. 사고 발생 전: 개인정보보호 정책·절차 수립, 담당조직 운영, 사고																		

현행	개정안
을 위한 침해·유출사고 대응팀 구성 - 체계화된 개인정보보호 정책 수립 등의 문서화 및 조직/인력에 대한 운영과 관리 나. 개인정보 침해·유출사고 대처 활동을 위한 조직 운영 - 개인정보보호 통제사항을 관리하기 위하여 담당부서는 개인정보 보호업무를 전담 운영·관리	대응 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.
제 3 장 개인정보 침해·유출사고 대응절차 ※ 아래 1~5절의 내용은 현행과 실질적으로 동일하며, 문장 종결어미가 명사형(“~함”, “~수립” 등)에서 서술형(“~한다”)으로 일괄 변경됨	
1. 개인정보 침해·유출사고 대응 방향 가. 개인정보보호 담당자는 유출 인원 등을 확인하여 [별지 제1호]의 통지방법에 따라 정보주체들에게 유출 통지 나. 수탁사업자가 수탁 업무를 처리하는 과정에서 개인정보가 유출된 경우 즉시 위탁자에게 보고하도록 위·수탁계약서에 명시하고, 수탁 사업자로부터 보고 받은 시점에서 지체 없이 유출 통지	1. 개인정보 침해·유출사고 대응 방향 가. (현행과 동일, “유출 통지한다.”로 어미 변경) 나. (현행과 동일, “유출 통지한다.”로 어미 변경)
2. 개인정보 침해·유출사고 절차 가. 1천명 이상의 고객에 관한 개인정보가 침해·유출된 경우에는 고객에 대한 통지 및 조치 결과를 72시간 이내에 공단에 보고 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 신고 다. 개인정보 침해·유출사고 보고 또는 신고는 별지 제1호 서식의 ‘개인정보 침해·유출 신고서’를 활용	2. 개인정보 침해·유출사고 절차 가.~바. (현행과 동일, 각 항목 “~한다.”로 어미 변경)

현행	개정안
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 가능 마. 1천명 이상의 고객에 관한 개인정보가 유출된 경우에는 통지와 함께 공단 홈페이지에 고객이 알아보기 쉽도록 7일 이상 게재할 수 있도록 개인정보 보호책임자에게 요청 바. 개인정보 침해·유출사고 신고는 별지 제2호 서식의 ‘개인정보 침해·유출 신고 관리대장’에 기록·관리	
3. 개인정보 침해·유출사고 보고 가. 개인정보 침해·유출사고가 발생한 것으로 확인된 때에는 개인정보 보호담당자는 지체 없이 개인정보 보호책임자에게 침해·유출 사고에 대한보고 나. 사고보고는 별지 제3호 서식 ‘개인정보 침해·유출사고 보고서’ 활용	3. 개인정보 침해·유출사고 보고 가.~나. (현행과 동일, “~한다.”로 어미 변경)
4. 개인정보 침해·유출사고 통지 가. 실제로 침해·유출 사고가 발생한 것으로 확인된 때에는 정당한 사유가 없는 한 72시간 이내에 해당 고객에게 아래사항 공지 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 필요 다. 침해·유출 사고의 조치를 취한 이후에는 고객에게 다음 아래의 사실만을 일차적으로 알리고, 추후 확인되는 즉시 알릴 수 있음 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 가능	4. 개인정보 침해·유출사고 통지 가.~라. (현행과 동일, 각 항목 “~한다.”로 어미 변경)

현행	개정안																
5. 개인정보 침해·유출사고 처리 및 종결 가. 공단에서는 개인정보 침해·유출사고 종결처리는 문서로 기록·관리 나. 개인정보 침해·유출사고에 대한 종결 처리되었음을 각 관련기관에 통지	5. 개인정보 침해·유출사고 처리 및 종결 가.~나. (현행과 동일, “~한다.”로 어미 변경)																
[별지 제2호] 개인정보 침해·유출 표준 통지문(안) ※ (현행과 동일) <table><tr><th>표준 통지문(안) 예시</th><th>부가 설명</th></tr><tr><td>(현행과 동일)</td><td>(현행과 동일)</td></tr><tr><td>(현행과 동일)</td><td>(현행과 동일)</td></tr><tr><td>▶ 피해 등 접수 담당부서 : 혁신성과팀 ▶ 피해 등 접수 전화번호 : 02-2061-3414 ▶ 피해 등 접수 e-메일주소 : lhj00@yys.or.kr</td><td>(현행과 동일)</td></tr></table>	표준 통지문(안) 예시	부가 설명	(현행과 동일)	(현행과 동일)	(현행과 동일)	(현행과 동일)	▶ 피해 등 접수 담당부서 : 혁신성과팀 ▶ 피해 등 접수 전화번호 : 02-2061-3414 ▶ 피해 등 접수 e-메일주소 : lhj00@yys.or.kr	(현행과 동일)	[별지 제2호] 개인정보 침해·유출 표준 통지문(안) ※ (현행과 동일) <table><tr><th>표준 통지문(안) 예시</th><th>부가 설명</th></tr><tr><td>(현행과 동일)</td><td>(현행과 동일)</td></tr><tr><td>(현행과 동일)</td><td>(현행과 동일)</td></tr><tr><td>▶ 피해 등 접수 담당부서 : 혁신성과팀 ▶ 피해 등 접수 전화번호 : 02-2061-3414 ▶ 피해 등 접수 e-메일주소 : ykhan@yys.or.kr</td><td>(현행과 동일)</td></tr></table>	표준 통지문(안) 예시	부가 설명	(현행과 동일)	(현행과 동일)	(현행과 동일)	(현행과 동일)	▶ 피해 등 접수 담당부서 : 혁신성과팀 ▶ 피해 등 접수 전화번호 : 02-2061-3414 ▶ 피해 등 접수 e-메일주소 : ykhan@yys.or.kr	(현행과 동일)
표준 통지문(안) 예시	부가 설명																
(현행과 동일)	(현행과 동일)																
(현행과 동일)	(현행과 동일)																
▶ 피해 등 접수 담당부서 : 혁신성과팀 ▶ 피해 등 접수 전화번호 : 02-2061-3414 ▶ 피해 등 접수 e-메일주소 : lhj00@yys.or.kr	(현행과 동일)																
표준 통지문(안) 예시	부가 설명																
(현행과 동일)	(현행과 동일)																
(현행과 동일)	(현행과 동일)																
▶ 피해 등 접수 담당부서 : 혁신성과팀 ▶ 피해 등 접수 전화번호 : 02-2061-3414 ▶ 피해 등 접수 e-메일주소 : ykhan@yys.or.kr	(현행과 동일)																
[별지 제3호] 개인정보 침해·유출 통지내용(예시) ((생략)) 당 공단은 조속한 범인 검거와 고객정보의 회수를 위하여 수사기관 및 관계 기관에 적극 협조할 것이며, 업계 전문가 및 관련 정부 기관들과 함께 유출 정보의 유포 방지 및 2차 피해 예방을 위하여 최선의 노력을 다할 것입니다. 관련하여 궁금한 점이 있으시면 아래 핫라인으로 연락주시기 바랍니다. 핫라인: 02-2061-3414 메일주소: lhj00@yys.or.kr (현행과 동일)	[별지 제3호] 개인정보 침해·유출 통지내용(예시) ((생략)) 당 공단은 조속한 범인 검거와 고객정보의 회수를 위하여 수사기관 및 관계 기관에 적극 협조할 것이며, 업계 전문가 및 관련 정부 기관들과 함께 유출 정보의 유포 방지 및 2차 피해 예방을 위하여 최선의 노력을 다할 것입니다. 관련하여 궁금한 점이 있으시면 아래 핫라인으로 연락주시기 바랍니다. 핫라인: 02-2061-3414 메일주소: ykhan@yys.or.kr (현행과 동일)																

현행	개정안
[별지 제4호] 고객의 대응방안 안내(예시) 개인정보 유출에 따른 2차 피해 예방을 위해 최선의 노력을 다하겠습니다. 배신자 파싱 배신자 유출된 비밀번호를 공인인증서로 로그인해 사기 보이스 파싱 음성으로 비밀번호를 입력 후 로그인 시도 스캠메일 차단 스캠메일로 유출된 비밀번호를 입력 후 로그인 시도 악성코드 바이러스 감염 악성코드에 감염된 컴퓨터로 로그인 시도 피싱방지 행동수칙 Do! 비밀번호를 정기적으로 변경 여러 사이트에서 동일한 비밀번호 사용은 피하고, 숫자, 특수 문자의 조합으로 변경해주세요. 보안백신을 설치, 주기적으로 업데이트 악성코드나 바이러스에 감염되지 않도록 주의해주세요. 최신 버전으로 업데이트하고 보안기능 설정 인터넷뱅킹사용 시 최신버전으로 유지하고 보안기능을 적극적으로 활용하세요. 사용하지 않는 백신, 메일, 바이러스 백신, 방화벽 등 보안 소프트웨어는 최신 버전으로 유지하고 보안기능을 사용하세요. Don't! 특정, 특정 출처의 비밀번호를 모든 사이트에 사용하는 습관을 올라라지 마세요. 불법사이트, P2P 금지 불법사이트나 불법 P2P서비스를 사용하지 마세요. 공용 PC 사용자 보안검사, 로그아웃! 사용 후 반드시 모든 프로그램을 로그아웃 해주세요. 공용 PC 사용자 자동로그인 금지 공용PC에서 개인용 프로그램을 자동로그인 / 재시도 : 비밀번호를 저장 기능을 해제해주세요.	[별지 제4호] 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 신상하지 않은 결제, 계좌이체, 휴대전화 개통, 소액결제 및 인증서 발급 내역이 있는지 확인합니다. 4 의심 연락 즉시 피면 협치 피싱스미어 문자, 메일, 전화번호, URL 및 접속기록은 삭제하고 전 직원에게 주의사항을 안내합니다. ⊗ 절대 하지 말아야 할 4가지 1 불분명한 링크·첨부파일 열기 금지 출처가 확실하지 않은 URL, 웹 사이트(link), 문서 첨부파일을 절대로 실행하지 않습니다. 2 민감 개인정보 및 인증번호 전달 금지 주요 개인정보(주민번호, 계좌·카드번호, 비밀번호, OTP) 인증번호를 전화·문자·메신저로 절대 전달하지 않습니다. 3 원격제어 및 앱 설치 요구 거절 피해 확인이나 보안/점검을 이유로 원격제어 앱이나 보안 앱 설치를 요구하면 즉시 통화를 종료합니다. 4 확인되지 않은 정보 온라인 확산 금지 유출 정보나 원인, 피해 규모가 공식 확인되지 않은 사실을 온라인이나 SNS에 전달하지 않습니다. ▲ 특히 이런 연락(사기/스미어)을 주의하세요! • 포상 및 환불 신청 형식: 발송 시에 포상금을 받으려다 특정 링크 입력이나 앱 설치를 유도하는 경우 • 보안 확인 문자: 유출 여부를 조회해주겠다며 아이디, 비밀번호, OTP 인증번호 입력을 요구하는 경우 • 가짜 사칭 송금 요구: 공단·경찰·금융감독관 직원을 사칭하여 계좌이체나 '인민계좌' 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, 휴대전화 개통 정지를 요청하세요. 2단계: 신고 & 상담 주요 신고기관 연결 • 경찰청: 112 • 금융감독원: 1332 • 개인정보침해신고센터: 118 3단계: 스미어 대응 보호나라 카카오톡 피싱스미어 URL, 문자 수신 시 카카오톡 '보호나라' 채널의 '스미어 피싱' 확인서 배스 를 이용하세요.