6. 개인정보 침해사고 대응방안

‘개인정보 침해사고 대응방안’ 은 개인정보의 처리 · 운용 과정에서 내부의 과실 및 오 · 남용 또는 외부 해킹 등으로 침해 · 유출 사고가 발생할 경우, 체계적이고 신속한 대응으로 피해를 최소화하려는데 목적이 있다.

6.1 침해사고 정의

개인정보 침해사고란 법규를 위반하여 개인정보를 외부의 제3자에게 노출 · 제공하는 것과 해킹에 의한 유출 · 업무무비 등의 제반적 사고를 총칭한다.

6.2 침해사고 대상

가. 개인정보를 수집, 처리 시 개인정보에 관한 권리 또는 이익의 침해를 받은 자

나. 개인정보파일을 보유함에 있어 개인정보에 관한 권리 또는 이익의 침해를 받은 자

6.3 침해사고 유형

사고유형	내용	인지경로
과실로 인한 개인정보 침해	- 정보주체의 동의 또는 법적근거 없이 개인정보를 제3자에게 제공하는 등 개인정보의 관리(수집 · 저장 · 이용 · 파기)가 미흡하여 정보주체에게 침해를 주는 경우	① 상시모니터링 ② 교육사이버안전센터(한국교육학술정보원) ③ 침해신고
과실로 인한 개인정보 유·노출	- 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터를 분실 또는 도난 당한 경우 - 권한이 없는 자에게 개인정보를 잘못 전달한 경우	
오·남용으로 인한 개인정보 유출	- 개인정보 부당이용 또는 사적유용을 목적으로 유출하는 경우	
외부 침투에 의한 개인정보 유출	- 홈페이지 해킹 등 외부 침투에 의해 정보주체의 개인정보가 유출되는 경우	

6.4 침해사고 발생 시 조치방법

단계	조치방법	세부 조치 사항
확인 단계	① 사고 인지 · 접수	- 침해 · 유출 사고 상황 파악 - 개인정보보호 책임자에게 보고 - 침해 · 유출 사고대응반 설치 - 개인정보보호 손해배상 책임보험사에 신속히 연락
	② 확인조사 실시	- 침해 · 유출 사고 내용(원인, 규모 등) 세부조사 ※ 법령 위반사실 증빙자료 취합
	③ 피해확산 여부 확인	- 확인조사 결과에 따른 분석을 통해 추가 유출가능성 및 피해 확산 여부 확인 - 해명 보도 자료 등 배포
조치 단계	④ 유출통지	- 정보주체에게 5일 이내 통지
	⑤ 유출통지 신고	- 행정안전부 또는 지정기관에 5일 이내 신고
	⑥ 사례전파 및 시스템 보완	- 기술적, 관리적 보완조치

가. 개인정보취급자는 개인정보 침해가 발생한 것을 인지하거나 의심되는 경우 지체 없이 **개인정보 침해사실 신고서[붙임 10]**를 작성하여 개인정보보호 담당자에게 신고하여야 한다.

나. 개인정보보호 담당자는 사고 접수 내역을 **개인정보 침해사고 관리대장[붙임 11]**에 기록하고 개인정보보호 책임자에게 즉시 보고한다.

6.5 침해사고 유출통지

가. 과실로 인한 개인정보 침해 사고

- 정보주체의 동의 또는 법적근거 없이 개인정보를 제3자에게 제공하는 등 개인정보의 관리가 미흡하여 정보주체에게 침해를 주는 경우

1) 침해사고 인지 및 접수
- 개인정보보호 담당자는 정기 실태점검 또는 침해신고(접수)를 통해 개인정보관리 침해사실 인지 및 접수
- 개인정보보호 담당자는 위반사항이 중대한 경우 개인정보 보호 책임자에게 보고
- 개인정보보호 책임자는 침해사고대응반 설치

2) 확인조사 실시
- 침해사고대응반에서는 개인정보 침해사고가 인지 또는 접수되어 침해사고 발생이 우려되는 부서에 대하여 확인조사 및 위험사실 확인
  ※ 필요 시 외부 전문가 협조 요청
- 사고발생 부서는 침해사고대응반의 현장 확인조사 시 적극 협조

3) 개선조치 및 사례전파
- 침해사고대응반은 확인조사 결과를 분석하여 개인정보보호 책임자에게 보고
- 침해사고대응반은 개인정보 침해사고 발생을 방지하기 위한 대책을 부서에 제시하고 필요한 경우 개선권고 요청
- 침해사고대응반은 관리미흡에 의한 사고사례를 내부에 전파하고, 유사한 사례가 발생하지 않도록 조치
- 실태점검 항목 강화 등 개인정보관리 철저를 위한 대책 강구

나. 과실로 인한 개인정보 유·노출 사고

- 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터를 분실 또는 도난당한 경우 - 권한이 없는 자에게 개인정보를 잘못 전달한 경우

1) 유·노출 사고 인지 및 접수
- 개인정보보호 담당자는 상시 모니터링, 실태점검을 통한 부주의 등 과실로 인한 개인정보 유·노출 사실 확인 또는 내·외부 침해신고 접수를 통해 유·노출 사고 인지

- 개인정보보호 담당자는 위반사항이 중대한 경우 개인정보보호 책임자에게 보고
- 개인정보보호 책임자는 침해사고대응반 설치

2) 확인조사 실시
- 침해사고대응반은 자체점검을 위한 자료(서비스 종류 및 로그값)를 확보하고, 현장 확인조사를 통해 과실여부, 침해규모, 경위, 방법 등을 조사
  ※ 필요 시 외부 전문가 협조 요청
- 사고발생 부서는 침해사고대응반의 현장 확인조사 시 적극 협조

3) 피해 확산 여부 확인
- 침해사고대응반은 확인조사 결과에 따른 분석을 통해 추가 유·노출 가능성 및 피해 확산 여부 확인
- 인터넷 등 언론동향 대응을 위한 보도자료 등 배포

4) 유출통지
- 침해사고대응반은 개인정보가 유출되었을 경우, 유출 사실을 지체 없이(5일 이내) 정보주체에게 통지
- 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없이 정보주체에게 통지
- 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 7일 이상 게재

5) 유출통지 신고
- 1천명 이상 유출된 경우에는 정보주체에게 유출 사실을 통지한 사항 및 피해를 최소화하기 위한 대책과 필요한 조치 결과를 행정안전부 또는 전문기관에 신고

6) 사례전파로 동일사례 발생 방지
- 부주의 등 과실로 인한 개인정보 유·노출 사고사례를 내부에 전파하고, 유사한 사례가 발생하지 않도록 조치
- 재발 방지를 위한 기술적 조치와 개인정보보호 교육 및 실태점검 강화

7) 사고내용 세부조사
- 침해사고대응반은 확인조사 결과 세부조사가 필요하다고 판단되는 경우, 개인정보보호 책임자에게 필요성 보고

8) 해당자 처분 및 조치
- 개인정보보호 책임자에게 세부조사 결과 보고
- 위반사항의 중요도에 따라 처분 및 조치 요청

다. 오·남용으로 인한 개인정보 유출 사고

1) 유출 사고 인지 및 접수
- 개인정보보호 담당자는 상시 모니터링, 실태점검 등을 통한 고의적 유출

사실 확인 또는 내·외부 침해신고 접수를 통해 사고 인지

- 개인정보보호 담당자는 위반사항이 중대한 경우 개인정보보호 책임자에게 보고
- 개인정보보호 책임자는 침해사고대응반 설치

2) 확인조사 실시

- 침해사고대응반은 자체점검을 위한 자료(서비스 종류 및 로그값)를 확보하고, 현장 확인조사를 통해 과실 여부, 침해규모, 경위, 방법 등을 조사
  ※ 필요 시 외부 전문가 협조 요청
- 사고발생 부서는 침해사고대응반의 현장 확인조사 시 적극 협조

3) 피해 확산 여부 확인

- 침해사고대응반은 확인조사 결과에 따른 분석을 통해 추가 유·노출 가능성 및 피해 확산 여부 확인
- 인터넷 등 언론동향 대응을 위한 보도자료 등 배포

4) 유출통지

- 침해사고대응반은 개인정보가 유출되었을 경우, 유출 사실을 지체 없이(5일 이내) 정보주체에게 통지
- 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없이 정보주체에게 통지
- 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 7일 이상 게재

5) 유출통지 신고

- 1천명 이상 유출된 경우에는 정보주체에게 유출 사실을 통지한 사항 및 피해를 최소화하기 위한 대책과 필요한 조치 결과를 행정안전부 또는 전문기관에 신고

6) 사례전파로 동일사례 발생 방지

- 부주의 등 과실로 인한 개인정보 유·노출 사고사례를 내부에 전파하고, 유사한 사례가 발생하지 않도록 조치
- 재발 방지를 위한 기술적 조치와 개인정보보호 교육 및 실태점검 강화

7) 사고내용 세부조사

- 침해사고대응반은 확인조사 결과 세부조사가 필요하다고 판단되는 경우, 개인정보보호 책임자에게 필요성 보고

8) 해당자 처분 및 조치

- 개인정보보호 책임자에게 세부 조사결과 보고
- 위반사항의 중요도에 따라 처분 및 조치 요청
  ※ 세부조사 결과 개인정보 부당이용 또는 사적유용을 목적으로 유출된 경우 고발 조치

라. 외부 침투에 의한 개인정보 유출 사고

1) 외부 침투에 의한 유출 사고 확인

- 개인정보보호 담당자는 외부침투(해킹 등)에 의한 개인정보 유출사실 확인
- 사이버공격 대응절차에 따른 경계단계별 대응반 가동 상태 확인
- 개인정보보호 담당자는 확인한 침해사실에 대해 개인정보보호 책임자에게 보고
- 개인정보보호 책임자는 침해사고대응반 설치

2) 피해 확산 여부 확인

- 침해사고대응반은 확인조사 결과에 따른 분석을 통해 추가 유·노출 가능성 및 피해 확산 여부 확인
- 인터넷 등 언론동향 대응을 위한 보도자료 등 배포

3) 유출통지

- 침해사고대응반은 개인정보가 유출되었을 경우, 유출 사실을 지체 없이(5일 이내) 정보주체에게 통지
- 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없이 정보주체에게 통지
- 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 7일 이상 게재

4) 유출통지 신고

- 1천명 이상 유출된 경우에는 정보주체에게 유출 사실을 통지한 사항 및 피해를 최소화하기 위한 대책과 필요한 조치 결과를 행정안전부 또는 전문기관에 신고

5) 사고 사례전파 및 시스템보완

- 침해사고대응반은 개인정보 유출 및 침해에 관한 사고사례를 전파하고 유사사례가 발생하지 않도록 조치
- 정보보안 담당자는 보안시스템 점검 강화 등의 기술적인 보안 조치

6) 해킹사고 세부조사 및 조치

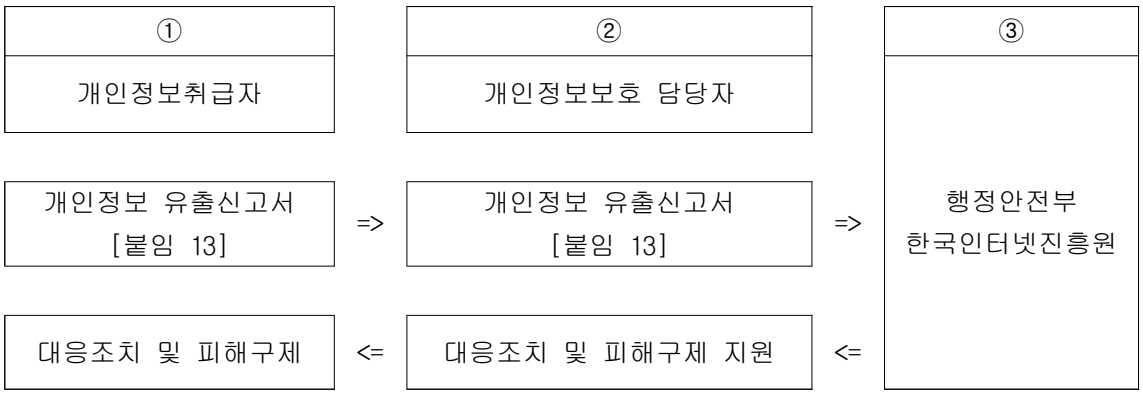
- 침해사고대응반은 국가정보원, 한국교육학술정보원 등에 세부조사 의뢰
- 세부조사 결과, 해킹사고의 업무상 과실 등 책임이 있는 담당자를 확인하여 고발 조치

6.6 침해사고 대응반 조직(연락) 및 역할

6.7 침해사고 발생 시 업무분장

조직별	담당자	담당 업무
개인정보보호 책임자	기획정보처장	- 개인정보 침해사고 대응 총괄 지휘
개인정보 침해사고 대응반	개인정보보호 담당자 개인정보보호 분야별 책임자, 정보보안 담당자, 전산담당자, 기타 협조부서	- 개인정보 침해사고 인지 · 접수 - 개인정보 침해사고 대응 절차 수립 - 개인정보 침해사고 사실 확인조사 실시 - 정보주체에게 유출사실 통지 - 행정안전부 또는 전문기관에 유출통지 신고 - 외부요인에 의한 유출의 경우, 국가정보원, 한국교육학술정보원(KERIS), 행정안전부 등과 협조하여 사고 해결 - 사고내용 세부조사 및 사후 인사조치가 필요한 경우 유관부서와 협조
사고발생부서	개인정보취급자	- 내부요인에 의한 침해 · 유출의 경우, 사고대응반에 사고내용 신고 - 침해사고대응반과 협력하여 사고처리 적극 지원
사고신고자	정보주체	- 개인정보를 침해 받은 피해자

6.8 침해사고 신고방법



가. 신고방법은 이메일, 팩스 또는 개인정보보호종합지원포털(www.privacy.go.kr) 로 신고

- 시간적 여유가 없거나 그밖에 특별한 사정이 있는 때에는 먼저 전화로 신고한 후, 나중에 **개인정보 유출신고서[붙임 13]** 제출

나. 1천명 이상의 개인정보가 유출된 경우에는 5일 이내에 행정안전부 또는 한국인터넷진흥원 중 한 곳에 신고

- 또한 홈페이지에 정보주체가 알아보기 쉽도록 해당 사항을 7일 이상 게제

6.9 침해사고 구제방법

가. 정보주체는「개인정보 보호법」제39조에 따라 개인정보취급자가 법을 위반한 행위로 손해를 입은 경우 개인정보취급자에게 손해배상을 청구할 수 있으며 이 경우 개인정보취급자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

나. 개인정보취급자는 개인정보가 유출되었음을 알게 되었을 때에는 지체없이 개인정보보호 담당자에게 신고하여야 하며, 개인정보보호 책임자는 **개인정보 유출 신고서[붙임 13]**를 작성 후 개인정보보호 책임자에게 보고한다. 해당 정보주체에게는 다음 각 호의 사실을 통지한다.

1) 유출된 개인정보의 항목
2) 유출된 시점과 경위
3) 유출에 의한 피해를 최소화하기 위해 정보주체가 할 수 있는 방법 등
4) 개인정보처리자의 대응조치 및 피해 구제절차
5) 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

다. 개인정보주체는 개인정보침해로 인한 피해를 구제 받기 위하여 개인정보 분쟁조정위원회, 한국인터넷진흥원 개인정보 침해-신고센터 등에 분쟁해결이나 상담 등을 신청할 수 있다.

1) 개인정보 분쟁조정위원회: 1833-6972 (www.kopico.or.kr)
2) 개인정보 침해신고센터: (국번없이) 118, (privacy.kisa.or.kr)
3) 대검찰청 사이버수사과: (국번없이) 1301, (www.spo.go.kr)
4) 경찰청 사이버안전국: (국번없이) 182, (cyberbureau.police.go.kr)

라. 개인정보의 열람, 정정·삭제, 처리정지 등에 대한 정보주체자의 요구에 대하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익을 침해 받은 자는 행정심판법이 정하는 바에 따라 행정심판을 청구할 수 있다.

※ 중앙행정심판위원회(www.simpan.go.kr)의 전화번호 안내 참조

6.10 침해사고 처리보고

가. 개인정보보호 담당자는 **개인정보 침해사고 처리보고서[붙임 12]**를 작성하여 개인정보보호 책임자에게 보고한다.

나. 처리보고서 제출 후 30일 이내에 근본원인 분석 및 예방을 위한 개선 대책을 마련하고, 전 직원을 대상으로 사고 처리 경과 및 예방을 위한 교육을 실시하여 사고의 재발을 방지한다.

다. 개인정보취급자는 동일 혹은 유사 사고가 발생하지 않도록 개인정보 관리에 철저를 가하여야 하며, 개인정보보호 책임자는 이를 위한 직원에 대하여 불이익 조치를 명할 수 있다.

6.11 사고예방

가. 사고예방 활동

1) 개인정보 침해·유출 사고를 대비하여 사전 사고예방 활동 실시
2) 개인정보보호 관리수준 현장조사
3) 개인정보 통합관제 실시
4) 웹사이트 개인정보 노출점검 실시

나. 사고요인 점검

1) 수집단계에서의 침해·유출 사고요인 검검
2) 불필요한 개인정보 수집 여부 점검
3) 수집된 개인정보의 개인정보보호 처리방침 게재 여부 점검
4) 개인정보 수집 시 정보주체 동의 여부 점검

다. 저장 및 관리단계에서의 침해·유출 사고요인 검검

1) 수집된 개인정보 불법적인 유출 위협 상태 점검
2) 수집 목적 달성 또는 보유기간 초과 여부 점검
3) 관리자 또는 이용자의 실수로 인한 개인정보 노출 여부 점검
4) 권한관리 등 시스템 오류로 인한 개인정보 노출 여부 점검

라. 이용 및 제공단계에서의 침해·유출 사고요인 검검

1) 개인정보보호 처리방침에 명시되지 않은 위탁사업자나 제3의 서비스 제공자에게 개인정보 제공 여부 점검
2) 개인정보를 제3자에게 양도하는 등 불법적 거래 여부 점검

마. 파기단계에서의 침해·유출 사고요인 검검

1) 수집 목적 달성 또는 보유기간 초과한 개인정보 파기 여부 점검
2) 권한이 없는 이용자의 개인정보 파기 여부 점검

바. 개인정보 특별점검 실시

1) 개인정보의 관리 미흡으로 개인정보 유출사고 발생 가능성이 우려되는 경우, 개인정보 특별점검 실시

2) 대상: 개인정보취급자 및 일반직원

[붙임 10]

개인정보 침해사실 신고서

신고인	성명		
	생년월일		
	연락처	전화번호(핸드폰)	
		전자우편	
		주소	
접수부서	부서명		
	연락처	전화번호	
		주소	
신고내용			

위와 같이 개인정보침해사실을 신고합니다.

붙임 :

년 월 일

신고인 : (서명 또는 인)

[붙임 11]

개인정보 침해사고 관리대장

접수		신고개요	침해사고 등급	처리 유형	종결 일자	처리내용	비고
일시	신고자 유형						

* 신고자 유형은 직원/고객으로 구분
* 신고 개요는 신고 내용을 기록
* 침해사고 등급은 1-8등급으로 구분
* 처리유형은 사실 확인 중/ 상담 및 자료 제공/ 타 기관 이송/ 위법성 통보/ 수사 의뢰/법 위반 확인 불가/ 기타(징계위원회 회부)로 구분
* 종결일자는 개인정보 침해사고 처리보고서 접수일을 기준으로 기록
* 처리내용은 처분 유형을 사법처리(징역, 벌금, 추징, 재판계류 중, 수사 중) 징계 처분(파면, 해임, 정직, 감봉, 견책, 기타)로 구분
* 비고란에는 처리보고서 문서번호를 기록

[붙임 12]

개인정보 침해사고 처리보고서

<table>
<tr><td>보고일자</td><td colspan="2"></td><td>문서번호</td><td></td></tr>
<tr><td>침해신고 접수정보</td><td colspan="4"></td></tr>
<tr><td>침해사고 등급</td><td colspan="2">(　　) 등급</td><td>침해대상정보</td><td></td></tr>
<tr><td>접수일시</td><td colspan="2"></td><td>신고일자</td><td></td></tr>
<tr><td>침해사고 처리책임자</td><td colspan="2"></td><td>신고자 연락처</td><td></td></tr>
<tr><td>신고 내용</td><td colspan="4"></td></tr>
<tr><td rowspan="2">대응 과정</td><td>일시</td><td colspan="3">대응활동</td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td>침해 내용</td><td colspan="4"></td></tr>
<tr><td>침해 발생 경위</td><td colspan="4"></td></tr>
<tr><td>관련자</td><td colspan="4"></td></tr>
<tr><td>침해 발생 원인</td><td colspan="4"></td></tr>
<tr><td>증거자료</td><td colspan="4"></td></tr>
<tr><td>복구 및 재발방지 조치</td><td colspan="4"></td></tr>
<tr><td>처분</td><td colspan="4"></td></tr>
</table>

* 침해 내용 : 확인된 침해 정보의 세부사항, 규모 및 침해 방법(노출, 외부자 제공, 수집, 접근, 분석, 이용, 내부자 제공, 불법 저장, 불안전한 저장, 파기, 비파기 등 세부사항) 기재

[붙임 13]

개인정보 유출신고(보고)서

기관명					
정보주체에의 통지 여부					
유출된 개인정보의 항목 및 규모					
유출된 시점과 그 경위					
유출피해 최소화 대책·조치 및 결과					
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차					
담당부서·담당자 및 연락처		성명	부서	직위	연락처
	개인정보 보호책임자				
	개인정보 취급자				

유출신고(보고) 접수기관	기관명	담당자명	연락처