
개인정보 내부관리계획

2017. 11.



수도권대기환경청

목 차

I. 총 칙	1
1. 목 적	1
2. 적용범위	1
3. 용어정의	1
4. 개인정보보호 원칙	3
II. 내부관리계획의 수립 및 시행	5
1. 내부관리계획 수립 및 승인	5
2. 내부관리계획의 공표	5
III. 개인정보 보호책임자 등 지정	6
1. 개인정보 보호책임자 지정	6
2. 개인정보 분야별 책임자 지정	6
3. 개인정보 보호담당자 지정	7
4. 개인정보취급자 지정	7
IV. 개인정보 처리 및 관리방법	9
1. 개인정보 수집제한	9
2. 개인정보의 수집	9
3. 개인정보의 이용 및 제공의 제한	10
4. 제3자에게 개인정보의 처리업무 위탁	11
5. 개인정보파일 등록	12
6. 개인정보 영향평가	12
7. 개인정보 열람·정정·처리 정지 요구에 대한 조치	13
8. 개인정보의 파기	14
9. 개인정보 유출 통지	15

목 차

V. 개인정보보호의 처리단계별

기술적·관리적 안전조치

16

1. 개인정보취급자 접근 권한 관리	16
2. 접근통제	16
3. 개인정보의 암호화	17
4. 접근기록의 보관 및 점검	19
5. 보안프로그램의 설치 및 운영	19
6. 물리적 접근제한	20
7. 안전성 확보조치 계획	20
8. 재해 및 재난 대비 안전조치	20

VI. 개인정보보호 교육 및 홍보

21

1. 개인정보보호 인력에 대한 교육	21
2. 개인정보보호 홍보 및 지도점검	21

VII. 개인정보 침해대응 및 피해구제

22

1. 개인정보 침해 신고	22
2. 권익침해 구제방법	22
3. 행정심판 청구절차	23

붙임 1. 개인정보 처리단계별 준수사항 및 위반시 벌칙사항

2. 개인정보처리자 개인정보보호 자가진단표
3. 개인정보파일 목록
4. 위탁업체 개인정보보호 관리실태 점검표
5. 접근권한 검토보고서
6. 접속기록 검토보고서
7. 개인정보 처리방침
8. 영상정보처리기기 운영·관리방침
9. 재해·재난 대비개인정보처리시스템 위기대응 매뉴얼

1. 목적

- 개인정보를 처리하는 직원이 개인정보의 안전성 확보를 위하여 이행해야 할 일반적 관리사항과 기술적·관리적 보호조치 등 세부기준을 제시하는 것을 목적으로 한다.

※ 개인정보 보호법 제29조(안전조치의무) 및 같은 법 시행령 제30조(개인정보의 안전성 확보조치)

2. 적용 범위

- 개인정보 내부 관리계획(이하 “내부 관리계획”이라 한다)은 정보통신망을 통하여 수집·이용·제공 또는 관리되는 개인정보뿐만 아니라, 서면 등 정보통신망 이외의 수단을 통하여 수집·이용·제공 또는 관리되는 개인정보에 대하여서도 적용하며 그 적용대상은 다음과 같다.
 - 수도권 대기환경청 전체 직원 및 외부업체 직원
 - 수도권 대기환경청에서 관리중인 개인정보 처리시스템 및 영상정보처리기기

3. 용어 정의

- “개인정보”란 살아 있는 개인에 관한 정보로서 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 것을 포함한다)를 말한다.
- “개인정보 처리”란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
- “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
- “개인정보 보호책임자”란 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자를 말한다.
- “개인정보 보호담당자”란 개인정보 보호책임자를 보좌하여 개인정보보호 업무에 대한 실무를 총괄하고 관리하는 자를 말한다.

- “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
- “개인정보 취급자”란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다.
- “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
- “정보통신망”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
- “개인정보처리시스템”이란 개인정보를 처리할 수 있도록 체계적으로 구성된 데이터베이스시스템을 말한다.
 - 개인정보처리시스템에 was 등 어플리케이션 포함 보호조치 필요
- “영상정보처리기기”란 일정한 공간에 지속적으로 설치되어 사람 또는 사물 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 폐쇄회로 텔레비전(CCTV) 및 네트워크카메라 등 일체의 장치를 말한다.
- “개인영상정보”란 영상정보처리기기에 의하여 촬영·처리되는 영상정보 중 개인의 초상, 행동 등 사생활과 관련된 영상으로서 해당 개인의 동일성 여부를 식별할 수 있는 정보를 말한다.
- “비밀번호”란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
- “접속기록”이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
- “민감정보”란 사상·신념, 노동조합·정당 등의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할

우려가 있는 개인정보로 유전자검사 등의 결과로 얻어진 유전정보, 범죄경력 자료에 해당하는 정보를 말한다.

- “고유식별정보”란 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 주민등록번호, 여권번호, 운전면허의 면허번호, 외국인등록번호를 말한다.
- “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
- “P2P(Peer to Peer)”란 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.
- “공유설정”이란 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것을 말한다.
- “보조저장매체”란 이동형 하드디스크(HDD), USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스크 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 분리할 수 있는 저장매체를 말한다.
- “위험도 분석”이란 개인정보처리시스템에 적용되고 있는 개인정보보호를 위한 수단과 유출시 정보주체의 권리를 해할 가능성과 그 위험의 정도를 분석하는 행위를 말한다.
- “모바일 기기”란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인 정보 처리에 이용되는 휴대용 기기를 말한다.
- “공개된 무선망”이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

4. 개인정보보호 원칙

- ① 개인정보의 처리 목적을 명확히 하고, 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

- ② 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 목적 외의 용도로 활용되어서는 아니 된다.
- ③ 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
- ④ 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험정도를 고려하여 개인정보를 안전하게 관리하여야 한다.
- ⑤ 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
- ⑥ 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
- ⑦ 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.
- ⑧ 법에 규정한 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

II 내부관리계획의 수립 및 시행

1. 내부관리계획의 수립 및 승인

- 개인정보 보호담당자는 개인정보의 안전한 처리를 위하여 개인정보를 관련한 법령 및 관련 규정을 준수하도록 다음 사항을 포함하여 내부 관리계획을 수립하여야 한다.
 - 개인정보 보호책임자의 지정에 관한 사항
 - 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
 - 개인정보의 안전성 확보에 필요한 조치에 관한 사항
 - 개인정보취급자에 대한 교육에 관한 사항
 - 그 밖에 개인정보 보호를 위하여 필요한 사항
- 개인정보 보호담당자는 매년 1회 이상 내부 관리계획의 타당성과 개정 필요성을 검토하고 개정이 필요하다고 판단되는 경우 내부 관리계획 개정안을 작성하여 개인정보 보호책임자에게 보고하고 승인을 받아야 한다. 타당성 검토에 고려되어야 하는 사항은 아래와 같다.
 - 「개인정보 보호법」 개정 등 대내외적 환경변화
 - 적용기술의 변화
 - 내/외부 이행점검 결과 등

<수립근거>

- 개인정보 보호법 제29조(안전조치의무)
- 같은 법 시행령 제30조(개인정보의 안전성 확보 조치)

2. 내부관리계획의 공표

- 개인정보 보호책임자는 개인정보 내부 관리계획을 수립하거나 개정안을 승인한 후 전 직원에게 공표하여야 한다.
- 내부 관리계획은 내부직원(비정규직 포함), 외부직원이 언제든지 열람할 수 있는 방법으로 비치하여야 하며, 변경사항이 있을 경우 이를 공지하여야 한다.
 - 비치장소 : 기획과
 - 공지방법 : (내부) 전체공지, (외부) 홈페이지

III 개인정보 보호책임자 등 지정

1. 개인정보 보호책임자 지정

- 개인정보 보호책임자 : 기획과장
 - 이메일 : ansh@korea.kr
 - 전화번호 : 031-481-1305, Fax : 031-486-7921
 - 주소 : 경기 안산시 단원구 원고잔로 34 수도권대기환경청
- 개인정보 보호책임자의 임무
 - 개인정보보호 계획의 수립 및 시행
 - 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
 - 부서별 정기점검 결과 및 관련 통계 관리·감독
 - 개인정보 수집에서 파기 등 전 단계에 대한 실태조사 실시
 - 개인정보 처리와 관련한 불만의 처리 및 피해 구제
 - 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
 - 개인정보보호 교육계획의 수립 및 시행
 - 개인정보파일의 보호 및 관리·감독

2. 개인정보 분야별 책임자 지정

- 개인정보 분야별 책임자 지정
 - 개인정보 보유 부서장을 분야별책임자로 지정하여 개인정보보호 책임자에게 통보
- 개인정보 분야별 책임자의 임무
 - 개인정보에 대한 안전성을 확보하고, 취급자에 대한 교육과 관리 감독 책임
 - 기관 자체 '개인정보 보호지침'을 준수
 - 개인정보취급자의 의무 등을 준수토록 교육 등 조치
 - 처리정보의 취급내역에 대한 로그(Log)기록 의무화
 - 개인정보에 대한 입력·수정·삭제·열람 사항 및 내역자 인적사항 기록을 의무화하여 정보유출 차단 및 책임 소재 명확화

- 개인정보보호 업무 관련 사항을 개인정보보호책임자에게 수시 보고
 - 개인정보 침해사례 및 개인정보취급 관련자들의 위법사항 등
 - 개인정보 이용·제공, 열람·정정·삭제 현황 등의 통계
- 개인정보 위탁업체에 대한 관리·감독 수행

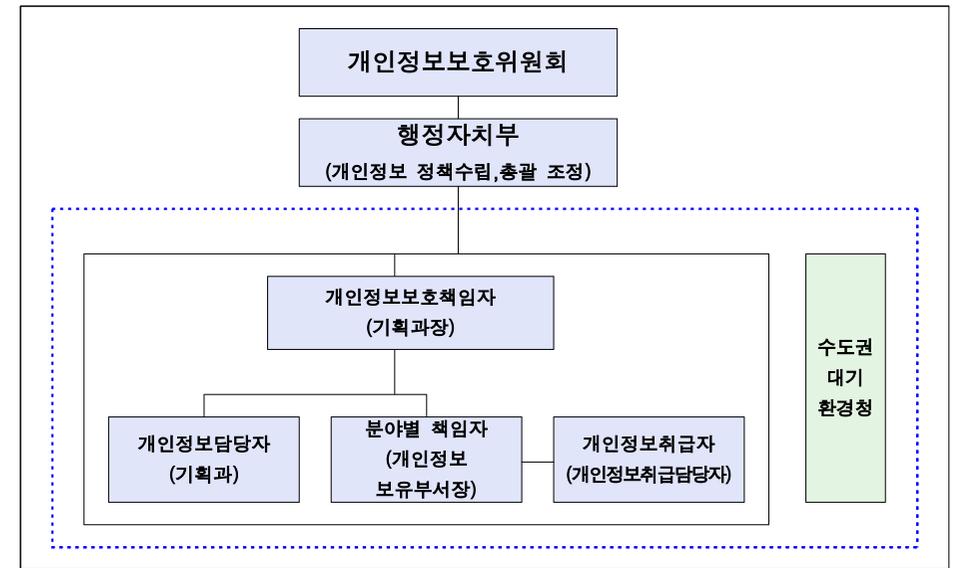
3. 개인정보 보호담당자 지정

- 기관의 행정정보 및 정보통신보안 업무를 수행하는 개인정보 총괄부서의 업무담당자를 지정
 - 개인정보 보호담당자
 - 이메일 : jisun7@korea.kr
 - 전화번호 : 031-481-1313, Fax : 031-486-7921
 - 주소 : 경기 안산시 단원구 원고잔로 34 수도권대기환경청
- 개인정보 보호담당자의 임무
 - 개인정보 보호계획 및 방침운영
 - 개인정보 침해대응
 - 개인정보 처리실태 관리 및 각종 자료 취합
 - 개인정보 보호법 관련 업무전반
 - 개인정보 보호책임자가 위임한 개인정보보호와 관련된 업무
 - 개인정보처리시스템과 관련 시스템간 연계 등과 관련된 업무

4. 개인정보취급자 지정

- 행정서비스의 업무를 수행함에 있어 개인정보를 취급하는 담당자
- 개인정보취급자의 임무
 - 업무를 수행함에 있어 처리되는 개인정보에 대한 보호관리(개인정보의 수집·보유·이용 및 제공·파기단계에서의 관리)
 - 내부관리계획의 준수 및 이행
 - 개인정보의 기술적·관리적 보호조치 기준 이행
 - 소속 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검 등

<참고 : 구성도>



IV 개인정보 처리 및 관리방법

1. 개인정보의 수집 제한

- 개인정보처리자는 다음 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.
 - 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
 - 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
 - 위 항에 준하여 주민등록번호 처리가 불가피한 경우로서 행정자치부령으로 정하는 경우
- 기본적인 인권에 관한 민감한 개인정보 및 고유 식별정보(운전면허번호, 외국인등록번호, 여권번호)를 수집하는 것을 금지한다. 다만, 정보주체에게 별도의 동의를 득하거나 수집대상 개인정보가 명시된 법률에 근거한 경우에는 수집을 허용한다.
- 개인정보처리자는 정보주체의 개인정보를 수집하는 경우, 적법하고 공정한 수단에 의하여 서비스 제공에 직접적으로 관련되어 필요한 성명, 연락처, 주소 등 최소한의 정보를 수집하여야 한다.

2. 개인정보의 수집

- 개인정보 수집에 따른 관리방안은 아래의 각 시기마다 검토되어야 한다.
 - 개인정보처리시스템 신규 구축 및 고도화
 - 오프라인 수집문서의 신규 및 변경
 - 법률 등에 의해 수집하는 개인정보 항목의 변경
 - 그 외 자체감사 등 개인정보보호 강화를 위한 활동 수행 시
- 개인정보처리자는 개인정보를 수집(온라인, 오프라인)하는 경우 정보주체의 동의를 받아야 한다. 기본 동의 외 별도로 동의를 받아야 하는 사항은 다음과 같다.
 - 민감정보 수집

- 고유식별정보(운전면허번호, 외국인등록번호, 여권번호) 수집
- 목적 외 이용 및 제3자 제공과 관련된 사항

- 개인정보처리자는 정보주체로부터 개인정보 보호법 제15조제1항의 규정에 의한 동의를 받고자 하는 경우에는 미리 다음 각호의 사항을 서면 또는 인터넷 홈페이지 등을 통하여 정보주체가 알기 쉽도록 알려야 하며, 다음 각 호의 어느 하나의 사항이라도 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

- 개인정보보호책임자의 성명·소속부서·지위·전화번호·전자우편주소, 기타 연락처
- 개인정보의 구체적인 수집 및 이용목적
- 동의 철회, 열람 또는 정정 요구 등 정보주체 및 법정대리인의 권리와 그 행사방법
- 개인정보처리자가 수집하고자 하는 개인정보 항목
- 수집하는 개인정보의 보유·이용기간 및 법적 근거 등 보유근거
- 기타 개인정보에 대한 가공 또는 관리방식
- 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익 내용

- 개인정보처리자는 만 14세 미만의 아동을 대상으로 개인정보를 수집하고자 할 경우에는 법정대리인의 동의를 받아야하며, 이 경우 법정대리인의 동의를 받기 위한 최소한의 정보는 해당아동으로부터 수집할 수 있다.
 - 홈페이지를 통해 수집할 경우에는 공공 I-PIN을 통하거나, 홈페이지에 별도의 가입화면을 제공하여야 함.

3. 개인정보의 이용 및 제공의 제한

- 수집한 개인정보는 수집 목적의 범위에서만 이용할 수 있으나, 수집 목적 외로 이용하여야 하거나 제3자에게 제공하여야 할 경우에는 다음 사항을 정보주체에게 알리고 동의를 받아야 한다.
 - 개인정보를 제공 받는 자, 개인정보를 제공 받는 자의 이용 목적, 제공하는 개인정보의 항목
 - 개인정보를 제공받은 자의 개인정보 보유 및 이용기간
 - 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익 내용
- 환경부 개인정보 보호지침 별지서식 제1호 서식에 따른 “개인정보의 목적 외 이용 및 제3자 제공대장” 기록하고 관리하여야 한다.

- 다음의 경우에는 개인정보를 제3자에게 제공할 수 있다.
 - 정보주체의 동의를 받은 경우, 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
 - 공공기관이 법령 등에서 정하는 소관 업무를 수행하기 위하여 불가피한 경우
 - 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태이거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
 - 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정개인을 알아볼 수 없는 형태로 제공하는 경우
 - 범죄수사, 재판업무를 위해 필요한 경우

4. 제3자에게 개인정보의 처리업무 위탁

- 개인정보처리자가 제3자에게 개인정보의 처리업무를 위탁하는 경우에는 환경부 개인정보 보호지침 별지서식 제2호에 따른 개인정보 처리 위탁 계약서에 의하여야 한다.
 - 수탁자는 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공 금지
- 정보 주체에게 위탁 사항 공개

<정보주체자에게 알려야 할 내용>
 - 위탁하는 업무의 내용, 개인정보 처리업무를 위탁받은 처리자

- 관보 또는 인터넷 홈페이지에 지속적으로 게재, 홈페이지에 게시할 수 없는 경우에는 하단의 방법으로 공개
 - 위탁자의 부서 등 가장 잘 보이는 장소에 30일 이상 비치
 - 정보주체에게 발행하는 간행물, 메일 등을 통하여 연2회 이상 발행
- 위탁자 의무 사항
 - 개인정보의 안전 관리에 관하여 수탁자 교육 등 감독
 - 매월 “붙임4. 위탁업체 개인정보보호 관리실태 점검표” 작성을 통해 수탁자의 개인정보 처리현황 등에 대한 사항을 관리·감독하여야 함

5. 개인정보파일 등록

- 개인정보파일 운용을 시작한 날부터 60일 이내에 환경부 개인정보 보호지침 별지 제7호서식을 작성하여 행정자치부 개인정보보호 종합지원포털(<http://www.privacy.go.kr>)에 등록되어야 하며 등록절차는 다음과 같음

단 계	등록신청	검토승인	공개
수행주체	개인정보보호 분야별 책임자	개인정보 보호책임자	행정자치부장관 (개인정보보호과)
수행활동	개인정보파일 등록변경신청서 작성 및 승인 요청	검토 및 승인 (본부에 요청)	개인정보보호 종합지원포털을 통한 공개

- 등록된 항목 중 하나라도 변경된 경우에는 60일 이내 재등록하여야 함 단, 생성·변경이 상시적으로 변경되는 경우에는 매년 분기마다 변경등록 하여야 함
- 개인정보파일 등록의 예외사항은 다음과 같음
 - 기관 내부 업무처리만을 위해 처리되는 개인정보파일(자문회의, 회의 참석자, 출입기자 등)
 - 국가안전, 범죄상 수사, 공소제기 및 공공기록물 관리에 관한 법률 등에 따라 비밀로 분류된 파일
 - CCTV 등 영상정보처리기를 통해 처리되는 개인영상정보파일

6. 개인정보 영향평가

- <개인정보영향평가 대상>에 해당되는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 개인정보 영향평가를 영향평가기관에 의뢰하여 실시하여야 한다.
 - 정보시스템 구축 고도화 시에는 설계단계에서 영향평가 수행여부 검토

<개인정보영향평가 대상>

- 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
- 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
- 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
- 개인정보영향평가를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일

<영향평가지 고려사항>

- 처리하는 개인정보의 수
- 개인정보의 제3자 제공 여부
- 정보주체의 권리를 해할 가능성 및 그 위험 정도
- 민감정보 또는 고유식별정보의 처리여부
- 개인정보 보유기간

- 영향평가 방법은 행정자치부장관(개인정보보호과)이 지정한 평가기관에 의뢰하고 세부내용은 “개인정보 영향평가에 관한 고시”에 따른다.
- 영향평가 결과를 통지받은 후 2개월 이내에 행정자치부장관에 제출되어야 한다.

7. 개인정보 열람·정정·처리 정지 요구에 대한 조치

- 개인정보의 열람·정정·처리 정지 요구의 접수는 각 개인정보를 처리하는 분야별 개인정보 책임자 및 취급자가 수행하며, 관련사항을 개인정보처리방침을 통해 공개하여야 한다.
- 개인정보처리자는 정보주체가 방문하거나 서면 전화, 전자우편, 전자서명 또는 이용자 ID 등을 이용하여 개인정보의 열람·정정·처리정지를 요구하는 경우에는 본인 여부를 확인하고 법령에 다르게 규정하고 있는 경우를 제외하고는 개인정보를 파기하는 등 지체 없이 필요한 조치를 취하여야 한다.
- 인터넷 홈페이지를 통하여 주된 서비스를 제공하는 개인정보처리자는 정보주체가 인터넷 홈페이지에서 열람·정정·처리정지 요구를 수행할 수 있도록 개인정보처리방침에 정보주체의 권리행사 방법을 명시하여야 한다.

- 개인정보처리자는 정보주체의 동의철회에 따라 정보주체의 개인정보를 파기하는 등의 조치를 취한 경우에는 그 사실을 환경부 개인정보 보호지침 별지서식 제11호, 제12호를 작성하여 정보주체에게 지체없이 통지하여야 한다.
- 개인정보처리자는 다른 법률에 명시되어 있거나 타인의 이익을 부당하게 침해할 우려가 있는 경우 정보주체의 열람·정정·처리정지 요구를 거절할 수 있으며, 이 경우 환경부 개인정보 보호지침 별지서식 제11호, 제12호의 내용을 작성하여 지체없이 통지하여야 한다.
- 정보주체가 열람·정정·처리정지 요구에 대한 거절조치에 이의를 제기할 경우, 개인정보처리자는 해당 사유를 서면, 유선전화 등을 통해 관련사항을 보다 상세하게 안내해야 한다.

8. 개인정보의 파기

- 홈페이지 회원의 개인정보는 회원탈퇴 시 즉시 파기하여야 한다. 또한 사이트의 운영 종료, 보유기간 경과, 개인정보 처리목적 달성 등 개인정보가 불필요하게 되었을 경우에도 지체없이 파기하여야 한다.
- 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 하며 파기방법은 다음과 같다.

개인정보 형태		파기방법
전자적	SQL, ORACLE DB	개인정보 단건파기 : DELETE FROM 테이블명 WHERE 조건절(예 : name="임격정") 개인정보 저장테이블 전체파기 : DROP TABLE 테이블명(테이블 자체를 파기하는 명령어로 사용에 주의를 요함)
	File 형태	GS인증을 득한 파일 영구삭제 프로그램 이용하여 삭제
	HDD, CD, USB 등 저장매체	물리적인 파기(권장) 물리적인 파기가 불가능한 경우 GS인증을 득한 파일 영구삭제 프로그램 이용하여 삭제
문서	파쇄기를 통한 파쇄 또는 소각	

※ 참고 : GS인증을 득한 파일영구삭제 프로그램

업체명	제품명	연락처
하우리	ViRobot DataEraser	02-3676-1100
에스엠에스	BlackMagic-SA	053-381-4114
파이널데이터	FINALERASER	02-3438-6600

- 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다.

9. 개인정보 유출 통지

- 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 사실을 알려야 한다.

<정보주체자에게 알려야 할 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 연락처

- 다만, 유출된 개인정보의 확산 및 추가유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 취한 후 지체 없이 정보주체에게 알릴 수 있다.
- 1만명 이상의 개인정보가 유출된 경우 서면 등의 방법과 함께 인터넷 홈페이지에 7일 이상 게재하여야 한다. 단, 인터넷 홈페이지를 운영하지 않을 경우에는 보기 쉬운 장소에 7일 이상 게시하여야 한다.
- 개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.
- 유출신고방법 및 절차는 다음과 같다.
 - 유출사고 발생 시 개인정보보호 분야별 책임자는 개인정보 유출신고서(환경부 개인정보 보호지침 별지 제3호서식)를 작성하여 환경부 본부 개인정보 보호책임자에게 제출
 - 개인정보 보호책임자는 1만명 이상의 정보주체에 관한 개인정보가 유출된 경우 행정자치부장관과 전문기관(한국정보화진흥원, 한국인터넷진흥원)에 신고

V

개인정보보호의 처리단계별 기술적·관리적 안전조치

1. 개인정보취급자 접근 권한 관리

- 접근권한 담당자는 “붙임5. 접근권한 검토보고서” 양식에 따라 각 개인정보처리시스템별로 반기1회 접근권한을 검토하여야 하며 상세관리방안은 다음과 같다.
 - 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 정하여 업무 담당자에 따라 차등 부여하여야 한다.
 - 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 한다.
 - 개인정보처리자는 개인정보처리시스템에 대한 접근권한의 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.
 - 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.
 - 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

2. 접근 통제

- 비밀번호 관리
 - 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.
 - ※ 세부내용은 환경부 정보보안지침 제30조(비밀번호 관리)에 따른다.
- 접근통제시스템 설치 및 운영 방안
 - 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 침입차단시스템(Firewall) 또는 침입방지시스템(IPS) 등을 설치·운영하여야 한다.
 - 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
 - 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 재분석하여 불법

적인 개인정보 유출 시도를 탐지

- 외부망으로부터 개인정보처리시스템에 대한 접속은 원칙적으로 차단하여야 한다. 다만, 개인정보처리자가 외부망을 통해 개인정보처리시스템에 접속이 필요한 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하여야 한다.
- 개인정보처리자는 인터넷 홈페이지에서 다른 법령에 근거하여 정보주체의 본인확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 추가적인 정보를 확인하여야 한다.
 - 추가적 정보 : 아이핀, 휴대폰, 공인인증서
- 개인정보처리시스템 또는 업무용 컴퓨터인 경우 P2P, 공유설정 등을 기본적으로 사용하지 않는 것이 원칙이나, 업무상 꼭 필요한 경우에는 권한 설정 등의 조치를 통해 업무상 꼭 필요한 자만 접근할 수 있도록 설정한다.
 - P2P, 공유설정 등의 사유를 명확히 명기하고 기록
 - 드라이브 전체 또는 불필요한 폴더가 공유되지 않도록 조치
 - 공유폴더에 개인정보파일이 포함되지 않도록 정기적으로 점검
 - 인터넷 홈페이지를 운영중인 개인정보처리시스템의 경우 상단의 조치사항을 필수적으로 이행하고 IDS/IPS 장비 등을 통해 접속자들의 지속적인 모니터링 필요
- 개인정보처리시스템을 이용하지 않고 단순히 업무용 컴퓨터에 개인정보를 저장하는 경우 운영체제(OS:Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 사용하여 불법적인 접근을 차단할 수 있다.
- 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점 점검
- 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등 보호조치

3. 개인정보의 암호화

- 「개인정보 보호법」 제24조 및 제24조의2에 근거하여 보유중이거나 신규로 수집하는 주민등록번호는 모든 구간에서 필수적으로 암호화하여야 한다.
- 「개인정보 보호법 시행령」 제21조, 제21조의2 및 제30조제1항제3호에 따라 암호화가 필요한 개인정보 및 암호화 방법은 다음과 같다.

구 분	암호화 대상		암호화
전송 시	고유식별정보, 비밀번호, 바이오정보		일방향 암호화(필수)
저장 시	비밀번호		일방향 암호화(필수)
	바이오 정보		양방향 암호화(필수)
	고유식별정보 (운전면허번호, 외국인 등록번호, 여권번호)	인터넷, DMZ 구간	양방향 암호화(필수)
		내부망	위험도분석 결과에 상관없이 암호화 여부 결정 가능
	업무용 PC, 모바일기기	어플리케이션 등을 활용한 암호화	

- 운전면허번호, 외국인등록번호, 여권번호 등을 내부망 저장하는 경우 개인정보 영향평가 또는 위험도 분석을 통해 암호화 여부를 결정할 수 있으며 위험도 분석은 “개인정보위험도분석 기준 및 해설서(행정자치부 공고 제2012-112호)”에 의해 수행되어야 함
- 개인정보처리자는 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.
 - 특히, SEED, MD5, SHA128, 자체개발 알고리즘과 같이 안전하지 않은 알고리즘을 사용하거나, 비밀번호 저장 시 양방향 암호화 알고리즘을 사용하지 않아야 함
 - 주민등록번호를 운영하는 시스템에서 검색 키를 사용하는 경우, 속도 등 성능을 고려하여 일부 정보만 암호화 조치를 취할 수 있음
 - ※ 주민등록번호의 경우 뒷자리 6개 번호 이상 암호화 조치 필요(예시: 700101-1#...&)
- 암호화 제품은 “환경부 정보보안지침 별표3 정보시스템 유형별 도입요건 (검증필 암호모듈)”을 만족하는 제품을 선정하여야 한다.
 - 전송구간 암호화는 SSL 인증서를 도입하여 적용
 - DB암호화는 구축환경의 성능, 안전성 등을 고려하여 응용 API 방식, DB 암호화 제품 도입 중에서 선택할 필요가 있으며, 상세한 내용은 “한국 인터넷진흥원, 개인정보암호화 조치안내서”를 참조하여야 함
- 암호화가 필요한 개인정보(고유식별정보, 비밀번호, 바이오정보)가 식별되는 경우 개인정보처리자는 암호화 계획을 수립하여 분야별 개인정보 책임자의 승인을 득한 후 적용하여야 한다.
- 고유식별정보를 업무용 컴퓨터에 저장하여 관리하거나, 개인정보처리시스템으로부터 개인정보취급자의 PC에 내려 받아 저장할 때는 안전한 암호화 알고리즘이 탑재된 암호화 소프트웨어 등을 이용하여 암호화함으로써 불법적인 노출 및 접근으로부터 차단하여야 한다.

4. 접근기록의 보관 및 점검

- 접근권한 담당자는 “붙임6. 접속기록 검토보고서” 양식에 따라 각 개인 정보처리시스템별로 반기1회 접속기록을 점검하여야 하며 상세관리방안은 다음과 같다.
- 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우, 수행한 업무내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등의 접속기록을 최소 6개월 이상 보관하여야 한다.
 - 개인정보취급자 1명(Root, Admin 등)이 개인정보처리시스템을 관리하는 경우, 전자적 로그를 남기지 않고, 접속 기록을 수기로 작성하여 상급자의 승인을 받아도 가능하다.

<접속기록 항목 예시>

필수 기록 항목	설명
ID	개인정보취급자 식별정보
날짜 및 시간	접속 일시
접속자 IP 주소	접속지 정보
수행 업무	열람, 수정, 삭제, 인쇄, 입력 등

- 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실 되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.
 - 정기적으로 접속기록 백업을 수행하여 개인정보처리시스템 이외의 별도의 보조저장매체나 별도의 저장장치에 보관하여야 함
 - 접속기록에 대한 위·변조를 방지하기 위해 CD-ROM 등과 같은 덮어쓰기 방지 매체를 사용하는 것이 바람직
 - 접속기록을 수정 가능한 매체(HDD 또는 테이프 등)에 백업하는 경우에는 무결성 보장을 위해 위·변조 여부를 확인할 수 있는 정보를 별도의 장비에 보관·관리할 수 있음

※ 접속기록을 HDD에 보관하고, 위·변조 여부를 확인할 수 있는 정보(HMAC 값, 전자서명값 등)는 별도의 HDD 또는 관리대장에 보관하는 방법으로 관리할 수 있다.

5. 보안프로그램의 설치 및 운영

- 보안프로그램 설치/운영 현황 및 버전 업그레이드 계획은 다음과 같음.

보안프로그램명	업데이트 주기	버전 업그레이드/교체계획
Ahn-Lab V3	매일	없음

- 보안프로그램 설치 운영에 따른 관리방안은 다음과 같아야 한다.
 - 백신 소프트웨어 등의 보안 프로그램은 실시간 감시 등을 위해 항상 실행된 상태를 유지
 - 백신 소프트웨어 등 보안 프로그램은 일 1회 이상 주기적 업데이트
- 운영체제(OS)·응용 프로그램의 보안 취약점을 악용하는 악성 프로그램 경보가 발령되었거나, 응용 프로그램, 운영체제 제작업체에서 보안 업데이트 공지가 있는 경우에는 감염 및 피해를 막기 위해 즉시 업데이트를 실시하여야 한다.

6. 물리적 접근제한

- 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.
 - 전산실을 제한구역으로 지정하여 출입통제(잠금장치 설치)
- 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.
- 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출입 통제를 위한 보안대책을 마련하여야 한다.

7. 안전성 확보조치 계획

- 「개인정보 보호법」 제24조 개정에 따른 안전성 확보조치 계획 수립

안전성 확보조치 활동	조치계획
개인정보 관리실태(개인정보 수집, 암호화, 파기여부 등) 점검	반기1회(5/10월)
개인정보파일 일제정비	연1회(7월)
‘내PC지키미’ 실행 및 취약점 제거조치 실시	매월

8. 재해 및 재난 대비 물리적 안전조치

- 개인정보처리자는 화재, 홍수 등의 재해·재난 발생시 붙임 9“재해·재난 대비개인정보처리시스템 위기대응 매뉴얼”의 대응절차를 준수하고 정기적으로 점검하여야 한다.
- 개인정보처리자는 재해·재난 발생시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

VI 개인정보보호 교육 및 홍보

1. 개인정보보호 인력에 대한 교육

- 개인정보보호책임자 등 관리자는 1회 이상 개인정보보호 교육 등에 참석
- 개인정보보호 담당자는 미래창조과학부 및 행정자치부 등에서 실시하는 개인정보보호 교육을 연간 20시간 이상 의무적으로 참석
- 분야별책임관은 개인정보 취급 업무를 처음 시작하는 자에게 의무사항을 주지시키고, 수시 또는 정기적으로 보안교육 실시
 - 개인정보보호책임자 및 분야별책임자는 담당자 부주의 또는 고의 등의 원인으로 개인정보 노출, 유출사례가 발생되지 않도록 조치
- 개인정보보호 교육에 다음의 내용이 포함될 수 있다.
 - 개인정보보호의 중요성 설명
 - 내부관리계획의 준수 및 이행
 - 위협 및 대책이 포함된 조직 보안 정책, 보안지침, 지시사항, 위협관리 전략
 - 개인정보시스템 하드웨어 및 소프트웨어를 포함한 시스템의 정확한 사용법
 - 개인정보의 기술적·관리적 보호조치 기준 이행
 - 개인정보보호 위반을 보고해야 할 필요성
 - 개인정보보호업무의 절차, 책임, 작업 설명
 - 개인정보보호 관련자들의 금지 항목들, 준수사항 이행 관련 절차 등
- 직원의 개인정보보호 교육 기회 제공
 - 매뉴얼 교재, e-learning 콘텐츠, 홍보영상물 등을 직장교육에 활용
 - 직원들의 개인정보보호 인식 제고를 위해 자체 교육을 실시하고, 교육 기관에서 운영하는 프로그램에 참석토록 조치

2. 개인정보보호 홍보 및 지도점검

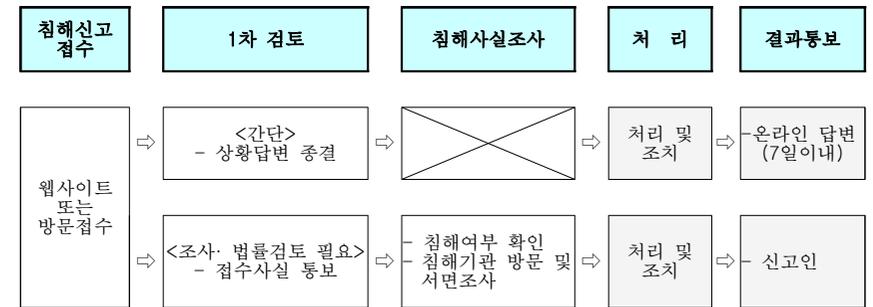
- 개인정보보호 관련 추진 지침 및 안내 자료 등을 전 직원을 대상으로 배포
- 개인정보관리실태를 연 1회 이상 정기적으로 점검

VII 개인정보 침해 대응 및 피해구제

1. 개인정보 침해 신고

- 개인정보처리자가 개인정보를 처리할 때 개인정보에 관한 권리 또는 이익을 침해받은 사람은 그 침해사실을 개인정보침해 신고센터로 신고할 수 있다.
- 개인정보침해 신고센터
 - 한국인터넷진흥원 개인정보침해 신고센터(<http://privacy.kisa.or.kr>)
 - ※ 팩스, 우편, 방문용은 민원신청서식을 다운받아 신청
 - 전화 : (국번없이) 118

【개인정보 침해신고 처리절차】



2. 권익침해 구제방법

- 개인정보 주체는 개인정보 침해로 인한 구제를 받기 위하여 개인정보 분쟁조정위원회, 한국인터넷진흥원 개인정보 침해신고센터 등에 분쟁 해결이나 상담 등을 신청할 수 있다.
- 기타 개인정보 침해의 신고 및 상담에 대하여는 아래의 기관에 문의한다.
 - 개인정보침해신고센터 : (국번 없이) 118
 - 개인정보분쟁조정위원회 : (국번 없이) 118
 - 대검찰청 사이버수사과 : 02-3480-3570 (<http://www.spo.go.kr>)
 - 경찰청 사이버안전국 : (국번 없이) 182 (<http://cyberbureau.police.go.kr>)

3. 행정심판 청구절차

- 법제35조(개인정보의 열람), 제36조(개인정보의 정정·삭제), 제37조(개인정보의 처리정지 등)의 규정에 의한 요구에 대하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 행정심판법이 정하는 바에 따라 행정심판을 청구할 수 있다.

※ 행정심판에 대한 자세한 사항은 온라인 행정심판(www.simpan.go.kr), 법제처 홈페이지(www.moleg.go.kr) 참고

개인정보 처리단계별 준수사항 및 위반시 벌칙사항

구분	주요내용	처벌 및 벌칙
수집·이용	민감정보(사상·신병·정당가입·건강 등) 처리기준 위반(제23조)	5년 이하 징역 또는 5천만원 이하 벌금
	고유식별정보(주민등록·여권·운전면허 번호 등) 처리기준 위반(제24조)	5천만원 이하 벌금
	부당한 수단이나 방법에 의해 개인정보를 취득하거나 개인정보처리에 관한 동의를 얻는 행위를 한 자(제59조)	3년 이하 징역 또는 3천만원 이하 벌금
	개인정보의 수집기준 위반(제15조)	
	만14세 미만 아동의 개인정보 수집시 법정대리인 동의획득여부 위반(제22조)	5천만원 이하 과태료
	탈의실·목욕실 등 영상정보처리기기 설치 금지 위반(제25조)	
	최소한의 개인정보 외 정보의 미동의를 이유로 재화 또는 서비스 제공을 거부한 자(제16조, 제22조)	3천만원 이하 과태료
제공·위탁	주민등록번호를 제공하지 아니할 수 있는 방법 미제공(제21조)	
	동의획득방법 위반하여 동의받은 자(제22조)	1천만원 이하 과태료
	정보주체의 동의 없는 개인정보 제3자 제공(17조)	10년 이하 징역 또는 1억원 이하 벌금
	개인정보의 목적 외 이용·제공(제18조, 제19조, 제26조)	
개인정보	개인정보 주체에게 알려야 할 사항을 알리지 아니한 자(제15조, 제17조, 제18조, 제26조)	3천만원 이하 과태료
	업무위탁 시 공개의무 위반(제26조)	1천만원 이하 과태료
	개인정보의 누설 또는 타인 이용에 제공(제59조)	5년 이하 징역 또는 5천만원 이하 벌금
	개인정보의 훼손, 멸실, 변경, 위조, 유출(제59조)	
	영상정보처리기기 설치목적과 다른 목적으로 임의 조작하거나 다른곳을 비추는 자 또는 녹음기능을 사용한 자(제25조)	3년 이하 징역 또는 3천만원 이하 벌금
	직무상 알게 된 비밀을 누설하거나 직무상 목적 외 사용한 자(제60조)	
	안전성 확보에 필요한 보호조치를 취하지 않아 개인정보를 도난·유출·변조 또는 훼손당하거나 분실한 자(제24조, 제25조, 제29조)	2년 이하 징역 또는 1천만원 이하 벌금
	안전성 확보에 필요한 조치의무 불이행(제24조, 제25조, 제29조)	
	영상정보처리기기 설치·운영기준 위반(제25조)	3천만원 이하 과태료
	개인정보를 분리해서 저장·관리하지 아니한 자(제21조)	
안전관리	개인정보 처리방침 미공개(제30조)	
	개인정보관리책임자 미지정(제31조)	
	영상정보처리기기 안내판 설치 등 필요조치 불이행(제25조)	1천만원 이하 과태료
	개인정보의 정정·삭제요청에 대한 필요한 조치를 취하지 않고, 개인정보를 계속 이용하거나 제2자에게 제공한 자(제36조)	
정보주체	개인정보의 처리정지 요구에 따라 처리를 중단하지 않고 계속 이용하거나 제3자에게 제공한 자(제37조)	2년 이하 징역 또는 1천만원 이하 벌금
	개인정보 유출사실 미통지(제34조)	3천만원 이하 과태료
	정보주체의 열람 요구의 부당한 제한·거절(제35조)	
	정보주체의 정정·삭제요청에 따라 필요 조치를 취하지 아니한 자(제36조)	
	처리정지된 개인정보에 대해 파기 등의 조치를 하지 않은 자(제37조)	
	시정명령 불이행(제64조)	1천만원 이하 과태료
	정보주체의 열람, 정정·삭제, 처리정보 요구 거부 시 통지의무 불이행(제35조, 제36조, 제37조)	
권익보호	관계물품·서류 등의 미제출 또는 허위제출(제63조)	
	출입·검사를 거부·방해 또는 기피한 자(제63조)	
	출입·검사를 거부·방해 또는 기피한 자(제63조)	1천만원 이하 과태료
파기	개인정보 미파기(제21조)	3천만원 이하 과태료

※ 개인정보정보법상의 처벌은 **벌칙**과 **과태료**로 구분, 벌칙은 업무방해 목적의 중대 법익침해에 해당되며 과태료는 주로 절차적 의무위반 사항에 대해 적용

개인정보처리자 개인정보보호 자가진단표

구분	질문항목	Yes	No	N/A
[법률준수]				
1. 개인정보보호 정책 및 자원	1) 개인정보보호 업무를 수행하기 위한 조직이 구성되어 있는가?			
	2) 개인정보보호를 위한 기반이(예산편성 등) 마련되어 있는가?			
	3) 개인정보 보호책임자가 지정되어 있는가?			
	4) 개인정보 보호책임자는 교육, 관리·감독 등 역할을 t행하고 있는가?			
	5) 개인영상정보 보호책임자 지정 및 역할을 수행하고 있는가?			
	6) 개인정보의 안전한 처리를 위한 내부 관리계획이 수립되어 있는가?			
	7) 개인정보처리자가 내부감사(관리·감도 등)를 수행하는가?			
2. 개인정보보호 교육	8) 개인정보보호 교육 계획이 수립되어 있는가?			
	9) 개인정보 보호책임자가 교육을 받고 있는가?			
	10) 개인정보보호 교육을 수행하고 있는가?			
3. 개인정보 처리방침	11) 업무위탁 시, 수탁자에 대해 개인정보보호 교육을 수행하고 있는가?			
	12) 개인정보 처리방침을 공개하고 있는가?			
	13) 개인정보 처리방침의 내용(처리 및 보유기간, 위탁사항, 파일등록 등)은 적절한가?			
4. 개인정보 영향평가	14) 개인정보 처리방침의 변경 내용을 지속적으로 공개 및 이력관리를 하는가?			
	15) 개인정보 영향평가 대상인가?			
5. 개인정보처리 시스템 보안운영	16) 대상이라면, 개인정보 영향평가를 수행 하는가?			
	17) 개인정보를 처리하는 시스템, 업무용컴퓨터에 백신소프트웨어를 설치운영 하는가?			
	18) 침입차단(F/W), 방화(IPS), 탐지(IDS) 등 접근통제시스템을 설치운영 하는가?			
	19) 개인정보를 처리하는 시스템에 비인가 접근 등에 대한 상시 모니터링을 수행하는가?			
6. 개인정보처리 시스템의 접근 통제	20) 인터넷 홈페이지 취약점 점검 등을 수행 하는가?			
	21) 개인정보처리시스템의 중요도(민감도) 및 업무연관성 등을 고려하여 담당자별 차등 접근권한 절차를 마련하는가?			
	22) 전보 또는 퇴직 인력에 대해 개인정보처리시스템의 접근권한을 즉시 삭제 하는가?			
	23) 접근권한 부여·변경·말소에 대한 이력관리를 수행하는가?			

구분	질문항목	Yes	No	N/A	
	24) 비밀번호 작성규칙을 수립하여 개인정보처리시스템에 적용하고 있는가?				
	25) 비인가된 P2P, 웹하드 등 공유설정에 대한 차단을 하고 있는가?				
	26) 개인정보처리시스템 접근관련 1인당 한 개의 사용자계정 발급 및 사용자 인증(PKI, IP제한 등)을 하고 있는가?				
	27) 전산실, 자료보관실 등 개인정보를 취급하는 공간에 대해 출입통제 절차를 수립·운영 하고 있는가?				
	28) 개인정보가 포함된 서류 및 저장매체(USB, CD) 등을 잠금 장치가 있는 안전한 장소에 보관하는가?				
	7. 개인정보 암호화	29) 고유식별정보(주민등록번호, 여권번호 등), 바이오정보(지문, 얼굴 등), 비밀번호가 암호화 되어 있는가?			
		30) 비밀번호는 일방향 암호화를 적용하여 저장되는가?			
31) 개인정보 암호화 시, 안전한 알고리즘을 사용하고 있는가?					
32) 사용자 PC부터 웹서버 구간 간 암호화를 적용 하였는가?					
33) 사용자 PC에 저장된 개인정보파일 암호화하고 있는가?					
8. 개인정보처리시스템 로그관리	34) 개인정보처리시스템 접속기록을 6개월 이상 보관 관리 하는가?				
	35) 개인정보처리시스템 접속 기록이 위변조 및 도난, 분실되지 않도록 안전하게 보관하고 있는가?				
	36) 개인정보처리시스템의 접속기록 점검 및 후속조치를 수행 하는가?				
9. 개인정보 수집 동의	37) 개인정보 수집 시, 정보주체의 동의를 받고 있는가?				
	38) 고유식별정보(주민등록번호, 여권번호 등) 수집 시, 별도로 동의를 받고 있는가?				
	39) 만 14세 미만 아동의 개인정보를 수집 시, 법정대리인에게 동의를 받고 있는가?				
	40) 동의를 받는 방법은 적절한가?				
10. 개인정보 수집	41) 서비스 제공을 위해 꼭 필요한 최소한의 정보만을 수집하는가?				
	42) 정보주체 이외로부터 수집한 개인정보가 있는 경우, 정보주체의 요구 시 알려주는가?				
	43) 회원가입 시, 주민등록번호 수집에 대한 대체수단(i-Pin 등)을 사용하고 있는가?				
11. 이용 및 제공	44) 제3자 제공에 관한 사항을 정보주체에게 알리고 동의를 받는가?				
	45) 개인정보의 처리 업무를 위탁하는 경우, 문서(계약서 등)에 의하여 하고 있는가?				
	46) 위탁업무의 내용과 수탁자(위탁받아 처리하는 자)를 공개하고 있는가?				
	47) 수탁자에 대한 교육 및 감독을 수행하고 있는가?				
	48) 개인정보 수집 목적을 넘어 이용하거나 제공하는 경우, 별도 동의를 받거나 다른 법률에 근거하고 있는가?				
	49) 영업양도, 합병 등으로 개인정보를 다른 사람에게 이전				

구분	질문항목	Yes	No	N/A
	하는 경우, 정보주체에게 그 사실을 알리는가?			
	50) 개인정보의 국외 이전 시, 정보주체에게 알리고 동의를 받는가?			
12. 개인정보 파기	51) 개인정보 처리목적 달성 시, 지체 없이 파기하고 있는가?			
	52) 개인정보를 파기할 때, 다시 복원하거나 재생할 수 없는 상태로 완벽하게 파기하는가?			
	53) 개인정보 파기에 관한 사항을 기록하고 관리하는가?			
	54) 다른 법령에 따라 개인정보를 파기하지 않고 보존하는 경우, 다른 개인정보와 분리하여서 저장·관리하는가?			
13. 개인정보파일	55) 개인정보파일을 운용하는 경우, 개인정보보호종합지원 시스템(intra.privacy.go.kr)에 등록 하였는가?			
	56) 개인정보파일 등록 항목을 모두 등록 하였는가?			
	57) 개인정보파일의 보유기간이 타당한가?			
	58) 개인정보파일이 불필요하게 되었을 때 지체 없이 파기 하는가?			
14. 영상정보처리기기 설치·운영	59) 영상정보처리기기 설치에 따른 전문가 및 이해관계자의 의견을 수렴 하였는가?			
	60) 영상정보처리기기 설치 시, 안내판을 설치하였는가?			
	61) 영상정보처리기기를 임의조작하거나 녹음기능을 사용하지 않는가?			
	62) 영상정보처리기기 운영·관리방침이 수립되어 있는가?			
	63) 영상정보처리기기가 설치목적에 맞게 이용되는지 등에 대한 점검을 수행하고 있는가?			
	64) 영상정보처리기기를 안전하게 보관·관리하고 있는가?			
	65) 목적달성 시 개인영상정보를 지체없이 파기하고 있는가?			
	66) 영상정보처리 위탁 시 문서를 통해 준행하고 있는가?			
	67) 정보주체의 개인영상정보 열람 요구에 관한 사항을 기록하고 관리하는가?			
	68) 개인영상정보를 이용·제공, 파기, 열람하는 경우 해당내용을 기록하고 관리하는가?			
15. 개인정보 유·노출 대응절차	69) 개인정보의 유·노출 및 침해사고에 대한 대응절차가 수립되어 있는가?			
	70) 당해연도에 개인정보 유출 또는 노출 사고가 발생하지 않았는가?			
	71) 개인정보 유출사고 발생에 따른 유출통지 및 신고를 하였는가?			
16. 정보주체의 권리 보장	72) 개인정보의 열람·정정·삭제 및 처리정지에 관한 사항을 안내하고 있습니까?			
	73) 다른 기관에서 개인정보를 제공받아 개인정보 정정·삭제 및 처리정지에 대한 사항 발생 시 보고조치를 수행하고 있습니까?			

[붙임 3]

개인정보파일 목록

기관명	부서	파일명
수도권대기환경청	자동차관리과	배출가스저감장치 부착차량 사후관리
		은행경유차 배출가스 저감사업 국고보조금 집행관리

*** 개인정보파일 등록**

> 개인정보파일 운용을 시작한 날부터 60일 이내에 행정자치부에서 운영하는 개인정보보호 종합지원시스템(intra.privacy.go.kr)에 개인정보파일을 게시한다.

위탁업체 개인정보보호 관리실태 점검표

(위탁업체명/사업명 : 000/0000 유지관리(000 시스템))

점검일시 : '17. . .

점검항목	점검방법	예	아니오	해당 없음	비고
1. 개인정보 처리방침의 수립 및 공개여부	유지관리 중인 웹사이트(홈페이지)에서 개인정보 수집 시 개인정보 처리방침 수립 및 공개여부 확인				내부 시스템 제외
2. 개인정보취급자의 보안서약서 작성여부	유지관리사업 용역계약 체결 시 보안서약서 또는 개인정보보호 서약서 징구여부 확인				
3. 개인정보취급자에 대한 교육 실시여부	위탁업체 직원들에 대한 개인정보보호 교육 실시여부 점검(교육계획서, 참석자 명단 등) ※ 본부는 주기적으로 정보화(담)에서 교육 실시한 것으로 같음 가능하나 소속·산하기관에서는 별도 교육 실시 필요				분기 또는 반기 교육 실시
4. 개인정보 암호화	고유식별정보(주민등록번호) 수집 시 암호화 여부				“비고”란에 시스템에 적용된 암호화 알고리즘 기입 ex> 3DES, AES 등
	바이오정보 수집 시 암호화 여부				상동
	웹사이트 사용자 비밀번호 암호화 여부 ※ 일방향 암호화 적용 ex> SHA-256, SHA-256, 384, 512 등				상동
	사용자 PC로부터 웹서버 구간 간 암호화 여부				SSL 인증서 설치

점검항목	점검방법	예	아니오	해당 없음	비고
5. 접근 권한 및 접근 통제	침입차단시스템 또는 침입탐지시스템의 설치 및 운영 여부 비인가된 P2P, 웹하드, 공유설정에 대한 차단여부				대전센터 입주시스템은 “예”로 점검
6. 물리적 접근 방지	전산실, 자료보관실 등 물리적 보관장소에 대한 출입통제 절차 수립여부 개인정보가 포함된 서류 및 저장장치에 대한 물리적 보안조치여부				대전센터 입주시스템은 “예”로 점검
7. 개인정보처리시스템에 대한 접근 권한 차등여부	개인정보처리시스템 업무에 따른 접근 권한 차등부여 및 1인 1계정 사용 여부				
8. 개인정보처리시스템에 대한 접속기록 보관·관리여부	접속기록(ID, 일시, 접속자 IP주소, 수행업무(열람, 수정, 삭제 등)에 대한 생성여부 접속기록 최소 6개월 이상 보관 여부				
9. 개인정보 목적 달성 시 지체없이 파기여부	개인정보 보유 목적 달성 시, 개인정보 보유기간 만료 시에 따른 파기 여부				
	전자적 파일형태 파기 시 복원이 불가능한 방법으로 영구 삭제 여부 ※ 복원이 불가능한 방법으로 영구 삭제 ex> 로우레벨포맷, 또는 디가우저를 이용한 HDD 파기 등				
10. 목적 외 이용 및 재위탁 금지 여부	출력물 문서 폐기 시 파쇄(분쇄) 또는 소각 처리 여부				
11. 개인정보취급자 PC에 대한 “PC 지킴이” 실행여부	위탁 업무 목적 외 개인정보 이용·제공 여부				
	매월 1회 이상 PC 지킴이 실행 및 취약점 조치 여부				

점검자(개인정보처리시스템 유지관리 담당자) :

(서명)

확인자(개인정보처리시스템 담당 공무원) :

(서명)

접근권한 검토보고서

점검일	2017.XX.XX	점검자	XXXXXX
점검 대상기간	2017.XX.XX~2014.XX.XX		
대상 시스템명	환경민원포털		
권한분류	관리자, 민원정보 관리자, 일반사용자 (예시)		
점검결과			
NO.	점검 시나리오	점검 결과	개선 여부
1	접근권한의 신규/변경/말소 기록이 대장이나 전자적인 형태(로그)로 관리되고 있다.	Y	Y
2	1의 항목에서 대장으로 관리하고 있을 경우 점검 대상기간 내 “입퇴사자 및 보직변경자 명단”이 모두 “개인정보접근권한 관리대장”에 기록되고 있으며 기록된 사항이 모두 정확하다.	N	N
3	2의 항목에서 신규/변경/말소내역이 있을 경우 시스템 관리자 화면 및 사용자 DB 테이블에서 해당 사용자의 권한정보를 조회하고 조회한 권한 정보가 “개인정보접근권한 관리대장”과 동일하다. (특히 다른부서로 이동하거나 퇴사, 계약만료된 사용자는 필히 확인한다.)		N/A
4	2의 항목 검토 후 신규/변경/말소내역이 없을 경우 기존 개인정보취급자를 대상으로 권한이 변경되거나 업무범위를 초과하여 권한이 부여된 내역이 있는지 확인한다.(업무범위를 초과한 내역이 있을 경우에만 Y)		
5	접근권한신규/변경/말소내역이 “접근권한관리대장”에 3년치이상 보관되고있다.		
6	1의 항목에서 전자적인 형태로 관리하고 있을 경우 점검기간내 “입퇴사자 및 보직변경자 명단”이 모두 접근권한 부여/해지 로그로 관리되고 있는지 확인한다.(2,3,4번 항목을 점검하고 결과를 기록한다. 모두 적정할 경우에만 Y)		
7	1의 항목에서 전자적인 형태로 관리하고 있을 경우 접근권한 부여해지 로그가 위·변조를 방지하기 위해 별도의 저장장치에 보관하고 있다. (웹서버에서 로그 관리하는 경우는 별도보관 아님)		
8	7의 항목에서 별도저장 되고 있을 경우 스토리지 용량이 3년치 이상의 로그를 수용할 수 있다.		
9	하나의 개인정보취급자 계정으로 다수의 PC에서 중복로그인 할 수 없다.		
10	OS, DB, ApplicatiOn에 특수권한 (SUPER USER) 이 부여된 사용자는 1명이다.		
11	개인정보취급자 등록 시 패스워드 작성규칙이 숫자,문자,특수문자 3자기 조합 9자리 이상으로 구성되어 있는지 확인한다.		

접속기록 검토보고서

점검일	2017.XX.XX	점검자	XXXXXX
점검 대상기간	2017.XX.XX~2014.XX.XX		
대상 시스템명	환경민원포털		
권한분류	관리자, 민원정보 관리자, 일반사용자 (예시)		
점검결과			
NO.	점검 시나리오	점검 결과	개선 여부
1	개인정보취급자의접속기록이관리되고있다.		
2	1의 항목에서 관리되고 있다면 취급자 ID, 접속 일시, 접속지 IP, 수행업무를 포함하여 관리하고 있다.		
3	1의 항목에서 관리되고 있다면 접속기록은 6개월 이상 보관하고 있다.		
4	1의 항목에서 관리되고 있다면 접속로그가 많이 기록된 일자의 내용을 샘플링하여 부적절한 IP, 권한 등으로 접속한 내역이 있는지 점검한다.		

개인정보 처리방침

제1조(개인정보의 처리목적) ① 수도권청은 다음의 목적을 위하여 개인정보를 처리합니다. 처리한 개인정보는 다음 목적 이외의 용도로는 사용하지 않습니다.

1. 민원처리

가. 민원인의 신원 확인, 민원사항 확인, 민원회신 등을 위한 연락·통지, 처리결과 통보 등의 목적으로 개인정보를 처리합니다.

나. 개인정보 열람, 개인정보 정정·삭제, 개인정보 처리정지 요구, 개인정보 유출 사고 신고 등 개인정보와 관련된 민원처리를 목적으로 개인정보를 처리합니다.

2. 수당 지급 및 연구개발사업 등의 업무처리

가. 수당 지급 및 연구개발사업 등의 업무처리를 위하여 개인정보를 처리합니다.

3. 기간제 근로자 및 무기계약직 관리

가. 기간제 근로자 및 무기계약직의 계약기간 및 임용 정보 등의 확인을 위하여 개인정보를 처리합니다.

4. 운행경유차 배출가스 저감사업의 국고보조금 집행관리 및 저감장치 부착차량 사후관리

가. 운행경유차 배출가스 저감장치 부착차량의 국고보조금 지급 금액의 적정성 여부 및 적정 부착 여부, 매연농도 측정 등을 위하여 개인정보를 처리합니다.

5. 위원회 구성 및 홍보단 등의 위촉 업무

가. 위원 및 홍보단 등의 위촉 업무를 위하여 개인정보를 처리합니다.

② 처리하고 있는 개인정보는 정해진 목적 이외의 용도로는 이용되지 않으며, 이용 목적이 변경될 경우에는 사전에 이용자에게 알리고 동의를 받을 예정입니다.

※ 좀 더 상세한 수도권대기환경청의 개인정보파일 등록사항 공개는 행정자치부 개인정보보호 종합지원 포털(www.privacy.go.kr) → 개인정보민원 → 개인정보열람 등 요구 → 개인정보파일 목록 검색 → 기관명에 “수도권대기환경청” 입력 후 조회 메뉴를 활용해주시기 바랍니다.

제2조(처리하는 개인정보의 항목) 민원처리 등을 위하여 처리하는 개인정보 항목은 아래와 같습니다.

1. 수집항목 : 성명, 생년월일, 집 주소, 직업, 이메일, 일반전화번호, 휴대전화번호, 계좌번호, 차량번호, 차대번호 등

제3조(개인정보의 처리 및 보유기간) ① 수도권청에서 처리하는 개인정보는 법령에 따른 개인정보 보유·이용기간 또는 정보주체로부터 개인정보를 수집 시에 동의 받은 기간 내에서 개인정보를 처리·보유합니다.

1. 민원처리

가. 수집근거 : 개인정보 보호법 제15조 제1항 “정보주체의 동의를 받은 경우”

나. 보유기간 : 회원 탈퇴 의사 표시 후 5일까지

2. 수당 지급 및 위원회 구성, 연구개발사업 등의 업무처리 : 사업종료 시까지

3. 기간제 근로자 및 무기계약직 관리 : 3년

4. 운행경유차 배출가스 저감사업의 국고보조금 집행관리 및 저감장치 부착차량 사후관리 : 10년

5. 용역 및 연구개발사업 등의 업무처리 : 사업 종료시까지

6. 위원회 구성 및 홍보단 등의 위촉 업무 : 위원회 및 홍보단 구성 종료시까지

제4조(개인정보의 제3자 제공) 수도권청은 이용자의 개인정보를 제1조(개인정보의 처리 목적)에서 명시한 범위 내에서 처리하며, 이용자의 사전 동의 없이 본래의 범위를 초과하여 처리하거나 제3자에게 제공하지 않습니다. 다만, 다른 법률에 특별한 규정이 있는 경우 또는 범죄 수사와 같이 개인정보 보호법 제18조 제2항에 해당되는 경우는 예외로 됩니다.

제5조(개인정보 처리의 위탁) ① 수도권청은 개인정보를 위탁 처리할 경우에는 개인정보 보호법 제25조에 따라 위탁업무 수행목적 외 개인정보 처리금지, 기술적·관리적 보호조치, 재위탁 제한, 수탁자에 대한 관리·감독, 손해배상 등 책임에 관한 사항을 계약서 등 문서에 명시하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독할 것입니다.

② 개인정보 처리를 위한 위탁업무가 발생할 시에는 지체 없이 본 개인정보 처리방침을 통하여 공개하도록 하겠습니다.

제6조 (정보주체의 권리·의무 및 그 행사방법) 정보주체(만 14세 미만인 경우에는

법정대리인을 말함)는 언제든지 다음 각 호의 개인정보 보호 관련 권리를 행사할 수 있습니다.

1. 개인정보 열람요구
2. 오류 등이 있을 경우 정정 요구
3. 삭제요구
4. 처리정지 요구

가. 권리 행사는 개인정보 보호법 시행규칙 별지 제8호 서식에 따라 작성 후 서면, 전자우편, 모사전송(FAX) 등을 통하여 하실 수 있으며, 수도권청은 이에 대해 지체 없이 조치하겠습니다.

나. 정보주체가 개인정보의 오류 등에 대한 정정 또는 삭제를 요구한 경우에는 정정 또는 삭제를 완료할 때까지 당해 개인정보를 이용하거나 제공하지 않습니다.

다. 권리 행사는 정보주체의 법정대리인이나 위임을 받은 자 등 대리인을 통하여 하실 수 있습니다. 이 경우 개인정보 보호법 시행규칙 별지 제11호 서식에 따른 위임장을 제출하셔야 합니다.

라. 개인정보 열람 및 처리정지 요구는 개인정보 보호법 제35조 제5항, 제37조 제2항에 의하여 정보주체의 권리가 제한 될 수 있습니다.

마. 개인정보의 정정 및 삭제 요구는 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없습니다.

바. 정보주체 권리에 따른 열람의 요구, 정정·삭제의 요구, 처리정지의 요구 시 열람 등 요구를 한 자가 본인이거나 정당한 대리인인지를 확인합니다.

* [개인정보 보호법 시행규칙 별지 제8호] 개인정보(열람, 정정·삭제, 처리정지) 요구서

* [개인정보 보호법 시행규칙 별지 제11호] 위임장

제7조 (개인정보의 파기) ① 수도권청은 개인정보 보유기간의 경과, 처리목적 달성 등 개인정보가 불필요하게 되었을 경우에는 지체 없이 해당 개인정보를 파기합니다.

② 정보주체로부터 동의 받은 개인정보 보유기간이 경과하거나 처리목적이 달성 되었음에도 불구하고 다른 법령에 따라 개인정보를 계속 보존하여야 하는 경우에는 해당 개인정보를 별도의 데이터베이스(DB)로 옮기거나 보관장소를 달리하여 보존합니다.

③ 개인정보 파기의 절차 및 방법은 다음과 같습니다.

1. 파기절차

파기하여야하는 개인정보(또는 개인정보파일)에 대해서는 파기계획 등을 수립하여 개인정보를 파기합니다.

가. 개인정보의 파기 : 보유기간이 경과한 개인정보는 종료일부터 지체 없이 파기 합니다.

나. 개인정보파일의 파기 : 개인정보파일의 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보파일이 불필요하게 되었을 때에는 개인정보의 처리가 불필요한 것으로 인정되는 날로부터 지체 없이 그 개인정보파일을 파기합니다.

2. 파기방법

처리하는 개인정보를 파기할 때에는 다음의 방법으로 파기 합니다.

가. 전자적 파일 형태인 경우 : 기록을 재생할 수 없는 기술적 방법 사용

나. 전자적 파일의 형태 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 파쇄 또는 소각

제8조 (개인정보의 안전성 확보 조치) 개인정보 보호법 제29조에 따라 다음과 같이 안전성 확보에 필요한 기술적, 관리적, 물리적 조치를 하고 있습니다.

1. 개인정보취급자 지정 최소화 및 교육

개인정보취급자의 지정을 최소화하고 정기적인 교육을 시행하고 있습니다.

2. 개인정보에 대한 접근 제한

개인정보를 처리하는 데이터베이스시스템에 대한 접근권한의 부여, 변경, 말소를 통하여 개인정보에 대한 접근을 통제하고, 침입차단시스템과 탐지시스템을 이용하여 외부로부터의 무단 접근을 통제하고 있으며 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하는 경우에는 정부 온라인원격근무서비스(GVPN : Government Virtual Private Network)을 이용하고 있습니다. 또한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하고 있습니다.

3. 접속기록의 보관 및 위변조 방지

개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관하고, 접속 기록이 위변조 및 도난, 분실되지 않도록 관리하고 있습니다.

4. 개인정보의 암호화

이용자의 개인정보는 암호화되어 저장 및 관리되고 있습니다. 또한 중요한 데이터는

저장 및 전송 시 암호화하여 사용하는 등의 별도 보안기능을 사용하고 있습니다.

5. 해킹 등에 대비한 기술적 대책

환경부는 해킹이나 컴퓨터 바이러스 등에 의한 개인정보 유출 및 훼손을 막기 접근이 통제된 구역에 시스템을 설치하고 기술적, 물리적으로 감시 및 차단하고 있습니다.

6. 비인가자에 대한 출입 통제

개인정보를 보관하고 있는 개인정보시스템의 물리적 보관 장소를 별도로 두고 이에 대해 출입통제 절차를 수립, 운영하고 있습니다.

제9조 (권익침해 구제방법) ① 정보주체는 아래의 기관에 대해 개인정보 침해에 대한 피해구제, 상담 등을 문의하실 수 있습니다.

1. 개인정보분쟁조정위원회(한국인터넷진흥원 운영) : (국번없이) 118번 (privacy.kisa.or.kr)
2. 개인정보침해신고센터(한국인터넷진흥원 운영) : (국번없이) 118번 (privacy.kisa.or.kr)
3. 대검찰청 사이버범죄수사단 : 02-3480-3582 (http://www.spo.go.kr)
4. 경찰청 사이버테러대응센터 : 1566-0112 (http://www.netan.go.kr)

② 개인정보 보호법 제35조(개인정보의 열람) 및 제36조(개인정보의 정정·삭제), 제37조(개인정보의 처리정지 등)의 규정에 의한 요구에 대하여 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 행정심판법이 정하는 바에 따라 행정심판을 청구할 수 있습니다.

제10조 (개인정보 보호책임자) ① 개인정보를 보호하고 개인정보와 관련된 사항을 처리하기 위하여 아래와 같이 개인정보 보호책임자 및 담당자를 지정하고 있습니다.

구 분	부서명	직위	성명	연락처
개인정보 보호책임자	기획과	과장	안승호	031-481-1305
개인정보 보호담당자	기획과	주무관	공지선	031-481-1313
개인정보 취급자	기획과	주무관	안재현	031-481-1314
	자동차관리과	주무관	박철영	031-481-1369
	자동차관리과	주무관	김누리	031-481-1389
	자동차관리과	주무관	박은주	031-481-1370

② 정보주체께서는 서비스를 이용하시면서 발생한 모든 개인정보 보호 관련 문의,

불만처리, 피해구제 등에 관한 사항을 개인정보 보호담당 부서로 문의하실 수 있습니다. 환경부는 정보주체의 문의에 대해 빠른 시일 내에 답변 및 처리해 드릴 것입니다.

	부서명	성명	연락처
개인정보 보호담당 부서	기획과	공지선	Tel : 031-481-1313 E-mail : jisun7@korea.kr

제11조 (개인정보의 처리방침의 변경) ① 이 개인정보처리방침은 2017년 11월 20일부터 적용됩니다.

② 이전의 개인정보처리방침은 수도권대기청 홈페이지에서 확인할 수 있습니다.

- 적용기간 : 2017.11.20. ~ 2018.11.19.

※ 필요시 기간 중 변경가능

영상정보처리기기 운영·관리방침

수도권대기환경청(이하 '수도권청'이라 함)은 영상정보처리기기 운영·관리 방침을 통해 처리하는 영상정보가 어떠한 용도와 방식으로 이용·관리되고 있는지 알려드립니다.

1. 영상정보처리기기의 설치 근거 및 목적

- 수도권청은 **개인정보 보호법 제25조 제1항**에 따라 다음과 같은 목적으로 영상정보처리기기를 설치·운영 합니다.
 - 시설안전 및 화재 예방
 - 민원인의 안전을 위한 범죄 예방
 - 차량도난 및 파손방지

2. 설치 대수, 설치 위치 및 촬영범위

설치 대수	설치 위치 및 촬영 범위
8대	정문, 현관, 서측 출입문, 동측 출입문, 별관 주차장, 본관 주차장, 본관 뒤, 지하실입구

3. 관리책임·담당자 및 접근 권한자

- 귀하의 영상정보를 보호하고 개인영상정보와 관련한 불만을 처리하기 위하여 아래와 같이 개인영상정보 보호책임자를 두고 있습니다.

구분	소속	직위	성명	연락처
관리 책임자	기획과	운영기획담당관	박승호	031-481-1311
관리 담당자	기획과	서무 담당자	공지선	031-481-1313
접근 권한자	기획과	복무 담당자	안재현	031-481-1314
접근 권한자	기획과	방호 담당자	장현섭	031-481-1318

4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법

촬영시간	보관기간	보관장소
24시간	촬영일로부터 7일간(7대) 촬영일로부터 6개월(1대)	당직실

- 처리방법 : 개인영상정보의 목적외 이용, 제3자 제공, 파기, 열람 등 요구에 관한 사항을 기록·관리하고, 보관기간 만료시 복원이 불가능한 방법으로 **영구 삭제**(출력물은 파쇄) 합니다.
- 보관장소 출입통제 : 잠금장치를 하여 접근권한이 부여된 자 외에는 출입을 엄격히 통제하고 있습니다.

5. 개인영상정보의 확인 방법 및 장소에 관한 사항

- 확인 방법 : 영상정보 관리책임자 및 접근 권한자에게 미리 연락하고 수도권청관을 방문하시면 확인 가능합니다.
- 확인 장소 : 기획과

6. 정보주체의 영상정보 열람 등 요구에 대한 조치

- 귀하는 개인영상정보에 관하여 열람 또는 존재확인·삭제를 원하는 경우 언제든지 영상정보처리기기 운영자에게 요구하실 수 있습니다.
 - 단, 귀하가 촬영된 개인영상정보 및 명백히 정보주체의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 개인영상정보에 한정됩니다.
- 수도권청은 개인영상정보에 관하여 열람 또는 존재확인·삭제를 요구한 경우 지체 없이 필요한 조치를 하겠습니다.

○ 다음의 경우에는 정보주체의 개인영상정보 열람 등 요구를 거부할 수 있습니다. 이 경우 관리책임자는 10일 이내에 서면 등으로 거부 사유를 정보주체에게 통지합니다.

- 범죄수사·공소유지·재판수행에 중대한 지장을 초래하는 경우
- 개인영상정보의 보관기간이 경과하여 파기한 경우
- 열람 요구에 대하여 필요한 조치를 취함으로써 타인의 사생활권이 침해될 우려가 큰 경우
- 기타 정보주체의 열람 등 요구를 거부할 만한 정당한 사유가 존재하는 경우

7. 영상정보의 안전성 확보조치

○ 수도권청에서 처리하는 영상정보는 암호화 조치 등을 통하여 안전하게 관리되고 있습니다.

- 개인정보에 대한 접근 권한을 차등부여
- 개인영상정보의 위·변조 방지를 위해 개인영상정보의 생성 일시, 열람시 열람 목적·열람자·열람 일시 등을 기록·관리
- 개인영상정보의 안전한 물리적 보관을 위하여 잠금장치 설치

8. 개인정보 처리방침 변경에 관한 사항

○ 이 영상정보처리기기 운영·관리방침은 2017년 6월 14일에 개정되었으며 법령·정책 또는 보안기술의 변경에 따라 내용의 추가·삭제 및 수정이 있을 시에는 시행하기 최소 7일전에 수도권청 홈페이지를 통해 변경사유 및 내용 등을 공지하도록 하겠습니다.

- 적용기간 : 2017년 6월 14일 ~ 2018년 6월 13일

[붙임 9]

재해·재난 대비 개인정보처리시스템 위기대응 매뉴얼 (절차서)

2017. 11.

수도권대기환경청

목 차

I. 개 요	1
1. 관련 법률	1
2. 관리 범위	1
3. 용어 정의	1
라. 대표적 개인정보 침해 유형	2
마. 개인정보 침해사고 유형	5
II. 위기대응 절차	6
1. 절차 개요	6
2. 단계별 정의	7
III. 위기대응 체계	12
1. 위기대응 조직의 구성	12
2. 위기등급 분류	22
3. 복구목표 설정	23
4. 백업 관리	23
5. 위기대응 훈련	23
6. 비상연락망 구성	23
[붙임 1] 개인정보처리시스템 구성 현황	29
[붙임 2] 백업 관리대장	33
[붙임 3] 비상 연락망	35

- 최근 지진, 화재 등 재해·재난 대응의 중요성이 높아짐에 따라 개인정보처리시스템 보호를 위한 위기대응 체계 수립
- 재해·재난 발생 시 개인정보처리시스템의 신속한 복구와 원활한 업무 처리의 재개를 위해 관련 절차 등의 대책 지원

I 개 요

1. 관련 법률

- 개인정보보호법 제29조, 시행령 제30조, 개인정보의 안전성확보 조치 고시 제12조 1항

2. 관리 범위

- 본 매뉴얼에서 정의한 재해·재난 발생 시 개인정보처리시스템의 운영 및 관리에 한하여 적용
- 개인정보처리시스템 위기 상황 해제 시 까지 개인정보처리시스템의 운영에 필요한 모든 행동요령을 포함
 - ※ 본 내용은 개인정보 처리시스템을 개별 운영할 경우 참고하도록 작성한 것으로 정부통합전산센터를 통해 개인정보 처리시스템을 운영할 경우 정부통합전산센터의 대응 절차 및 매뉴얼을 따름

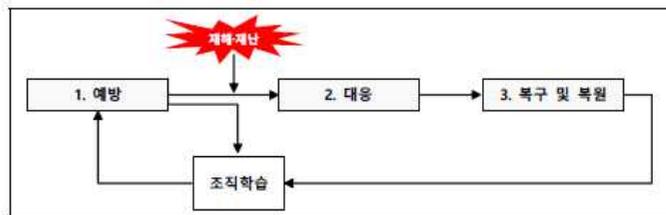
3. 용어 정의

- 재해·재난 : 태풍, 홍수, 지진, 낙뢰 등 이상적인 자연현상 또는 붕괴, 폭발 등으로 사회적 혼란을 유발할 수 있는 사고
- 개인정보처리시스템 위기 : 개인정보처리시스템이 장애로 인해 가동이 전면 중단되거나 중단 가능한 시간을 초과하는 경우
- 재해복구시스템 : 재해·재난 발생 시 데이터를 보존하고 자동 복구하는 장치
- 백업 : 잘못되거나 부주의한 조작으로 인하여 데이터가 손실될 것에 대비하여 미리 남겨둔 복사본

II 위기대응 절차

1. 절차 개요

- 개인정보처리시스템의 위기 발생 시 예방, 대응, 복구 및 복원으로 이루어지는 3가지 단계를 체계적으로 구조화해야 함



▲ 위기대응 절차 예시

2. 단계별 정의

- 1단계 : 예방
 - 위기상황이 발생하기 전 예상되는 문제들을 미리 보완하고 대비
 - 위기대응 조직, 위기등급, 복구목표 등 위기대응 체계 검토
 - 주기적 백업 실시 및 위기대응 훈련 실시를 통해 위기대응 준비
- 2단계 : 대응
 - 재해·재난으로 위기상황이 발생하여 위기대응 체계에 따라 대응 실시
 - 위기대응 조직을 소집하고 위기등급을 정의하여 위기상황 선포
 - 비상연락체계를 가동하고 위기대응 조직의 역할에 따라 대응 실시
- 3단계 : 복구 및 복원
 - 복구목표에 따라 우선순위가 높은 업무부터 복구 및 복원 실시
 - 복구 및 복원이 완료되면 위기상황의 종료를 선언하고 위기대응 시 이슈사항을 위기대응 체계에 반영하여 개선
 - 위기상황으로 인한 피해를 수습하고 위기내용 학습

III 위기대응 체계

1. 위기대응 조직의 구성

○ 업무분장 및 임무 및 역할

구 분	역 할
개인정보처리시스템 책임자	- 위기대응 업무의 총괄 - 위기선포 및 위기대응 조직 구성원에게 업무를 지시 - 위기대응 상황 종료 시 결과를 공유
개인정보처리시스템 담당자	- 위기상황 발생 시 각 업무기능의 복구 총괄 - 책임자의 위기선포에 따라 위기상황 전파 - 유관기관과 연락망 가동 및 정보공유
기술 담당자	- 평상 시 위기대응 절차 및 계획의 검토 - 개인정보시스템의 기술적 복구 및 운용 담당 - 책임자 및 담당자 지시에 따라 필요한 활동 지원

○ 위기대응 조직 및 비상연락망

구 분	담당부서	구 성 인 원
개인정보 보호책임자		• 기획과장(☎ 031-481-1305)
개인정보처리시스템 담당자	기획과	- 개인정보보호 담당자(☎ 031-481-1313) - 개인정보취급자(☎ 031-481-1314)
	자동차관리과	- 개인정보취급자(☎ 031-481-1389, 369, 370)
	환경부 정보화담당관실	- 개인정보보호 담당자(☎ 044-201-6411) - 정보보안담당자(☎ 044-201-6415-6) - 사이버안전센터(☎ 044-201-6450)

2. 위기등급 분류

○ 위기 등급 분류

구분	역 할
1등급	- 개인정보처리시스템 장애시간이 24시간 이상 지속되는 경우 - 개인정보처리시스템 운용의 전면 중단 - 데이터의 중대하 손상으로 복구 불가 - 개인정보처리시스템 장비의 전원공급 단절
2등급	- 개인정보처리시스템 장애시간이 24시간 이하로 지속되는 경우 - 개인정보처리시스템 운용 시 일부 기능 작동 중단 - 데이터의 일부 손상으로 복구 필요 - 개인정보처리시스템 장비의 전원공급 이상
3등급	- 개인정보처리시스템 장애가 일시적으로 발생한 경우 - 개인정보처리시스템의 운용이 일시적 작동 중단 - 데이터의 경미한 손상이나 운영에 지장 없음

3. 복구목표 설정

- 개인정보처리시스템의 위기 발생 시 신속한 대응 및 복구를 위한 복구목표시간(RTO) 및 복구목표시점(RPO)을 정의해야 함
- 복구목표는 개인정보처리시스템별 업무 영향도를 고려하여 우선 순위를 정해야 하며 위기선포 시부터 적용
- 복구목표시간(RTO : Recovery Time Objective)
 - 서비스 또는 사업 감내 목표를 초과하여 영향을 미치기 전 시점까지의 최고 중단 허용시간
 - 개인정보처리시스템의 책임자는 업무 영향도를 고려하여 복구목표 시간의 정의 필요
- 복구목표시점(RPO : Recovery Point Objective)
 - 업무를 계속적으로 수행하기 위해 손실된 데이터에 대한 유실 허용시점

- 복구목표시점은 재해발생 직전까지이며, 재해복구시스템이 준비되어 있지 않은 시스템은 최종 백업 시점까지

4. 백업 관리

- 개인정보처리시스템 담당자는 신속한 업무 복구를 위해 백업 대상을 선정하고 필요한 내용을 주기적으로 백업해야 함
- 백업 대상은 DB, 개발소스 및 메일 데이터, 로그, 서버 OS 그리고 기타 중요도가 높다고 판단되는 데이터를 대상으로 함
- 개인정보처리시스템 담당자는 안전한 백업매체를 선정하고 백업의 주기 및 소산 유무를 결정해야 함
- 백업매체는 비인가자가 접근할 수 없는 격리된 곳에 보관하여 비인가자에 의한 백업정보 유출이 일어나지 않도록 해야 함
- 백업매체의 물리적인 접근통제 및 백업일자 목록은 '붙임2(백업관리 대장)'에 기록하여 유지·관리해야 함

5. 위기대응 훈련

- 개인정보처리시스템의 위기가 발생하는 경우 피해를 최소화하고 신속한 복구를 위해 주기적으로 위기대응 훈련을 실시해야 함
- 위기대응 훈련은 평소 운영 중에 재해·재난 복구시스템이 정상 작동되는지 확인해야 하며 위기상황 발생 시와 동일하게 위기대응 조직의 역할을 수행해야 함
- 위기대응 훈련 시에는 다음의 사항을 유의하여 실시해야 함
 - 재난·재해 복구시스템의 정상 작동

- 위기대응 조직 구성원별 역할 숙지
- 복구목표의 달성
- 실 데이터의 안정성 보존
- 비상 연락망 정상 가동상황
- 위기대응 체계 운용 시 이슈사항

- 위기대응 훈련 종료 후 훈련 시 도출된 미흡사항 및 이슈사항을 위기대응 체계에 반영하여 개선해야 함

6. 비상연락망 구성

- 개인정보처리시스템 담당자는 위기대응 조직원, 유관기관, 관련 업체 등으로 이뤄진 비상연락망에 기록 관리해야 함
- 개인정보처리시스템 담당자는 비상연락망을 주기적으로 검토하고 평상시에도 연락체계를 활용하여 정보를 공유해야 함
- 위기상황 발생 시 위기상황 종료 시까지 비상연락망을 가동하여 신속한 대응을 지원해야 함

IV 위기대응 절차

1. 위기대응 절차도

○ 단계별 위기대응 절차

구 분	조치방법	조치사항
확인	재해·재난 인지	재해·재난 상황 파악 상황보고 및 재해·재난 상황 알림 재해·재난 대응팀 설치
	확인조사 실시	재해·재난 내용(원인, 규모 등) 세부조사
	피해확산 여부 조사	확인조사 결과 개인정보처리시스템 전면 중단 및 중단 가능성 여부 확인
조치 (복구 및 복원)	복구대상 범위 조사	피해 사항 확인 복구 목표 설정 - 복구목표시간, 복구목표시점 복구대상·범위 조정
	백업현황 확인	백업 자료 확인 복구방법 및 절차 결정
	복구	시스템 및 데이터 복구 작업
사후관리	피드백	기술적, 관리적 보완조치 매뉴얼 현행화

2. 확인

- 재해·재난 인지
 - 개인정보처리시스템의 장애 상태 파악
 - 개인정보보호책임자에게 재해·재난 발생 상황보고 및 개인정보처리 시스템 관련자에게 상황보고
- 확인조사 실시
 - 개인정보처리시스템의 장애 여부 조사
- 피해확산 여부 조사
 - 재해·재난의 범위에 따라 피해가 언제까지 계속되는지 조사

3. 조치(복구 및 복원)

- 복구대상 범위 조사
 - 기존 시스템의 피해 상태 확인
 - 복구 목표 설정(복구목표 시간, 복구목표시점)
 - 업무 영향도를 고려하여 우선 순위 등 복구 대상·범위 조정
- 백업현황 확인
 - 백업 관리대장에서 백업내용 확인
- 복구
 - 기존 시스템과 백업 관리대장에 따라 복구 스케줄 작성
 - 정보시스템별 장애 복구 절차에 따라 시스템 복구

4. 사후관리

- 피드백
 - 위기대응 훈련, 복구 완료 후 보완사항을 절차서에 반영하여 단계 별 대응역량 강화

