

[제·개정 이력]

순 번	버전	구 분	시행 일자	제정 · 개정 주요내용
1	1.0	제정	2023.02	1. 최초 작성
2	2.0	개정	2024.03.	1. 일부 개정 (KISA 표준안에 따라 조항 정리 및 자구 수정)

한국뇌연구원 개인정보보호 내부 관리계획

2024. 3.

## 목 차

<b>목 차</b>	
제1장 총 칙 .....	1
1. (목적)	
2. (용어 정의)	
3. (적용 범위)	
제2장 내부 관리계획의 수립 및 시행 .....	3
1. (내부 관리계획의 수립 및 승인)	
2. (내부 관리계획의 공표)	
제3장 개인정보 보호책임자의 역할 및 책임 .....	4
1. (개인정보 보호책임자의 지정)	
2. (개인정보 보호담당자 지정)	
3. (개인정보 취급자 지정)	
제4장 개인정보 보호 교육 .....	6
1. (개인정보 보호책임자의 교육)	
2. (개인정보취급자의 교육)	
제5장 기술적 안전조치 .....	6
1. (접근 권한의 관리)	
2. (접근 통제)	
3. (개인정보의 암호화)	
4. (접속기록의 보관 및 점검)	
5. (악성프로그램 등 방지)	
6. (관리용 단말기의 안전조치)	
제6장 관리적 안전조치 .....	11
1. (개인정보 보호조직 구성 및 운영)	
2. (개인정보 유출 사고 대응)	
3. (위험도 분석 및 대응)	
4. (수탁자에 대한 관리 및 감독)	
제7장 물리적 안전조치 .....	12
1. (물리적 안전조치)	
2. (재해 및 재난 대비 안전조치)	
3. (개인정보의 파기)	
제8장 내부 관리계획의 관리 .....	13

본 내부 관리계획은 개인정보처리자가 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전 조치에 관한 사항 등을 규정한 계획, 규정, 지침 등을 말함

— 총 칙 —

## 1 목적

- 한국여연구원 개인정보 내부 관리계획은 「개인정보 보호법」 제29조와 같은 법 시행령 제30조 그리고 ‘개인정보의 안전성 확보 조치 기준’ (제2016-35호)에 따라 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 사항을 정하는 것을 목적으로 한다. <개정 2024.03.>

## 2 용어 정의

**제2조(용어 정의)** 개인정보 내부 관리계획에서 사용하는 용어의 뜻은 다음과 같다.

1. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
2. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
3. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
4. “대기업”이란 「독점규제 및 공정거래에 관한 법률」 제14조에 따라 공정거래위원회가 지정한 기업집단을 말한다.
5. “중견기업”이란 「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」 제2조에 해당하는 기업을 말한다.
6. “중소기업”이란 「중소기업기본법」 제2조 및 동법 시행령 제3조에 해당하는 기업을 말한다.
7. “소상공인”이란 「소상공인 보호 및 지원에 관한 법률」 제2조에 해당하는 자를 말한다.
8. “개인정보 보호책임자”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.
9. “개인정보취급자”란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는

- 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
10. “개인정보처리시스템”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성된 시스템을 말한다.
  11. “위험도 분석”이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.
  12. “비밀번호”란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
  13. “정보통신망”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
  14. “공개된 무선망”이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
  15. “모바일 기기”란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
  16. “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
  17. “보조저장매체”란 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(DigitalVersatile Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.
  18. “내부망”이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
  19. “접속기록”이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신 가능한 상태를 말한다.
  20. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.
  21. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

### ③ 적용 범위

- 한국뇌연구원이 개인정보를 처리하거나 한국뇌연구원의 개인정보 처리 업무를 위탁받아 처리하는 수탁자에게는 본 개인정보 내부관리계획이 적용된다. <개정 2024.03.>

## II 내부 관리 계획의 수립 및 시행

### ① 내부 관리계획의 수립 및 승인

- 개인정보 보호담당자는 개인정보의 안전한 처리를 위하여 개인정보를 관련한 법령 및 관련 규정을 준수하도록 다음 사항을 포함하여 내부 관리 계획을 수립하여야 합니다. <개정 2024.03.>
  - 개인정보 보호책임자의 지정에 관한 사항
  - 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
  - 개인정보 안정성 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

### ② 내부 관리계획의 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 : 우리원 전체
  - 공지방법 : (내부) 전체공지, (외부) 홈페이지
  - 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

### III 개인정보 보호책임자의 역할 및 책임

#### ① 개인정보 보호책임자 지정 <신설 2024.03.>

- 한국뇌연구원은 「개인정보 보호법」 제31조와 같은 법 시행령 제32조에 따라 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 경영기획실장으로 정한다.
- 개인정보 보호책임자의 임무
  - 개인정보 보호 계획의 수립 및 시행
  - 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
  - 개인정보 처리와 관련한 불만의 처리 및 피해 구제
  - 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
  - 개인정보 보호 교육 계획의 수립 및 시행
  - 개인정보파일의 보호 및 관리·감독
  - 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행

- 개인정보 보호 관련 자료의 관리
- 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기
- 그 밖에 개인정보의 보호를 위해 필요하다고 인정되는 사항

#### ② 개인정보 보호담당자 지정

- 개인정보 보호책임자 또는 분야별책임자는 개인정보보호와 관련된 업무를 처리하기 위하여 개인정보 보호담당자를 지정할 수 있다. <개정 2024.03.>
- 개인정보 보호담당자의 임무
  - 개인정보 보호계획 및 방침 운영
  - 개인정보 침해대응
  - 개인정보 처리실태 관리 및 각종 자료 취합
  - 개인정보 보호법 관련 업무전반
  - 개인정보 보호책임자가 위임한 개인정보보호와 관련된 업무

#### ③ 개인정보 취급자 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

## IV 개인정보 보호 교육

### ① 개인정보 보호책임자의 교육

- 개인정보 보호책임자를 대상으로 연 2회 이상 개인정보 보호와 관련된 교육을 실시한다.

### ② 개인정보취급자의 교육

- 개인정보 보호책임자는 개인정보의 적절한 취급을 보장하기 위하여 다음 각 호의 사항을 정하여 개인정보취급자에게 필요한 개인정보보호 교육 계획을 수립하고 실시하여야 한다.
  - 교육 목적 및 대상
  - 교육 내용
  - 교육 일정 및 방법
- 개인정보보호 교육을 실시한 결과 또는 이를 입증할 수 있는 관련 자료 등을 기록·보관하여야 한다.

## V 기술적 안전조치

### ① 접근 권한의 권리

- 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.
- 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

- 개인정보처리자는 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.
- 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 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.
- 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.
- 개인정보처리자는 개인정보처리시스템에 대하여 다음 각 호의 내용이 포함된 권한관리지침을 수립하여 운영하여야 한다.
  1. 권한에 대한 총괄 관리책임자 지정에 관한 사항
  2. 사용자 등록, 권한 부여·변경·중지 등에 관한 사항
  3. 사용자 및 정보 중요도별 접근권한 차등 부여에 관한 사항
  4. 외부인력 및 업무보조자의 권한 관리에 관한 사항
  5. 접근권한 관리이력 보관에 관한 사항
  6. 보안서약서 징구 등에 관한 사항

### ② 접근 통제

- 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한

2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응

※ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 않고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 적용하지 않을 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근 통제 기능을 이용할 수 있음

○ 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

○ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.

○ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.

○ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.

○ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

### ③ 개인정보의 암호화

○ 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

○ 개인정보처리자는 비밀번호 및 바이오정보를 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 않도록 일방향 암호화하여 저장하여야 한다.

○ 개인정보처리자가 인터넷 구간 및 인터넷 구간과 내부망의 중간지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

○ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 개인정보 영향평가의 결과를 고려하여 암호화의 적용여부 및 적용범위를 정할 수 있다.

○ 개인정보처리자는 개인정보를 암호화하는 경우 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

○ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

※ 「개인정보의 안전성 확보조치 기준 고시」 별표의 유형2의 적용대상에 해당하는 각 기관의 개인정보처리자는 위의 조치를 하지 아니할 수 있음

### ④ 접속기록의 보관 및 점검

○ 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관·관리하여야 한다.

○ 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는

훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을  
반기별로 1회 이상 점검하여야 한다.

- 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

## 5 악성프로그램 등 방지

- 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.
  1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
  2. 악성 프로그램 관련 정보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시
  3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

## 6 관리용 단말기의 안전조치

- 개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.
  1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
  2. 본래 목적 외로 사용되지 않도록 조치
  3. 악성프로그램 감염 방지 등을 위한 보안조치 적용

# VI 관리적 안전조치

## 1 개인정보 보호조직 구성 및 운영

- 개인정보 보호 담당자는 개인정보의 안전한 처리를 위하여 다음 각 호의 사항을 포함하는 개인정보 보호 조직을 구성하고 운영하여야 한다.
  1. 개인정보 보호책임자의 지정
  2. 개인정보 보호책임자의 지휘·감독 하에 개인정보 보호책임자의 업무를 지원하는 담당자의 지정
  3. 개인정보를 처리하는 개인정보취급부서의 지정

## 2 개인정보 유출 사고 대응

- 개인정보보호 책임자는 개인정보 유출 사고 발생 시 피해를 최소화하기 위하여 「개인정보 침해사고 대응절차서」를 마련하고 시행하여야 한다. <개정 2024.03.>

## 3 위험도 분석 및 대응

- 개인정보보호 책임자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 위험도 분석을 수행하고 필요한 보안조치 적용 등 대응방안을 마련하여야 한다.

## 4 수탁사에 대한 관리 및 감독

- 개인정보보호 책임자는 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 사항을 정하여 수탁자를 교육하고 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.
  1. 교육 및 감독 대상
  2. 교육 및 감독 내용
  3. 교육 및 감독 일정, 방법

## VII 물리적 안전조치

### 1 물리적 안전조치

- 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.
- 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.
- 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입통제를 위한 보안대책을 마련하여야 한다.

※ 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 위의 사항을 적용하지 않을 수 있음

### 2 재해 및 재난 대비 안전조치 <개정 2024.03.>

- 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.
- 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

### 3 개인정보의 파기

- 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.
  1. 완전파괴(소각·파쇄 등)
  2. 전용 소자장비를 이용하여 삭제
  3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

- 개인정보처리자는 개인정보의 일부만을 파기하는 경우, **위의 방법으로** 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다. <개정 2024.03.>

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

## VIII 내부 관리계획의 관리

- 책임자는 내부 관리계획의 이행 실태를 연 1회 이상 점검·관리하여야 한다.