

개인정보 유출 등 사고 대응 매뉴얼

2026. 9.



부산광역시 남구시설관리공단

I. 개요	1
1. 필요성	1
2. 적용 범위	1
3. 용어정리	2
II. 정보 유출 등 유출 대응체계 구축	3
1. 개인정보 유출 등 사고 발생 사실 보고 체계	3
2. 개인정보 유출 등 사고 신속 대응팀 구성 및 운영	4
III. 피해 최소화 및 긴급 조치	6
1. 해킹에 의한 경우	6
2. 내부자가 유출한 경우	6
3. 이메일 오발송에 의한 경우	6
4. 개인정보 노출에 의한 경우	7
IV. 개인정보 유출 등 통지 및 신고	8
1. 개인정보 유출 등의 통지	8
2. 개인정보 유출 등의 신고	10
V. 정보주체 피해 구제 및 재발 방지	12
1. 정보주체의 피해 구제	12
2. 재발 방지 대책 마련	14
<부록>	
1. 관련 법률	15
2. 유출 등 신고서 양식	20
3. 해킹에 의한 유출 시 조치사항	21
4. 경찰 수사 및 침해사고 신고	23
5. 개인정보 유출에 따른 2차 피해 유형 및 대응방안	24

개인정보 유출사고 등 매뉴얼 개정사항

제·개정번호	일 자	제·개정 내용
1	2024. 6. 5.	• 부산광역시 남구시설관리공단 개인정보 유출사고 등 매뉴얼 제정
2	2026. 9. 18.	• 부산광역시 남구시설관리공단 개인정보 유출사고 등 매뉴얼 개정 - CPO 변경에 관한 사항 반영, 개인정보보호법 및 동법 시행령 개정 사항 현행화, 표준 개인정보 보호지침 개정사항 현행화

I. 개 요

1. 필요성

- ☐ 개인정보가 분실·도난·유출 사고가 발생 시 신속한 대응 및 조치를 통한 피해확산 방지 및 정보주체에 대한 피해구제
- * 개인정보의 분실·도난·유출(이하 “유출 등”이라 한다)이란 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것을 말함
- ☐ 개인정보의 종류, 처리하는 방법 및 환경, 개인정보 처리주체의 유형(성격) 등에 따라 다르게 적용될 수 있으므로 각각의 환경을 고려하여 개인정보 유출 등 사고 대응 매뉴얼 마련 필요

2. 적용범위

- ☐ 개인정보처리자가 개인정보 유출 시 「개인정보 보호법」 제34조 적용

근거 법률		개인정보 보호법
		제34조(개인정보 유출 등의 통지·신고)
법률간의 관계		일반법
적용 대상		개인정보처리자
적용 범위		개인정보 유출 등
의무 사항		통지 및 신고
벌칙 규정		3천만원 이하의 과태료
유출 통지	규모	1명 이상
	시점	72시간 이내
	방법	홈페이지, 서면 등의 방법으로 개별 통지
	항목	유출 등이 된 개인정보 항목, 유출 등이 된 시점과 그 경위, 유출 등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보 주체가 할 수 있는 방법 등에 관한 정보, 개인정보처리자 대응조치 및 피해 구제절차, 피해 신고·상담 부서 및 연락처 등
유출 신고	규모	1. 1천명 이상 2. 민감정보, 고유식별정보 유출 등 3. 외부로부터의 불법적인 접근에 의해 개인정보가 유출 등
	시점	72시간 이내
	기관	개인정보보호위원회 또는 한국인터넷진흥원(KISA)

3. 용어 정리

구분	용어설명
개인정보	· 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다. - 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 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다. - 가명 처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보
개인신용정보	· 기업 및 법인에 관한 정보를 제외한 살아 있는 개인에 관한 신용정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다. - 해당 정보의 성명, 주민등록번호 및 영상 등을 통하여 특정 개인을 알아볼 수 있는 정보 - 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 특정 개인을 알아볼 수 있는 정보
개인정보처리자	· 업무를 목적으로 개인정보파일을 운영하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
침해	· 법적 근거, 규정 또는 본인 동의에 의하지 않고 이루어지는 개인정보의 수집, 저장, 이용 및 제공, 파기 행위 일체를 말함
개인정보 유출	· 법령이나 개인정보 처리자의 자유로운 의사에 의하지 않고, 정보 주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 것
개인정보 노출	· 일반 인터넷 사용자가 해킹 등 특별한 방법을 이용하지 않고, 정상적으로 인터넷을 이용하면서 타인의 개인정보를 취득할 수 있도록 인터넷에 방치되어 있는 경우

II. 개인정보 유출 등 대응체계 구축

1. 개인정보 유출 등 사고 발생 사실 보고 체계

- 개인정보 유출 등 사실을 알게 된 경우, 개인정보 보호책임자는 즉시 개인정보처리자에게 보고하고 개인정보보호·정보보호 부서 등을 중심으로 “개인정보 유출 등 사고 신속 대응팀” 등을 구성하여 피해 확산 방지 및 최소화를 위한 조치 필요

이사장	의사 결정	· 이사장은 개인정보 침해관련 개인정보 보호책임자의 보고를 받음 · 사고 종료시까지의 대응방향을 포함한 최종 의사 결정
개인정보 보호책임자	유출대응 총괄	· 개인정보침해관련 접수사항과 접수 이후 추가 확인된 사항을 이사장에게 보고 · 개인정보 유출원인을 파악하여 필요시 개인정보 유출대응 신속대응팀을 구성 · 개인정보처리자의 의사 결정사항에 따른 개인정보 유출대응 총괄
개인정보 보호 담당자	사고접수 및 사실확인	· 개인정보 침해사고 및 사실 관계 확인 후 개인정보 보호책임자에게 보고 · 신고 내용의 사실 관계 확인을 유관부서 신고 내용 확인 요청
전 직원	사고신고 및 대응지원	· 개인정보 유출 또는 이상징후 확인시 개인정보 보호담당자에게 신고 · 개인정보 유출대응 신속대응팀 요청에 따른 유출대응 지원

- (전직원) 개인정보 유출 등 사실을 발견하거나 의심스러운 정황을 알게된 경우에는 즉시 개인정보 보호담당자에게 전화, 이메일 등으로 신고
- (개인정보 보호담당자) 신고를 받은 즉시 관련자에게 유출 등 규모, 경로 등 유출 등 사실 여부를 확인 요청하고, 개인정보 보호책임자에게 유출 등 사실 및 피해 규모, 대응 상황 등을 신속하게 보고
- (개인정보 보호책임자) 해당 시점까지 파악된 현황을 개인정보처리자에게 신속하게 보고하고 새로운 상황이 발생될 때마다 수시로 보고해야 하며, 개인정보 유출 등 사고가 확인되는 즉시 “개인정보 유출 신속대응팀(T/F)”을 운영
- (이사장) “개인정보 유출 등 사고 신속 대응팀”을 중심으로 유관부서가 유기적으로 대응하도록 지원하고 유출 등 대응에 대한 방향성 제시 등 의사결정 진행

2. 개인정보 유출 등 사고 신속 대응팀 구성 및 운영

- “개인정보 유출 등 사고 신속대응팀”을 운영하여 개인정보 유출 사고 발생에 따른 사고 분석, 처리, 사후 복구 및 예방 조치 등을 수행
- 개인정보 보호책임자를 중심으로 내부 조직 및 인력을 효율적으로 분배하여 유출 원인분석 및 대응, 유출 등 신고·통지, 이용자 피해 구제 등 고객지원 등으로 세분화하여 신속히 대응

□ 단계별 절차

단계	주요 내용	비고
사고 인지 긴급 조치	- 개인정보 유출 사고 인지 및 신고 접수 - 유출사고 발생이 의심되는 경우, 지체 없이 개인정보 보호담당자에게 신고 - 개인정보 보호담당자는 사고 내용 등에 대해 개인정보 보호책임자에게 보고 - 개인정보 유출 신고 등 사고 신속 대응팀 구성 - 피해 최소화를 위한 긴급 조치 수행 - 유출된 개인정보 비공개 또는 삭제 조치 - 유출 접속 경로 차단, 취약점 점검 및 보완 등 긴급조치, 재발방지 조치 등	개인정보 유출 시설 담당자, 개인정보 보호담당자, 개인정보 보호책임자
정보주체 유출통지	1건이라도 개인정보 유출 시, 정보주체에게 유출사실 통지 (72시간 이내) - 유출된 개인정보의 항목, 유출된 시점과 그 경위, 피해 구제절차 등	개인정보 보호책임자
개인정보 유출신고	1천명 이상의 정보주체에 관한 개인정보가 유출 등이 된 경우, 민감정보 또는 고유식별정보가 유출된 경우, 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출 등이 된 경우	개인정보 보호책임자
사고분석	- 개인정보 유출 신고 등 사고 신속 대응팀의 조사 및 분석 - 사고 원인 분석, 유출 규모 확인, 사고 원인에 대한 조치 등	개인정보 유출 등 사고 신속대응팀장
민원대응	- 민원대응을 위한 별도의 온/오프라인 창구를 개설 및 운영 - 피해자 구제방안, 수사 진행상황 등에 대한 답변 방향 결정 및 응대 2차 피해 방지를 위한 조치방법 안내 등 고객 불안 해소 조치 및 피해구제 절차 안내	개인정보 유출 시설 담당자, 민원부서장
유출사고 결과보고	개인정보 유출사고 결과보고서 작성 및 보고	개인정보 유출 등 사고 신속대응팀장
개선 및 이행점검	개인정보 유출사고 사례 전파 교육 및 개선 대책 시행(재발방지)	개인정보 보호책임자

□ 개인정보 유출 신속대응팀 업무절차(요약)

○ 개인정보 유출 신속대응팀 구성



○ 유출원인 파악 및 추가 유출 방지조치

신속 대응팀	· 개인정보 유출등 신고 접수 및 사실여부 확인 · 개인정보 유출 사고 원인 파악	· 접근통제, 모니터링 강화 · 유출된 개인정보 회수
--------	--	----------------------------------

○ 개인정보 유출 신고 및 통지

신속 대응팀			
↓	↓	↓	↓
개인정보 유출신고	개인정보 유출통지	침해사고 신고(필요 시)	경찰청(필요 시)
개인정보위원회 한국인터넷진흥원	이용자	과학기술정보통신부 한국인터넷진흥원	범죄신고

○ 이용자 피해구제 및 재발방지 대책 마련

신속대응팀	개인정보 유출 사고 전파	→	관계사
	이용자 피해구제, 개인정보 분쟁조정 안내	→	이용자
	재발방지 대책 수립	→	전직원

III. 피해 최소화 및 긴급 조치

1. 해킹에 의한 경우

- ☐ 개인정보 유출 원인을 파악한 후, 피해 최소화 등을 위해 취약점 제거 등 유출 원인을 제거하는 긴급 대응 조치를 실시
- ☐ 침해사고 발생으로 인해 개인정보가 유출된 사실을 알게 된 경우, 개인정보 추가 유출 방지를 위한 대책을 마련하고 피해를 최소화할 수 있는 조치 강구
 - 유출된 시스템 분리·차단 조치, 관련 로그 등 증거자료 확보, 유출 원인분석, 이용자 및 개인정보취급자 비밀번호 변경 등 기술적 보호조치 강화, 시스템 변경, 기술지원 의뢰 및 복구 등과 같은 긴급 조치를 시행
 - * 일방향 암호화되지 않은 비밀번호가 유출, 해커 등이 이용자의 비밀번호를 알고 있다고 판단되는 경우에는 이용자가 비밀번호를 변경하지 않으면 이용할 수 없도록 하고, 일방향 암호화된 비밀번호가 유출된 경우에도 비밀번호 변경을 유도하여 추가 피해 예방 방지
 - 사고원인 조사 등이 완료된 이후에는 개인정보 유출의 직·간접적인 원인을 즉시 제거하고, 취약점 개선 조치 등을 수행
 - ※ 긴급 조치 등이 어려운 경우에는 한국인터넷진흥원에 기술지원을 요청할 수 있음

2. 내부자가 유출한 경우

- ☐ 개인정보 유출자가 개인정보처리시스템에 접속한 이력 및 개인정보 열람·다운로드 등 내역 확인
- ☐ 개인정보 유출자의 개인정보처리시스템에 대한 접근·접속 경로 등이 정상적인지 여부 등을 확인, 비정상적인 접속인 경우 우회 경로를 확인하여 접속 차단
- ☐ 개인정보취급자의 개인정보처리시스템 접속계정, 접속권한, 접속기록 등을 검토하여 추가적인 유출 여부 확인
- ☐ 개인정보 유출에 활용된 단말기(PC, 스마트폰 등)와 매체(USB, 이메일, 출력물 등)를 회수, 필요시 수사기관 등과 협조하여 유출된 개인정보를 회수하기 위한 방법 강구

3. 이메일 오발송에 의한 경우

- ☐ 이메일 회수가 가능한 경우에는 즉시 회수 조치, 불가능한 경우에는 이메일 수신자에게 오발송 메일 삭제 요청
- ☐ 메일서버 외 첨부파일서버(대용량 메일 등)를 이용하는 경우 첨부파일서버 운영자에게 관련 파일 삭제 요청

4. 개인정보 노출에 의한 경우

- ☐ (검색엔진을 통한 노출의 경우) 노출된 사업자의 웹페이지 삭제를 검토하고, 검색엔진에 노출된 개인정보 삭제를 요청하여야 하며, 인증 절차 추가 및 로봇배제 규칙 적용 등 외부 접근 차단
- ☐ (시스템 오류로 인한 노출의 경우) 소스 코드 오류, 서버 설정 오류 등 개인정보가 노출된 원인이 된 시스템 오류를 파악하여 수정
- ☐ (개인정보취급자 부주의로 인한 노출의 경우) 게시글 및 첨부파일 내 개인정보 노출 부분을 마스킹 처리하여 게시

개인정보 유출 사고 대응 방안

개인정보 유출사고 예방

유출사고의 주요 원인으로 확인되는 기술적·관리적 안전조치에 관하여 사전 점검하고 개선조치 등 사고예방 활동이 필요

기술적 안전조치 예시



01 | 파일 업로드 취약점 예방

- 웹서버 내 이용자가 첨부하는 파일의 확장자를 제한
 - ※ (예시) 이미지 파일만 허용하는 경우 '.jpg', '.png', '.gif' 등의 확장자를 가진 파일만 허용
- 첨부할 수 있는 파일의 최대 크기를 제한
- 사용자가 파일 업로드 시 파일명을 임의로 변경하여 저장
- 사용자 및 업로드 폴더의 권한을 설정하여 권한이 있는 사용자만 업로드할 수 있도록 변경 등



02 | SQL 인젝션 취약점 예방

- 사용자가 입력한 데이터에 대해 특수 문자가 SQL 문법으로 인식되지 않도록 보안 조치 적용
 - ※ (예시) PHP 기준, mysql_real_escape_string() 함수 사용 등
- 예외 메시지가 노출되지 않게 설정하거나 일반적인 오류 메시지만 표시하여 정보를 추출하는 것을 방지
- 정기적인 웹 취약점 점검 진행(연 1회 이상) 및 웹 에디터 등 게시판 도구 업데이트(상시)
- 웹 방화벽을 사용하고 정기적으로 보안 업데이트 실시 등



03 | CSRF 인젝션 스텔링 예방

- 서버 및 보안장치에 접속을 시도하는 데이터를 분석하여 접근 일체치를 설정
 - ※ (예시) 동일한 IP에서 0분 간 Δ초 이상 접속을 시도하는 경우 등
- 일체치를 초과하여 접속하는 경우 해당 IP에서 서버 접근을 일정 시간 차단하고, 보안 담당자에게 알림 기능 등 활성화
- 개인정보처리시스템 모니터링으로 불법적이거나 비정상적인 접속 시도 등을 탐지 및 차단 필요
- 일정 횟수 이상 로그인 실패 시 로그인 절차에 추가적으로 2차 인증수단 또는 CAPTCHA 등을 추가하여 인증 강화 등
 - ※ 이외에도 비인가 접근통제 강화, 접근권한 최소화 관리, 지속적인 모니터링 통해 안전조치 필요

관리적 안전조치 예시



▶ 업무 과실 예방

- 다수의 수신자에게 메일 발송 시에는 '개별 발송' 또는 '숨은 참조' 기능을 활용하거나 발송 버튼 클릭 시 팝업 등으로 수신자재 확인
- 구글, 네이버 등 웹 설문조사 서비스 이용 시 설문 참여자·편지자의 정보 공개범위를 '비공개(제한됨)'로 설정하는 등 공개범위 설정
- 개인정보가 포함된 엑셀 파일을 외부 공개 시 개인정보를 '숨김'으로 처리하지 않고 삭제 후 게시
- 개인정보취급자의 개인정보 처리실태 점검 등 지속적인 관리·감독 실시 등

IV. 개인정보 유출 등의 통지 및 신고

1. 개인정보 유출 등 통지

☐ (통지 주체) 개인정보를 처리하는 “개인정보처리자”

☐ (통지 시점) 개인정보의 유출 등 사실을 알게 되었을 때

- 단, 유출 등이 된 개인정보의 확산 및 추가 유출 등을 방지하기 위해 긴급한 조치가 필요한 경우에는 해당 조치를 취한 후 지체없이 정보주체에게 알릴 수도 있음

※ 개인정보 유출 등 사고를 인지하지 못해 유출 등 통지가 지연된 경우에는 실제 유출 등 사고를 알게 된 시점을 입증하여야 함

☐ (통지 규모) 단 1명의 정보주체에 관한 개인정보가 유출 등이 된 경우 해당

☐ (통지 방법) 서면 등의 방법을 통하여 개별 통지가 원칙

- 단, 법에서 정한 일정규모 이상의 정보주체에 관한 개인정보가 유출 등이 된 경우에는 해당 법에서 정한 방법으로 통지
 - 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우, 인터넷홈페이지에 30일 이상 게시. 인터넷 홈페이지를 운영하지 아니하는 경우, 사업장 등의 보기 쉬운 장소에 30일 이상 게시

- 대규모 유출 등으로 72시간 이내 전체 통지가 기술적으로 불가능한 경우에는 홈페이지 팝업창 등을 통해 방문하는 이용자가 모두 알 수 있도록 현재까지 파악된 유출 등 사실을 게시를 하고 나서 추가적으로 해당 정보주체에게 개별적으로 통지

※ 유출 등 통지를 할 때에는 정보주체가 실제 확인 가능하도록 이용 빈도가 높은 방법을 우선 활용하여 통지하는 것이 바람직하며, 휴대전화번호를 보유하고 있는 경우에는 전 화통화 및 문자 등을 활용하고 곤란한 경우에는 이메일, 팩스, 우편 등의 방법을 활용

☐ (통지 내용) ① 유출 등이 된 개인정보 항목, ② 유출 등이 된 시점과 그 경위, ③ 정보주체가 취할 수 있는 피해 최소화 조치, ④ 개인정보처리자 대응조치 및 피해 구제절차, ⑤ 정보주체가 피해 신고·상담 등을 접수할 수 있는 부서 및 연락처 등을 통지

- 유출 등 통지하여야 하는 사항 중, 구체적인 내용이 확인되지 않은 경우에는 확인 된 내용을 중심으로 우선 통지, 추가로 확인되는 내용은 확인되는 즉시 통지

※ 구체적 사실관계 파악을 이유로 정보주체에게 유출 등 사실 통지를 지연하는 경우에는 3천만원 이하의 과태료가 부과될 수 있음

홈페이지 개인정보 유출 등 통지문(예시)

**개인정보 유출 사실을 통지해 드리며,
깊이 사과드립니다.**

① 고객님의 개인정보는 0000년 00월 00일 해커에 의한 홈페이지 내 악성코드가 삽입되어 00점이 유출된 것으로 확인되었습니다. 유출된 정확한 일시는 000에서 현재 수사가 진행 중이며, 확인 되면 추가로 알려 드리도록 하겠습니다.

② 유출된 개인정보 항목은 이름, 아이디(ID), 비밀번호(P/W), 이메일, 휴대전화번호 총 5개 항목입니다.

③ 유출 사실을 인지한 후 해당 악성코드는 즉시 삭제하였으며, 해커가 접속한 해당 IP와 우회 접속한 IP를 차단하고, 추가적인 홈페이지 취약점 점검과 보완 조치를 하였습니다. 더불어 침입방지시스템을 추가 도입하여 24시간 모니터링을 수행하고 있습니다.

④ 이번 사고로 인해 유출된 개인정보를 이용하여 웹사이트 명의도용, 보이스피싱, 피싱 등 2차 피해의 우려가 있으므로 혹시 모를 피해를 막기 위하여 고객님의 비밀번호를 변경하여 주시기 바랍니다.

⑤ **비밀번호 변경하기**

⑥ 개인정보 악용으로 의심되는 전화, 메일 등을 받으시거나 기타 궁금하신 사항은 아래 피해 등 접수 담당부서로 연락해주시기 바랍니다.

▶ 피해 등 접수 담당부서: 00000(000-2345-0000)

▶ 피해 등 접수 e-메일: 0000@0000.co.kr

⑦ 개인정보 유출 등으로 인하여 손해가 발생하였다면 개인정보 분쟁조정위원회에 분쟁조정을 신청하실 수 있습니다.

▶ 개인정보 분쟁조정 신청 : kopic.go.kr(1833-6972)

(주) 000 대표이사 000

⑧ 개인정보 유출 여부 조회하기

■ 개인정보 유출 통지문 작성 준수사항

① 개인정보 유출 등이 발생한 시점과 확인한 유출 건수를 누구나 이해할 수 있게 상세 하게 설명

※ 잘못된 사례: '일부 고객, 회원정보 일부' 등

② 유출된 개인정보 항목은 누락없이 모두 나열하여야 함

※ 잘못된 사례: '등'으로 생략하거나, 회사전화 번호, 잠금번호를 전화번호로 통지

③ 개인정보처리자 등의 대응 조치 내용

접속경로 차단 등 예시된 항목 외에도 망분리, 방화벽 설치, 개인정보 암호화, 인증 등 접근통제, 시스템 모니터링 강화 등 조치한 사항을 설명

④ 이용자가 취할 수 있는 조치 방법

유출된 개인정보, 경로 등에 따라 발생할 수 있는 피해를 추정하여 가능한 피해예방 조치를 모두 안내(예: 보이스피싱, 피싱메일, 불법 TM, 스톱모자 등)

⑤ 이용자의 비밀번호 변경페이지로 연결

⑥ 이용자가 상담 등을 접수할 수 있는 부서 및 연락처

전담처리부서 안내를 원칙으로 하되, 대량 유출로 일시적으로 콜센터 등 다른 부서를 지정한 경우 해당 부서를 안내

⑦ 개인정보 유출 등으로 손해가 발생하였을 경우 개인정보 분쟁조정위원회를 통하여 손해배상을 요구하는 분쟁조정을 신청할 수 있음을 안내

⑧ 이용자가 자신의 개인정보 유출여부를 조회할 수 있도록 절차를 마련

2. 개인정보 유출 등 신고

☐ (신고 주체) 개인정보를 처리하는 “개인정보처리자”

☐ (신고 시점) 최초 개인정보의 유출 등 사실을 알게 되었을 때로부터의 신고 시점을 말함

- 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우에는 해당 사유가 해소된 후 지체 없이 신고할 수 있으며, 개인정보 유출 등의 경위가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있음

☐ (신고 규모) 법에서 정하는 일정규모 이상의 정보주체에 관한 개인정보가 유출 등이 된 경우에는 신고해야 함

- ① 1천명 이상, ② 민감정보, 고유식별정보 유출 등, ③ 외부로부터의 불법적인 접근에 의해 개인정보가 유출 등

☐ (신고 방법) 개인정보 포털(privacy.go.kr)를 통해 개인정보 보호위원회 또는 한국인터넷진흥원(KISA)에 신고

☐ (신고 내용) 유출된 개인정보의 항목, 유출된 시점과 그 경위, 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보, 개인정보처리자의 대응조치 및 피해 구제절차, 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처를 서면등의 방법으로 제출

- 유출 등을 신고하여야 하는 사항 중, 구체적인 내용이 확인되지 않은 경우에는 그 때까지 확인된 내용을 중심으로 우선 신고하고, 추가로 확인되는 내용은 확인되는 즉시 신고하여야 함

☐ 개인정보 유출 등 신고서 작성 방법

유출 등 신고서 양식	작성 방법
① 유출 등이 된 개인정보 항목	• 유출 등이 된 개인정보 항목을 모두 기재해야 하며, ‘등’과 같이 일부 생략하거나 휴대전화번호와 집 전화번호를 ‘전화번호’로 기재하여서는 안됨 • 유출 등이 된 개인정보의 모든 항목을 적어야 하며, 유출 등 규모도 현 시점에서 파악된 내용을 모두 작성
② 유출 등이 된 시점과 그 경위	• 유출 등 시점, 인지시점을 명확히 구분하여 날짜 및 시간 모두 작성해야 하며, 유출 등 경위와 인지경위를 포함
③ 정보주체가 취할 수 있는 피해 최소화 조치	• 개인정보 유출 등으로 발생 가능한 스팸 문자, 보이스피싱, 금융 사기와 같은 2차적인 피해 방지를 위해 이용자가 할 수 있는 조치를 기재(예: 비밀번호 변경 등)
④ 개인정보처리자 대응조치 및 피해 구제절차	• 유출 등 사실을 안 후 긴급히 조치한 내용과 향후 이용자의 피해 구제를 위한 계획 및 절차를 기재 ex) 경찰에 신고, 일시적 홈페이지 로그인 차단(홈페이지 해킹일 경우) 등
⑤ 정보주체가 피해 신고·상담 등을 접수할 수 있는 부서 및 연락처	• 실제 신고 접수 및 상담이 가능한 전담 처리부서와 해당 담당자 연락처를 기재
⑥ 기타	• 유출 등이 된 기관명, 사업자번호, 사업자 주소, 웹사이트 주소 등 기재

V. 정보주체 피해 구제 및 재발 방지

1. 정보주체의 피해 구제

- ☐ **(유출 여부 조회)** 정보주체가 개인정보 유출 여부 등을 확인가능 하도록 별도의 홈페이지 등을 제공
 - 본인확인 수단으로 휴대전화, 이메일 인증 등을 활용 가능하나, 주민등록번호는 활용하지 않도록 주의
 - 해당 홈페이지를 통하여 추가적인 개인정보 유출이 발생하지 않도록 웹 취약점 제거, 전송구간 암호화 등 안전조치를 이행
- ☐ **(민원대응)** 개인정보 유출로 인한 정보주체의 피해 신고·접수, 상담·문의 등 각종 민원대응을 위한 방안을 모색
 - 개인정보 유출 문의에 신속히 대응할 수 있도록 상담 스크립트를 운영하고 전화, 이메일, 홈페이지, SNS 등 다양한 채널을 통해 개인정보 유출 사실, 경위 등을 확인할 수 있는 창구 마련
 - 유출 규모와 상황을 종합적으로 고려하여 원활한 민원 대응을 위해 민원 대응 전담부서 운영, 통신회선 증설 등이 필요
- ☐ **(현장 혼잡 최소화)** 유출 대응 현장에서의 긴급·돌발 상황 발생 등에 따른 혼란 최소화를 위한 방안을 강구
 - 현장에서 물리적 시스템 장애, 파괴 그리고 불필요한 인력 등으로 인하여 개인정보가 분실, 도난, 훼손되지 않도록 주의
- ☐ **(고객불안 해소)** 보이스피싱 등 2차피해 방지를 위한 유의사항을 사전 안내하고 유출·피해 및 대응 현황 등을 실시간으로 정확하고 투명하게 공개하는 등 고객 불안 해소를 위해 노력
- ☐ **(피해 구제)** 정보주체의 피해 구제 계획을 마련하고 개인정보 분쟁조정위원회, 손해배상제도 등도 함께 안내

☐ 관련 사이트

구분	화면
① 털린 내 정보 찾기	사이트명: 털린 내 정보 찾기 서비스 
② 본인확인 내역조회	사이트명: 개인정보포털 
③ 웹사이트 회원탈퇴	사이트명: 개인정보포털 
④ 지우개(잊힐권리) 서비스	사이트명: 개인정보포털 
⑤ 개인정보 분쟁조정위원회	사이트명: 개인정보 분쟁조정위원회 

2. 재발 방지 대책 마련

- ☐ 개인정보 유출 원인, 취약점 등에 적절한 대책을 마련하고 개인정보 취급자 대상 개인정보보호 교육을 정기적으로 실시
- ☐ 개인정보 유출 대응 시나리오 작성 및 모의훈련 등을 실시하여 유출 대응 체계를 점검하고 지속적으로 보완
- ☐ 홈페이지 취약점 등으로 인한 유출 사고 예방을 위해 안전조치를 강화
 - 홈페이지의 취약점을 연 1회 이상 정기적으로 점검
 - 개인정보가 인터넷상에 노출되는 것을 방지하기 위해 인증 절차 추가 및 로봇 배제 규칙을 적용하여 홈페이지 접근을 제한
 - 홈페이지에 첨부파일을 포함한 게시물 작성 시 개인정보 포함 여부를 확인
 - 홈페이지 게시판 등에 정보주체가 글 작성 시 개인정보가 노출되지 않도록 주의할 것을 안내
 - 관리자 페이지에 접근하는 IP를 제한하거나 아이디, 비밀번호 외 추가적인 인증수단을 사용하여 접속

부록1 관련 법률

1. 개인정보 유출 사고 대응 계획 수립·시행

☐ 「개인정보 보호법」

법 제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

시행령 제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다.

1. 개인정보의 안전한 처리를 위한 다음 각 목의 내용을 포함하는 내부 관리계획의 수립·시행 및 점검
 - 가. 법 제28조제1항에 따른 개인정보취급자(이하 “개인정보취급자”라 한다)에 대한 관리·감독 및 교육에 관한 사항
 - 나. 법 제31조에 따른 개인정보 보호책임자의 지정 등 개인정보 보호 조직의 구성·운영에 관한 사항 다. 제2호부터 제8호까지의 규정에 따른 조치를 이행하기 위하여 필요한 세부 사항

개인정보의 안전성 확보조치 기준(고시), 시행령 제30조제1항 관련

제4조(내부 관리계획의 수립·시행) ① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다. 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있다.

12. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항

2. 개인정보 유출 등 사고 대응 매뉴얼 마련

☐ 「개인정보 보호법」

법 제12조(개인정보 보호지침) ① 보호위원회는 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 표준 개인정보 보호지침(이하 “표준지침”이라 한다)을 정하여 개인정보 처리자에게 그 준수를 권장할 수 있다.

표준지침 제29조(개인정보 유출 등 사고 대응 매뉴얼 등) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리자는 유출 등 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 「개인정보 유출 등 사고 대응 매뉴얼」을 마련하여야 한다.

1. 법 제2조제6호에 따른 공공기관
 2. 그 밖에 1천명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리자
- ② 제1항에 따른 개인정보 유출 등 사고 대응 매뉴얼에는 유출 등 통지·조치 절차, 영업점·인터넷회선 확충 등 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불만 해소조치, 피해자 구제조치 등을 포함하여야 한다.
- ③ 개인정보처리자는 개인정보 유출 등에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

3. 개인정보 유출 등의 통지 및 신고

☐ 「개인정보 보호법」

제34조(개인정보 유출 등의 통지·신고) ① 개인정보처리자는 개인정보가 유출등이 되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.

1. 유출등이 된 개인정보의 항목
2. 유출등이 된 시점과 그 경위
3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 구체적인 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
6. 개인정보 유출등으로 인한 제39조에 따른 손해배상과 제39조의2에 따른 법정손해배상의 청구 및 제43조에 따른 분쟁조정 등 피해를 입은 정보주체의 법적 권리와 그 행사 방법 등에 관한 정보
7. 그 밖에 개인정보가 유출등이 된 정보주체의 보호를 위하여 대통령령으로 정하는 사항

② 제1항에도 불구하고 개인정보의 유형, 정보주체에게 미치는 영향 및 유출등의 위험 정도를 고려하여 대통령령으로 정하는 유출등의 가능성이 있음을 알게 되었을 때에는 지체 없이 유출등의 가능성이 있는 모든 정보주체에게 피해를 최소화하기 위한 정보 등 대통령령으로 정하는 사항을 알려야 한다.

③ 개인정보처리자는 개인정보가 유출등이 된 경우에는 해당 개인정보의 회수·삭제 등 피해 확산을 방지하기 위한 조치를 포함하여 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

④ 개인정보처리자는 개인정보의 유출등이 있음을 알게 되었을 때에는 개인정보의 유형, 유출등의 경로 및 규모 등을 고려하여 대통령령으로 정하는 바에 따라 제1항 각 호의 사항을 지체 없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 보호위원회 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

⑤ 제1항·제2항에 따른 통지 및 제4항에 따른 유출등의 신고의 시기, 방법, 절차 등에 필요한 사항은 대통령령으로 정한다.

시행령 제39조(개인정보 유출 등의 통지) ① 개인정보처리자는 개인정보가 유출등이 되었음을 알게 되었을 때에는 서면등의 방법으로 72시간 이내에 법 제34조제1항 각 호의 사항을 정보주체에게 알려야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 해당 사유가 해소된 후 즉시 정보주체에게 알릴 수 있다.

1. 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출등이 된 개인정보의 회수·삭제 등 긴급한 조치가 필요한 경우
2. 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우

② 제1항에도 불구하고 개인정보처리자는 같은 항에 따른 통지를 하려는 경우로서 법 제34조제1항제1호 또는 제2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출등이 된 사실, 그 때까지 확인된 내용 및 같은 항 제3호부터 제6호까지의 사항을 서면등의 방법으로 우선 통지해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지해야 한다.

③ 제1항 및 제2항에도 불구하고 개인정보처리자는 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 법 제34조제1항 각 호 외의 부분 단서에 따라 같은 항 각 호의 사항을 정보주체가 쉽게 알 수 있도록 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제1항 및 제2항의 통지를 갈음할 수 있다. 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 사업장등의 보기 쉬운 장소에 법 제34조제1항 각 호의 사항을 30일 이상 게시하는 것으로 제1항 및 제2항의 통지를 갈음할 수 있다.

제39조의2(개인정보 유출등의 가능성 통지 대상) ① 법 제34조제2항에서 “대통령령으로 정하는 유출등의 가능성이 있음을 알게 되었을 때”란 다음 각 호의 구분에 따른 때를 말한다.

1. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 불법적인 접근이 발생하여 개인정보 유출등이 의심되는 정황이 있으나 그 개인정보의 정보주체를 특정하기 곤란한 경우: 해당 불법적인 접근을 알게 된 때
 2. 개인정보처리자가 처리하는 개인정보가 법, 이 영 또는 개인정보 보호에 관한 다른 법령을 위반하여 제3자에 의해 거래되는 등 일부 개인정보가 유출등이 된 사실이 확인된 경우로서 다른 정보주체에 관한 개인정보도 유출등이 되었을 수 있다고 인정되는 경우: 해당 사실을 알게 된 때
- ② 법 제34조제2항에서 “피해를 최소화하기 위한 정보 등 대통령령으로 정하는 사항”이란 다음 각 호의 사항을 말한다.
1. 유출등의 가능성이 있는 개인정보의 항목
 2. 유출등이 있었을 것으로 의심 또는 인정되는 시점과 그 경위
 3. 법 제34조제1항제3호부터 제5호까지의 사항
 4. 유출등의 여부가 확정될 경우 추가 통지를 하겠다는 사실

제39조의3(개인정보 유출등의 가능성 통지 시기·방법 등) ① 개인정보처리자는 법 제34조제2항에 따라 제39조의2제2항 각 호의 사항을 통지하려는 경우 같은 조 제1항 각 호의 구분에 따른 때부터 72시간 이내에 서면등의 방법으로 통지해야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 기한 내에 통지하기 곤란한 경우에는 해당 사유가 해소된 후 즉시 통지해야 한다.

② 개인정보처리자는 제1항에 따른 기한 내에 개인정보가 실제로 유출등이 된 사실을 확인한 경우에는 법 제34조제2항에 따른 통지에 갈음하여 같은 조 제1항에 따른 통지를 해야 한다.

③ 법 제34조제2항에 따른 통지를 한 개인정보처리자는 개인정보가 실제로 유출등이 되지 않은 사실을 확인한 경우 즉시 정보주체에게 그 사실을 통지해야 한다.

④ 개인정보처리자는 법 제34조제2항 또는 이 조 제3항에 따른 통지의 대상인 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 개인정보 유출등의 가능성(제39조의2제2항 각 호의 사항을 포함한다) 또는 개인정보가 실제로 유출등이 되지 않은 사실을 정보주체가 쉽게 알 수 있도록 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 법 제34조제2항 및 이 조 제3항의 통지를 갈음할 수 있다. 다만, 인터넷 홈페이지를 운영하지 않는 개인정보처리자의 경우에는 사업장등의 보기 쉬운 장소에 30일 이상 게시하는 것으로 법 제34조제2항 및 이 조 제3항의 통지를 갈음할 수 있다.

제40조(개인정보 유출 등의 신고) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우로서 개인정보가 유출등이 되었음을 알게 되었을 때에는 72시간 이내에 법 제34조제1항 각 호의 사항을 서면등의 방법으로 보호위원회 또는 같은 조 제4항 전단에 따른 전문기관에 신고해야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 즉시 신고할 수 있으며, 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권리 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있다.

1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우
 2. 민감정보 또는 고유식별정보가 유출등이 된 경우
 3. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우
- ② 제1항에도 불구하고 개인정보처리자는 제1항에 따른 신고를 하려는 경우로서 법 제34조제1항제1호 또는 제2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출등이 된 사실, 그 때까지 확인된 내용 및 같은 항 제3호부터 제5호까지의 사항을 서면등의 방법으로 우선 신고해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 신고해야 한다.
- ③ 법 제34조제3항 전단 및 후단에서 “대통령령으로 정하는 전문기관”이란 각각 한국인터넷진흥원을 말한다.

표준지침 제25조(개인정보의 유출등) 개인정보의 분실·도난·유출(이하 "유출등"이라 한다)은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것을 말한다.

표준지침 제26조(유출등의 통지시기 및 항목) ① 개인정보처리자는 개인정보가 유출등이 되었음을 알게 된 때에는 72시간 이내에 해당 정보주체에게 다음 각 호의 사항을 알려야 한다.

1. 유출등이 된 개인정보의 항목
 2. 유출등이 된 시점과 그 경위
 3. 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
 4. 개인정보처리자의 대응조치 및 피해구제절차
 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
- ② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 해당 사유가 해소된 후 지체 없이 정보주체에게 알릴 수 있다.
1. 유출등이 된 개인정보의 확산 및 추가 유출등을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출등이 된 개인정보의 회수·삭제 등 긴급한 조치가 필요한 경우
 2. 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 통지하기 곤란한 경우
- ③ 개인정보처리자는 제1항 각 호의 사항을 모두 확인하기 어려운 경우에는 정보주체에게 다음 각 호의 사실만을 우선 알리고, 추후 확인되는 즉시 알릴 수 있다.
1. 정보주체에게 유출등이 발생한 사실
 2. 제1항의 통지항목 중 확인된 사항
- ④ 개인정보처리자는 개인정보 유출등의 사고를 인지하지 못해 유출등의 사고가 발생한 시점으로부터 72시간 이내에 해당 정보주체에게 개인정보 유출등의 통지를 하지 아니한 경우에는 실제 유출등의 사고를 알게 된 시점을 입증하여야 한다.

표준지침 제27조(유출등의 통지방법) ① 개인정보처리자는 정보주체에게 제26조제1항 각 호의 사항을 통지할 때에는 서면등의 방법을 통하여 정보주체에게 알려야 한다.

② 개인정보처리자는 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 법 제34조제1항 각 호 외의 부분 단서에 따라 같은 항 각 호의 사항을 정보주체가 쉽게 알 수 있도록 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제1항의 통지를 갈음할 수 있다. 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 사업장등의 보기 쉬운 장소에 법 제34조제1항 각 호의 사항을 30일 이상 게시하여야 한다.

표준지침 제28조(개인정보 유출등의 신고) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우로서 개인정보가 유출등이 되었음을 알게 되었을 때에는 72시간 이내에 제26조제1항 각 호의 사항을 서면등의 방법으로 보호위원회 또는 한국인터넷진흥원에 신고해야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 72시간 이내에 신고하기 곤란한 경우에는 해당 사유가 해소된 후 지체 없이 신고할 수 있으며, 개인정보 유출등의 경위가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권리 침해 가능성이 현저히 낮아진 경우에는 신고하지 않을 수 있다.

1. 1천명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우
 2. 민감정보, 고유식별정보가 유출등이 된 경우
 3. 개인정보처리시스템 또는 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 대한 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우
- ② 제1항에 따른 신고는 별지 제1호서식에 따른 개인정보 유출등 신고서를 통하여 하여야 한다.

③ 개인정보처리자는 개인정보 포털(www.privacy.go.kr)을 통하여 유출등 신고를 할 수 있다.

④ 개인정보처리자는 제1항에 따른 신고를 하려는 경우로서 법 제34조제1항제1호 또는 제2호의 사항에 관한 구체적인 내용을 확인하지 못한 경우에는 개인정보가 유출등이 된 사실, 그때까지 확인된 내용 및 같은 항 제3호부터 제5호까지의 사항을 서면등의 방법으로 우선 신고해야 하며, 추가로 확인되는 내용에 대해서는 확인되는 즉시 신고해야 한다.

표준지침 제29조(개인정보 유출등 사고 대응 매뉴얼 등) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리자는 유출등 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 「개인정보 유출등 대응 매뉴얼」을 마련하여야 한다.

1. 법 제2조제6호에 따른 공공기관
 2. 그 밖에 1천명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리자
- ② 제1항에 따른 개인정보 유출등 대응 매뉴얼에는 유출등 통지·조치 절차, 영업점·인터넷회선 확충 등 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다.
- ③ 개인정보처리자는 개인정보 유출등에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

표준지침 제30조(개인정보 침해 사실의 신고 처리 등) ① 개인정보처리자의 개인정보 처리로 인하여 개인정보에 관한 권리 또는 이익을 침해받은 사람은 법 제62조제2항에 따른 개인정보 침해 신고센터에 침해 사실을 신고할 수 있다.

② 제1항에 따른 개인정보침해 신고센터는 다음 각 호의 업무를 수행한다.

1. 개인정보 처리와 관련한 신고의 접수·상담
2. 개인정보 침해 신고에 대한 사실 조사·확인 및 관계자의 의견 청취
3. 개인정보처리자에 대한 개인정보 침해 사실 안내 및 시정 유도
4. 사실 조사 결과가 정보주체의 권리 또는 이익 침해 사실이 없는 것으로 판단되는 경우 신고의 종결 처리
5. 법 제43조에 따른 개인정보 분쟁조정위원회 조정 안내 등을 통한 고충 해소 지원

부록2 유출 등 신고서 양식

「(개인정보보호위원회) 표준 개인정보 보호 지침」 [별지 제1호서식]

개인정보 유출신고서

기관명					
유출등이 된 개인정보 항목 및 규모					
유출된 시점과 그 경위					
유출등 피해 최소화를 위해 정보주체가 할 수 있는 방법 등					
개인정보처리자의 대응 조치 및 피해 구제절차					
정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처					
유출등 신고 담당자		성명	부서	직위	연락처
	개인정보 보호책임자				
	담당자				

유출등 신고 접수기관	기관명	담당자명	연락처

부록3 해킹에 의한 유출 시 조치사항

1. 해커가 삽입한 악성코드 확인 및 삭제

- ☐ 한국인터넷진흥원에서 배포중인 '휘슬'을 활용하여 웹서버에 삽입된 악성코드와 웹shell 파일을 찾아서 삭제

※ 악성코드 탐지도구 제공 페이지 : KISA 보호나라 → 다운로드 → 휘슬 / 캐슬

2. 침해 발생 시스템의 계정, 로그 등을 점검하여 침해 현황 확인

점검 항목	점검 내용	비고
계정	- 사용하지 않는 계정 및 숨겨진 계정 확인 - 윈도우 : [관리도구] → [컴퓨터 관리] → [로컬 사용자 및 그룹] → [사용자] 정보 확인 - 리눅스 : /etc/passwd 확인	\$ 문자가 포함된 계정 확인 - 패스워드 미설정 계정 확인 /bin/bash 설정 계정 확인
로그파일	- 이벤트 로그 및 시스템 로그 변조 유무 확인 - 윈도우 : [관리도구] → [컴퓨터 관리] → [이벤트 뷰어] 확인 - 리눅스 : /var/log/secure, message 등 확인 - 윈도우 웹로그 경로 및 변조 유무 확인 [관리도구] → [인터넷정보서비스(IIS)관리]에서 - 리눅스 웹로그 경로 확인 /usr/local/apache/logs 확인	웹로그 생성/수정 시간 확인
웹shell	- 확장자별 웹shell 패턴 점검 - asp, aspx, asa, cer, cdx, php, jsp, html, htm, jpg, jpeg, gif, bmp, png	휘슬 사용
백도어	- 네트워크 상태 확인 - nmap -sV 침해사고시스템IP - 비정상 포트 및 외부연결 확인 - 윈도우: netstat, TCPView 등 사용 - 리눅스: netstat -nlp, lsof -i	6666, 6667 등 의심 Port 확인 - 의심 Port를 사용하는 프로세스 확인
루트킷	- 숨겨진 프로세스 및 비정상 프로세스 확인 - 변조된 파일 및 시스템 명령어 확인 - Windows: IceSword, GMER 등 사용 - Linux: Rootkit Hunter, Check Rootkit 등 사용	Rootkit Hunter 업데이트 필수

3. 로그분석 결과에 따른 접속경로 차단 등

- ☐ 로그 분석 결과 침입자 접속경로가 확인된 경우 접속경로를 차단하고 경유한 시스템은 추가적인 분석

구분	접속 경로 차단 방법	비고
서버	• 윈도우 [제어판]→[Windows 방화벽]→[일반]방화벽 사용 → [예외] → 원격데스크톱 → 편집 → 범위변경 → 사용자 지정 목록 설정(허용할IP)	특정 IP에 원격데스크톱 서비스를 허용하고 나머지 IP접속은 차단
	• 리눅스 iptables -A INPUT -p TCP --dport 22 -s 허용할IP -j ACCEPT iptables -A INPUT -p TCP --dport 22 -s -j DROP	특정 IP에 ssh 서비스를 허용하고 나머지 IP접속은 차단
네트워크	• 방화벽/라우터/스위치 access-list 101 permit tcp 허용할IP host 접근서버 IP eq 22 interface ethernet 0 ip access-group 101 in	특정 IP에 ssh 서비스 허용정책을 ethernet 0 인터페이스에 인바운드 정책 적용

4. 기타 조치사항

- ☐ 서버, PC 등 정보처리시스템의 백신을 최신으로 업데이트하고 전체 디렉토리를 점검
- ☐ 직원 PC의 운영체제, 오피스 프로그램의 보안 업데이트를 실시
- ☐ 가능한 경우 침해사고 원인을 식별하고 재발방지를 위해 개인정보 유출 시스템의 휘발성 및 비휘발성 정보 수집
- 기술적인 사항은 한국인터넷진흥원이 배포하는 「침해사고 분석절차 안내서」 참조
- ※ 제고 페이지: 한국인터넷진흥원/ 자료실/ 관련법령·기술안내서/ 기술안내 가이드 내
- ☐ 수사기관과 협조하여 유출된 개인정보를 회수하기 위한 조치를 강구

부록4 경찰 수사 및 침해사고 신고

1. 경찰수사

- ☐ 해커 등 개인정보 유출자 검거 및 개인정보 회수를 위한 조치가 필요한 경우에는 경찰청 사이버 안전국에 범인 검거를 위한 수사를 요청하고 유출된 개인정보 회수를 위한 조치를 실시

※ 사이버범죄 신고 : 경찰청 → 신고/지원 → 사이버범죄 신고/상담



2. 침해사고 신고

- ☐ 해킹 등 침해사고가 발생하면 즉시 관계 기관에 신고하여 사고 원인분석 및 취약점 보완조치 등을 실시

- 공공부문 : 국가정보원
- 민간부문 : 과학기술정보통신부 또는 한국인터넷진흥원

※ 침해사고 신고 : KISA 보호나라 → 침해사고 신고 → 신고하기, ☎ 국번없이 118



부록5 개인정보 유출에 따른 2차 피해 유형 및 대응방안

구분	피해종류	활용된 개인정보 주요항목	개인정보 악용절차	정보주체 대응 방안
금전적	온라인 사기쇼핑	주민등록번호, 카드번호, 유효기간 등	① 카드번호, 유효기간으로 온라인 결제가 가능한 국내외 홈쇼핑 사이트에 접속 ② 홈쇼핑 홈페이지, ARS를 통한 온라인 사기 결제·주문	• 신용카드 정지 및 재발급 신청 ※ 신고기관 : 각 카드사, 한국 소비자원 소비자 상담센터 (☎1372) 등
	명의도용을 통한 통신서비스 가입	이름, 주소, 주민등록번호 등	① 유출된 개인정보를 이용하여 휴대전화, 인터넷전화 등 가입 ※ 통신서비스 가입 시 본인확인절차가 있으므로 주민등록증 위조 등 추가적인 불법 행위 수반이 예상됨 ② 불법 가입한 전화번호로 스팸을 발송하여 금전적 이익을 취득함 ※ 명의를 도용당한 사람은 서비스 이용제한을 당하거나 명의도용 소명절차를 밟는 등 피해를 당함	• 한국정보통신진흥협회(KAIT)의 명의도용 방지서비스(M-Safer)를 통한 불법 통신서비스 신규 가입 여부 확인 ※ 신고기관 : 통신민원조정센터(msafer.or.kr) ※ 명의도용방지서비스(M-Safer) 통신서비스 신규가입 시 이메일·문자로 가입여부 통보
	명의도용을 통한 신용정보 복제	이름, 신용카드 번호, 유효기간 등	① 유출된 개인정보를 이용하여 신용카드 불법 복제 ※ 특수장비를 이용하여 카드번호, 유효기간, 이름 등으로 복제 가능 ② 불법 복제된 카드를 국내외에서 활용하여 상품 결제 등에 악용 ※ 국내외 POS단말기의 경우 마그네틱 부분만을 이용하여 결제 가능	• 신용카드 정지 및 재발급 신청, 이용내역 통지 서비스 가입 ※ 신고기관 : 각 카드사, 경찰, 금융감독원(☎1332)
	스미싱	휴대전화번호	① '정보유출 확인 안내' 등 금융기관을 사칭하는 문자메시지에 악성코드(인터넷주소)를 삽입하여 발송 ② 금융기관 사칭 메시지를 받은 피해자가 인터넷주소(URL)를 클릭하면 악성코드에 감염되어 소액결제 피해 및 개인·금융정보 탈취	• 수상한 문자메시지 삭제 및 메시지 상 링크 클릭하지 않기 또는 카드사 공지 전화 번호 확인 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☎118)

구분	피해종류	활용된 개인정보 주요항목	개인정보 악용절차	정보주체 대응 방안
비금전적	보이스피싱	신용카드번호, 휴대전화, 집전화번호, 집주소 등	① 경찰, 금융감독당국 또는 금융회사 직원을 사칭하여 전화 ② 금융관련 업무 목적 사칭을 통한 개인정보·금융정보 탈취(비밀번호, 보안카드번호 등) ③ 유출된 금융사를 사칭, 개인정보 유출 확인을 빙자하여 ARS를 통해 계좌번호/비밀번호 등 금융정보 입력 요청	• 수상한 전화 거부 및 각 카드사에서 공지한 전화번호 확인 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☎118)
	명의도용을 통한 온라인회원 가입	이름, 이메일, 연락처 등	① 유출된 개인정보를 이용하여 웹사이트 가입 ※ 일부 홈페이지의 경우 이름, 이메일, 연락처만으로 회원가입 가능 ② 명의도용을 통해 본인도 모르는 수십 여개의 웹사이트 가입하여 개인정보 불법 이용	• e프라이버시 클린서비스(www.eprivacy.go.kr)를 활용한 해당 사이트 탈퇴 요청 ※ 신고기관 : 경찰, 불법스팸대응센터(☎118) ※ 국내 사이트로 주민번호 사용 내역이 있는 경우만 가능하며, 주민번호 마스킹 시 서비스 불가
	휴대전화/ 이메일 스팸발송	휴대전화 번호, 이메일 주소 등	① 유출된 개인정보를 이용해 불특정 다수에게 스팸 발송 ※ 유출된 모든 휴대전화, 이메일로 도박 등 스팸 무작위 발송 가능 ※ 신용정보, 연소득 등 활용 대출 스팸 발송, 자동차 보유여부를 활용한 보험 스팸 발송 등 특정유형의 개인에 대한 타겟 마케팅 가능 ② 휴대전화, 이메일 서비스 이용자는 원치 않는 홍보·마케팅 광고 수신	• 지능형 스팸차단서비스를 이용한 스팸 차단, 수신 스팸 적극 신고 ※ 신고기관 : 카드사, 경찰, 불법스팸대응센터(☎118) ※ 지능형 스팸차단서비스 : 발신·회신번호 등 발송패턴을 분석하여 스팸을 차단해주는 서비스
	사회공학적 기법을 활용한 유포메일 발송	이메일주소 등	① 해커가 특정 대상을 목표로 스팸/피싱 시도용 첨부파일이 포함되어 있거나 연결을 유도 URL이 포함된 이메일 발송 ② 수신자들이 이메일에 포함된 첨부파일 및 URL을 클릭 ③ 해커가 수신자의 PC를 장악하여 기밀 및 개인정보를 빼냄	• 의심가는 이메일을 받은 경우 첨부파일 열람하지 않고 바로 삭제 • 사용자 PC의 바이러스 백신을 항상 최신버전으로 유지 및 정기적 검사 수행 ※ 신고기관 : 경찰, 불법스팸대응센터(☎118)