개인정보 침해 · 유출사고 대응지침

2016. 3.

[목 차]

제 1 장 총 칙

1. 목적

센터 내부의 과실 및 오·남용 또는 외부 해킹 등으로 개인정보 침해·유출 사고가 발생할 경우, 체계적이고 신속한 대응이 이루어져 피해를 최소화하려는데 목적이 있음.

2. 관련근거

가.「개인정보 보호법」(이하 '법'이라 함)
나.「개인정보 보호법 시행령」
다.「개인정보 보호법 시행규칙」
라.「표준 개인정보 보호지침」(행정자치부 고시 제2011-45호)
마. 센터의 「정보보안지침」
바. 센터의 「개인정보 내부관리계획」

3. 다른 지침 등과의 관계

개인정보 침해·유출사고 대응 등에 관하여 다른 규정 또는 지침에서 특별히 정한 것을 제외하고는 이 지침에 의함.

4. 용어 정의

가. "침해·유출"이란 법령이나 센터의 자유로운 의사에 의하지 않고, 고객의 개인정보에 대하여 센터가 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 이용하

여 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.

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

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

2. 개인정보 침해·유출사고 대응 방향

가. 개인정보 침해·유출사고 상황의 전반적인 개인정보보호 통제 수행을 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

3. 개인정보 침해·유출사고 대응 업무분장

구분	분장내용	담당		비고
발생 전 (대응방안)	○ 개인정보보호 통제를 위한 정책 수립	센터	개인정보 보호책임자	전략 수립
	○ 개인정보보호 통제를 위한 절차 수립	정보관리실	개인정보 보호담당자	
	○ 개인정보보호 활동을 위한 조직 구성			
발생 후	○ 개인정보 침해·유출사고 발생에 따른 정보 수집	정보관리실	개인정보 보호담당자	지침 이행
	○ 사고 발생에 따른 개별취재 등 언론대응(홍보 관련 부서 협조) - 대 고객 사과문 발표 등			
	○ 대응방안 취합 및 대책반 구성·개최 준비			
	○ 위험 상황 전사 공유(전 부서 협조)			
	○ 대응방안 검토 결과 대응방침 결정	센터	개인정보 보호책임자	

제 3 장 개인정보 침해·유출사고 대응절차

1. 개인정보 침해·유출사고 신고

가. 1천명 이상의 고객에 관한 개인정보가 침해·유출된 경우에는 고객에 대한 통지 및 조치 결과를 5일 이내에 센터에 보고

나. 고객에 관한 개인정보가 1천명 이상의 침해·유출된 경우에는 고객에 대한 통지 및 조치결과를 5일 이내에 센터 이사장과 교육부장관을 경유하여 행정자치부장관 또는 한국정보화진흥원 또는 한국인터넷진흥원 중 어느 하나에 신고

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

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. 1만명 이상의 고객에 관한 개인정보가 유출된 경우에는 통지와 함께 센터

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

2. 개인정보 침해·유출사고 보고

가. 개인정보 침해·유출사고가 발생한 것으로 확인된 때에는 개인정보 보호담당자는 지체없이 개인정보 보호책임자에게 침해·유출 사고에 대한 보고

나. 사고 보고는 별지 제3호 서식 '개인정보 침해·유출사고 보고서' 활용

3. 개인정보 침해·유출사고 통지

가. 실제로 침해·유출 사고가 발생한 것으로 확인된 때에는 정당한 사유가 없는 한 5일 이내에 해당 고객에게 아래사항 공지

- 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
- 센터의 대응조치 및 피해구제절차
- 고객에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
- 별표 제1호 '개인정보 침해·유출 통지 절차'
- 별표 제2호 '개인정보 침해·유출 통지문(안)'
- 별표 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 필요

다. 침해·유출 사고의 조치를 취한 이후에는 고객에게 다음 아래의 사실만을 일차적으로 알리고, 추후 확인되는 즉시 알릴 수 있음

- 고객에게 유출이 발생한 사실
- 통지항목 중 확인된 사항

라. 고객에게 통지할 때에는 서면, 전자우편, 팩스, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 5일 이내에 고객에게 알려야 함과 동시에, 홈페이지 등을 통하여 공개 가능

- 별표 제4호 ‘고객의 대응방안 안내(예시)’

4. 개인정보 침해·유출사고 처리 및 종결

가. 센터에서는 개인정보 침해·유출사고 종결처리는 문서로 기록·관리

- 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 통지

- 센터 이사장
- 교육부장관
- 행정자치부장관 또는 한국정보화진흥원 또는 한국인터넷진흥원 중 어느 하나에 통지 (1만명 이상의 고객에 관한 개인정보가 유출된 경우)

제 4 장 문제발생에 따른 3단계 대응절차

1. 심각단계

가. 발생 시나리오

- 센터의 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, 센터 이사장 보고, 유출경로 분석
- 비판여론 수용, 신속한 대 고객 사과조치 및 재발방지 약속, 개선방안 제시

다. 침해·유출사고 대응 업무분장

구 분	업 무 분 장
센터장	· 침해·유출사고수준 발생 시 상황보고 받고 대응책 지시 · 개인정보 보호책임자에게 접수 받은 내용을 검토하고 즉시 보고
개인정보	· 침해·유출사고수준 발생 시 대내외 홍보계획을 추진하고 침해·유

구 분	업 무 분 장
보호책임자	출사고 대응팀 구성 · 침해·유출사고 대응팀 구성여부를 센터 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 센터 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 재활활동	· 침해·유출사고 상황 종료 후 센터 이미지 재활을 위한 PR 활동 전개 · 침해·유출사고 대응 내용을 교재화하여 임직원 침해·유출사고 의식 교육 활용

2. 경계단계

가. 발생시나리오

- 센터의 내부기밀 및 특정 개인정보 언론 노출
  · 전문지·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
센터장	· 침해·유출사고수준 발생 시 개인정보 보호책임자로부터 보고를 받고 필요한 대응책 지시 · 개인정보 보호책임자에게 접수 받은 내용을 검토하고 즉시 보고
개인정보 보호책임자	· 침해·유출사고 유형 및 수준을 판단하고 침해·유출사고수준 발생 시 센터 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 징후 입수 및 정보수집 · 침해·유출사고 진행에 따라 대응절차 준비
정보수집 / 침해·유출사고대응	· 침해·유출사고의 종류 및 정도에 따라 대응방법 선택 · 개별취재 등 언론 대응은 센터 홍보팀으로 이관 · 유출경로 추적 및 로그분석
사후 대응 및 재활활동	· 침해·유출사고 상황 종료 후 센터 이미지 재활을 위한 PR 활동 전개 · 침해·유출사고대응 내용을 교재화하여 임직원 침해·유출사고의식 교육 활용

3. 주의단계

가. 발생 시나리오

- 센터 내부갈등의 외부 노출
- 언론, 유관기관 등을 통해 센터 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
센터장	· 개인정보 보호책임자로부터 보고 받은 내용을 검토하고 필요한 대응책 지시
개인정보 보호책임자	· 침해·유출사고 유형 및 수준을 판단하고 침해·유출사고수준 발생 시 센터장에게 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 징후 입수 및 정보수집 · 침해·유출사고 진행에 따라 대응절차 준비
정보수집 / 침해·유출사고대응	· 침해·유출사고의 종류 및 정도에 따라 대응방법 선택 · 개별취재 등 언론 대응은 센터 홍보팀으로 이관 · 유출경로 추적 및 로그분석
사후 대응 및 재활활동	· 침해·유출사고 상황 종료 후 센터 이미지 재활을 위한 PR 활동 전개 · 침해·유출사고대응 내용을 교재화하여 임직원 침해·유출사고의식 교육 활용

제 5 장 사후 대응 및 모니터링 방안

1. 사후 대응 및 재활활동 방안

가. 비판여론 수용, 신속한 대 고객 사과조치 및 재발방지 약속

- 센터 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 의심스런 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 PDCA(Plan-Do-Check-Act) 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)

[별표 제1호]

개인정보 침해·유출 통지 절차

구분	세 부 내 용	법적근거
침해·유출 통지방법	센터는 개인정보 유출이 발생했을 경우 지체 없이 정보주체에게 개인정보 유출 관련 사항을 통지	법 제34조 시행령 제40조 보호지침 제26조
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 센터의 경우 사업장 등의 보기 쉬운 장소에 통지내용을 게시	시행령 제40조 보호지침 제28조, 제29조
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 센터의 대응조치 및 피해구제절차 ⑤ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처	법 제34조 제1항 보호지침 제27조 제1항
통지시기	5일 이내(유출사고 최초발생 시점과 확인된 시점 사이에 시간적 차이가 있는 경우 이에 대한 과실유무를 입증해야 함)	보호지침 제27조
통지연기	1. 개인정보 유출확산방지를 위해 조치가 필요한 경우 유출통지를 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. 센터는 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 보호지침 제29조
신고기관	http://www.privacy.go.kr	시행령 제39조 제2항 보호지침 제29조
신고시기	5일 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	행정자치부장관 또는 한국정보화진흥원장 또는 한국인터넷진흥원장은 신고접수사실 확인(신고자 전자우편, 팩스)	

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

벌칙		
벌칙조항	개인정보 유출신고(5일이내) 위반시 과태료 3천만원이하	제75조 제2항 제9호

[별표 제2호]

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 안전한 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), 생년월일, 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 안됨
유출 사실을 인지한 후 즉시 해당 IP와 불법접속 경로를 차단하고, 취약점 점검과 보완 조치를 하였습니다. 또한, 유지보수업체 서버에 있던 귀하의 개인정보는 즉시 삭제 조치하였습니다.	<센터의 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 정보주체가 할 수 있는 방

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 안내해 드리고, 신속하게 대응하도록 하겠습니다.	법을 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 해 드리고, 필요한 조사를 거쳐 손실보상이나 손해배상 등의 구제절차를 진행하도록 하겠습니다. 한국인터넷진흥원의 개인정보 분쟁 조정이나 민사 상 손해배상 청구, 감독기관인 행정자치부 개인정보침해신고센터 등을 통해 피해를 구제받고자 하실 경우에도 연락주시면 그 절차를 안내하고 필요한 제반 지원을 아끼지 않도록 하겠습니다.	<센터의 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.	(센터의 향후 대응계획) - 추가적인 향후 대응계획을 포함
항상 믿고 사랑해 주시는 귀하께 심려를 끼쳐 드리게 되어 거듭 진심으로 사과드립니다.	(사과문)
▸ 피해 등 접수 담당부서 : OOO팀 ▸ 피해 등 접수 전화번호 : 063-905-OOOO ▸ 피해 등 접수 e-메일주소 : privacyOO@jeonjuscc.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
<기관명> 직원 일동	(발신명의)

[별표 제3호]

개인정보 침해·유출 통지내용(예시)

고객 여러분의 개인정보가 유출되어
심려를 끼치게 된 점 진심으로 사과드립니다.

고객 여러분께 알려드립니다.
당 센터에서는 내부 모니터링을 통해 **고객의 일부 정보가 00월 00일 해킹에 의해 유출된 사실을 11월 11일 확인**하였으며 고객 여러분의 피해예방 및 조속한 범인검거를 위하여 **수사기관 및 관계기관에 즉시 조사를 의뢰**하였음을 알려드립니다.

현재까지 파악된 바는 유출된 개인정보는 **암호화된 비밀번호, 암호화된 주민등록번호** 등이며, **비밀번호, 주민등록번호는 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 센터의 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 센터에서는 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 센터에서는 비밀번호 변경 캠페인을 정기적으로 진행하고 있으며 무작위 조합을 통한 비정상 로그인 시도를 차단하기 위하여 틀린 비밀번호 입력 시 인증을 강화하였습니다.

당 센터는 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 피해 예방을 위하여 최선의 노력을 다할 것입니다. 관련하여 궁금한 점이 있으시면 아래 핫라인으로 연락주시기 바랍니다.
핫라인: 063-905-OOOO 메일주소: privacyOO@jeonjuscc.or.kr

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

개인정보 유출여부 확인을 위한 기능은 빠른 시간 내에 제공하겠습니다.

[별표 제4호]

고객의 대응방안 안내(예시)