믿을 수 있는 개인정보 활용, 신뢰사회의 기본입니다.

Privacy by Trust, Trust by Privacy

2017년

# 개인정보 보호법 주요내용

행정안전부 | KISA 한국인터넷진흥원

# Contents

# I 개 요

# 개인정보 보호법 주요내용

## 개인정보 보호 원칙 및 정책

- 개인정보보호 원칙
- 정보주체의 권리
- 개인정보보호 정책 추진체계

## 개인정보의 처리 단계별 의무

- 개인정보 처리단계별 규정
  - 개인정보 수집, 이용, 제공, 파기 단계별 준수해야 할 사항
- 개인정보 처리제한
  - 주민등록번호, 민감정보 처리 제한

## 개인정보의 안전한 관리

- 안전조치 의무
  - 관리적, 기술적, 물리적 보호조치
- 보호책임자 지정, 처리방침 공개
- 유출 시 조치 해야 할 사항
  - 통지 및 신고, 대책 수립 및 시행

## 권리 보장 및 구제

- 정보주체의 권리 보장
  - 열람, 정정, 삭제, 처리 정지, 손해배상 등
- 개인정보 분쟁조정
  - 조정의 신청, 절차 등
- 단체소송
  - 단체소송 대상, 절차 등

# 개인정보 보호 관련 법률간 관계

개인정보 보호법은 개인정보 보호 분야의 **일반법**

**타 법률에 특별한 규정이 없는 경우**

**개인정보 보호법 적용**

- 사회전반의 개인정보 보호를 규율
- 모든 사업자, 개인 등

**타 법률에 특별한 규정이 있는 경우**

**해당 법률 규정 적용**

- 정보통신망법
- 신용정보법, 전자금융거래법
- 의료법, 고등교육법 등

# 개인정보 보호 환경

## 유출, 침해의 초 대량화

개인정보 대량집적 추세
→ 유출사고 초 대량화 (1~2천만건)

**전국민의 개인정보가 유출 위험**

## 개인정보 취급분야 확대

(기존)정보통신업 + { 기타 사업분야 / 비영리단체 등

**다양한 분야에서 문제 발생 가능**

## 새로운 기술 환경

스마트폰, 클라우드 컴퓨팅,
CCTV, AI, 빅데이터 등

**새로운 기술에 기반한**
**개인정보보호 이슈 발생**

## 정보 주체의 인식 변화

집단소송, 분쟁조정, 침해신고 등
개인정보 침해에 적극적 대응

**정보주체의 권리보장 강화**

# Ⅱ 총 칙

# 개인정보 정의

**특정 개인을 식별**할 수 있는 정보

예) 주민번호, 영상정보, 문자, 음성 등

**다른 정보와 결합**하여
개인을 식별할 수 있는 정보

예) 이름 + 전화번호
이름 + e-mail
전화번호 + e-mail
{ 홍길동 + 010-XXXX-0000

**성명, 전화번호, 주소**는 다른 정보와 쉽게 결합하여 개인을 식별할 수 있는 정보로서 **개인정보 보호법상 개인정보이다.**

# 개인정보의 종류

**일반적 정보**
- 주민등록번호
- 이름, 주소

**통신•위치 정보**
- 통화, I P주소
- G P S 등

**사회적 정보**
- 교육 정보
- 근로 정보
- 자격 정보

**정신적 정보**
- 기호, 성향
- 신념, 사상

**신체적 정보**
- 신체정보
- 의료, 건강정보

**재산적 정보**
- 개인 금융정보
- 개인 신용정보

**다른 정보와 쉽게 결합하여 개인을 식별할 수 있는 정보는 점점 확대되는 추세!**

# [참고] 일상생활에서의 개인정보 활용

# [참고] 일상생활에서의 개인정보 활용

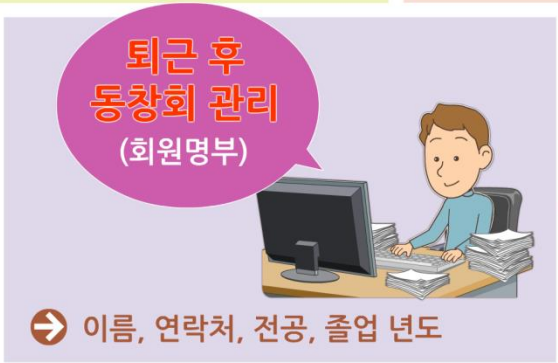
하루 동안 홍길동씨의 개인정보는 어떻게 활용될까?


ID, PW, 이름, 계좌


ID, 신용카드, 주소, 연락처


건강보험번호, 이름, 병명, 진료기록


이름, 동 · 호수, 연락처




이름, 연락처, 전공, 졸업 년도

# [참고] 용어 정리

| | |
|---|---|
| **개인정보** | • 성명, 주민번호 등을 통하여 살아있는 개인을 알아볼 수 있는 정보<br>• 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 정보<br>**※ 개인정보 보호법은 정보통신망법과는 달리 이용자뿐 아니라 임직원, 주주, 협력업체 등 모든 사람의 개인정보에 적용됨** |
| **처리** | • 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 행위 |
| **정보주체** | • 처리되는 정보에 의해 알아볼 수 있는 그 정보의 주체가 되는 사람 |
| **개인정보 파일** | • 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物) |
| **개인정보 처리자** | • 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체, 개인 등 |
| **공공기관** | • 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관,<br>• 중앙행정기관( 대통령 소속 기관과 국무총리 소속 기관 포함) 및 그 소속 기관, 지방자치단체.<br>• 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관<br>- 국가인권위원회, 공공기관 운영에 관한 법률에 따른 공공기관, 지방공사, 지방공기업<br>- 특별법에 따른 특수법인, 초등교육법이나 고등교육법에 따른 각급 학교 |

# [참고] 용어 정리

| | |
|---|---|
| 개인정보보호 책임자 | • 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자 |
| 개인정보 취급자 | • 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등 |
| 개인정보 처리시스템 | • 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 응용시스템 |
| 접속기록 | • 개인정보취급자 등이 개인정보처리시스템에 접속한 사실을 알 수 있는 계정, 접속일시, 접속자 정보, 수행업무 등을 전자적으로 기록한 것.<br>* "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말함 |
| 영상정보처리기기 | • 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치 |
| 개인영상정보 | • 영상정보처리기기에 의하여 촬영·처리되는 영상정보 중 개인의 초상, 행동 등과 관련된 영상정보로서 해당 개인을 식별할 수 있는 정보 |
| 공개된 장소 | • 공원, 도로, 지하철, 상가 내부, 주차장 등 불특정 또는 다수가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소 |

# 개인정보 보호 원칙 (제3조)

1. **처리 목적의 명확화**, 목적 내에서 **적법하고 정당하게 최소 수집**
2. 처리 목적 내에서 처리, **목적 외 활용 금지**
3. 처리 목적 내에서 **정확성·완전성·최신성** 보장
4. 정보주체의 권리침해 위험성 등을 고려하여 **안전하게 관리**
5. 개인정보 처리사항 공개, **정보주체의 권리보장**
6. **사생활 침해 최소화** 방법으로 처리
7. 가능한 경우 **익명 처리**
8. 개인정보처리자의 **책임 준수**, 정보주체의 **신뢰성 확보**

# 정보주체의 권리 (제4조)

1. 개인정보의 처리에 관한 정보를 **제공받을 권리**

2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 **선택, 결정할 권리**

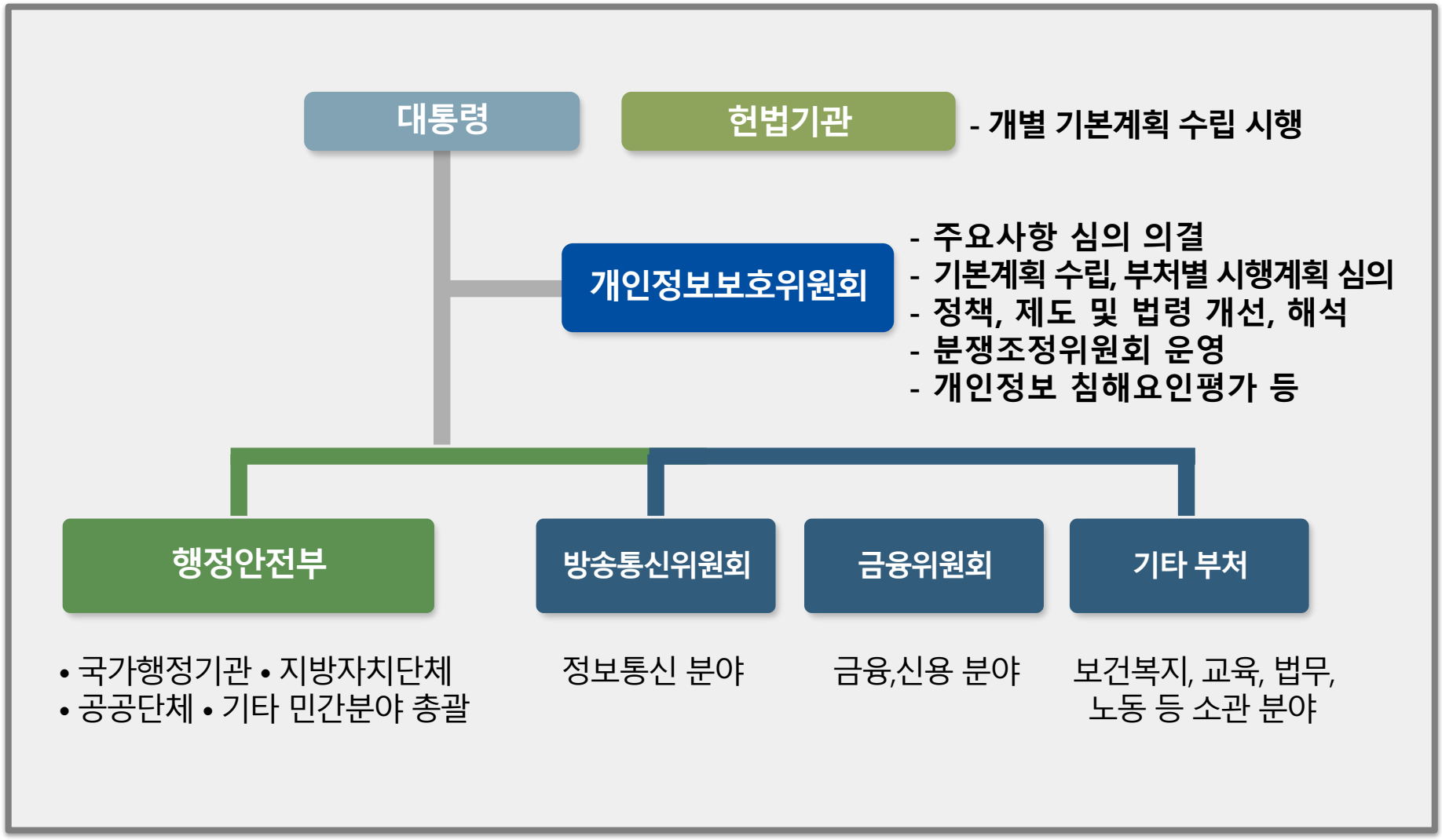
3. 개인정보의 처리 여부 확인, 개인정보 **열람을 요구할 권리**

   (사본의 발급 포함)

4. 개인정보의 **처리 정지, 정정·삭제 및 파기를 요구할 권리**

5. 개인정보의 처리 **피해를 신속, 공정하게 구제받을 권리**

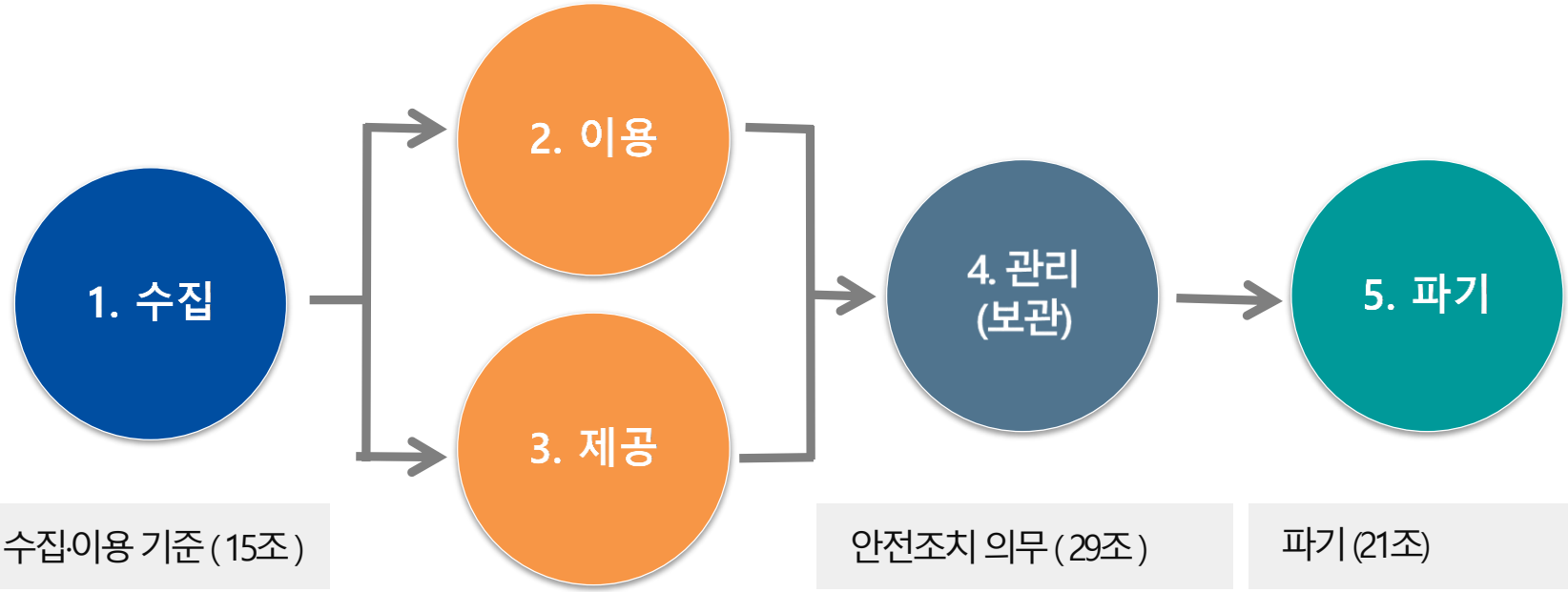
# 개인정보 보호 추진체계


대통령
헌법기관
- 개별 기본계획 수립 시행
개인정보보호위원회
- 주요사항 심의 의결
- 기본계획 수립, 부처별 시행계획 심의
- 정책, 제도 및 법령 개선, 해석
- 분쟁조정위원회 운영
- 개인정보 침해요인평가 등
행정안전부
방송통신위원회
금융위원회
기타 부처
• 국가행정기관 • 지방자치단체
• 공공단체 • 기타 민간분야 총괄
정보통신 분야
금융,신용 분야
보건복지, 교육, 법무,
노동 등 소관 분야

# Ⅲ 개인정보의 처리

(개인정보 보호법 제 3장)

# 개인정보 처리단계별 보호조치




- 수집·이용 기준 (15조)
- 최소 수집 (16조)
- 14세 미만 법정 대리인 동의 (22조)
- - 처리제한 - 민감정보 (23조), 고유식별정보 (24조) 주민번호 (24조의 2)

- 목적외 이용·제공 제한 (18조)
- 제3자 제공 (17조)
- 처리위탁 (26조)
- 영업양도양수(27조) (민간)
- 국외이전(17조)

- 안전조치 의무 (29조)
- 처리방침 (30조) 보호책임자 (31조)
- 개인정보 유출 통지·신고 (34조)
- 개인정보파일 등록 (32조) (공공기관)

- 파기 (21조)

# 개인정보 수집·이용·제 3자 제공

**개인정보 수집·이용**
(법 제15조)

목적 내 제3자 제공

목적 외 이용 ·제공

※ 민감정보, 고유식별정보는 제15조, 제17조, 제18조 해당 없음!

1. 정보주체의 **동의**를 받은 경우

**※ 동의 받을 때 고지 의무 사항**

① 수집·이용 목적
② 수집 항목
③ 보유·이용 기간
④ 동의거부 권리 및 동의거부 시 불이익 내용

2. **법률의 특별한 규정, 법령상 의무 준수**를 위해 불가피한 경우
3. 공공기관이 법령 등에서 정한 소관업무를 위해 불가피한 경우
4. **정보주체와의 계약 체결이행에 불가피한 경우**
5. 정보주체 등의 급박한 생명, 신체, 재산의 이익 보호
6. **개인정보처리자의 정당한 이익 달성을 위해 필요한 경우**

**위반 시 → 5천만원 이하의 과태료**

# 개인정보 수집·이용·제 3자 제공

개인정보 수입·이용 | **목적 내 제 3자 제공** (법 제17조) | 목적 외 이용 ·제공

※민감정보, 고유식별정보는 제15조, 제17조, 제18조 해당 없음!

1. 정보주체의 동의를 받은 경우

**※ 동의 받을 때 고지의무 사항**

① 개인정보를 **제공받는 자**
② 제공받는 자의 개인정보 **이용 목적**
③ 제공하는 개인정보의 **항목**
④ 제공받는 자의 개인정보 **보유·이용기간**
⑤ **동의거부 권리** 및 **동의거부 시 불이익** 내용

2. 법률의 특별한 규정, 법령상 의무 준수를 위해 불가피한 경우
3. 공공기관이 법령 등에서 정한 소관업무를 위해 불가피한 경우
4. 정보주체 등의 급박한 생명, 신체, 재산의 이익 보호

**위반 시 → 5년 이하의 징역 또는 5천만원 이하의 벌금**

# 개인정보 수집·이용·제 3자 제공

개인정보 수입·이용 | 목적 내 제 3자 제공 | **목적 외 이용·제공** (법 제18조)

※민감정보, 고유식별정보는 제15조, 제17조, 제18조 해당 없음!

**목적외 이용·제공은 원칙적으로 금지, 다만 정보주체 또는 제3자의 이익을 부당하게 침해할 우려 가 없는 경우 예외적 허용**

1. 정보주체의  별도 동의를 받은 경우
2. 다른 법률의 특별한 규정
3. 명백히 정보주체 또는 제3자의 생명, 신체, 재산의 이익에 필요한 경우
4. 통계작성 및 학술연구 목적에 필요한 경우로 특정개인을 알아볼 수 없는 형태로 제공하는 경우

**공공기관만 해당**

5. 개인정보를 목적 외로 이용하거나 제3자에게 제공하지 않으면 다른 법률에서 정하는 소관업무 수행 불가한 경우로 개인정보 보호위원회의 심의·의결을 거친 경우
6. 조약, 국제협정 이행을 위해 외국정부 등 제공에 필요한 경우
7. 범죄수사 및 공소제기·유지
8. 법원의 재판업무 수행
9. 형 및 감호, 보호처분 집행

**위반 시 → 5년 이하의 징역 또는 5천만원 이하의 벌금**

# [참고] 목적 외 제 3자 제공 요구 법률 규정 예시

| | |
|---|---|
| 고엽제후유의증 등 환자지원 및 단체설립에 관한 법률 | **제7조(고엽제후유의증환자 등에 대한 진료 등)**<br>③ 다음 각 호의 어느 하나에 해당하는 의료기관의 장은 그 진료과정에서 해당 환자가 고엽제후유증환자·고엽제후유의증환자 또는 고엽제후유증 2세환자로 판단되면 대통령령으로 정하는 바에 따라 지체 없이 진료기록 및 임상소견서(임상소견서)를 보훈병원장에게 보내야 한다. |
| 감염병의 예방 및 관리에 관한 법률 | **제11조(의사 등의 신고)**<br>① 의사나 한의사는 다음 각 호의 어느 하나에 해당하는 사실(제16조제5항에 따라 표본감시 대상이 되는 감염병으로 인한 경우는 제외한다)이 있으면 소속 의료기관의 장에게 보고하여야 하고, 해당 환자와 그 동거인에게 보건복지부장관이 정하는 감염 방지 방법 등을 지도하여야 한다. 다만, 의료기관에 소속되지 아니한 의사 또는 한의사는 그 사실을 관할 보건소장에게 신고하여야 한다.<br>(각 호 생략)<br>② 제1항에 따라 보고를 받은 의료기관의 장은 제1군감염병부터 제4군감염병까지의 경우에는 지체 없이, 제5군감염병 및 지정감염병의 경우에는 7일 이내에 관할 보건소장에게 신고하여야 한다. |

# 목적 외 이용 • 제공(제18조)에 따른 이행사항

| 제공자 | 요청 | 제공 받는 자 |
| --- | --- | --- |
| 개인정보를 제공받는 자에게 이용목적, 이용방법 그 외 필요 사항에 대한 제한 및 개인정보 안전성 확보 조치 마련 요청 | ▶ | 개인정보 안전성 확보 조치 이행 |

## 공공기관 이행사항

- 개인정보 이용 및 제공 관련 법적 근거, 목적 및 범위 관련 사항을 관보 또는 인터넷 홈페이지 게재
- 개인정보 목적 외 이용 및 제3자 제공 대장 기록 관리

# [참고] 목적 외 이용 및 제3자 제공 대장

■ 개인정보 보호법 시행규칙 제3조 [별지 제1호서식]

| | | | |
|---|---|---|---|
| 개인정보 또는 개인정보파일 명칭 | | | |
| 이용 또는 제공 구분 | [ ]목적 외 이용 | [ ] 제 3자 제공 | |
| 목적 외 이용기관의 명칭<br>(목적 외 이용의 경우) | | 담당자 | 소속 :<br>성명 :<br>전화번호 : |
| 제공받는 기관의 명칭<br>(제3자 제공의 경우) | | 담당자 | 소속 :<br>성명 :<br>전화번호 : |
| 이용하거나 제공한 날짜, 주기 또는 기간 | | | |
| 이용하거나 제공한 형태 | | | |
| 이용 또는 제공의 법적 근거 | | | |
| 이용 목적 또는 제공받는 목적 | | | |
| 이용하거나 제공한 개인정보의 항목 | | | |
| 「개인정보 보호법」 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용 | | | |

# 정보주체 이외로부터 수집한 개인정보의 처리(제 20조)

- **정보주체 이외로부터 수집한 개인정보를 처리할 때, 정보주체의 요구가 있으면 즉시 다음의 사항을 알려야 함** (법 제20조제1항)

  - 개인정보 수집 출처, 개인정보 처리 목적,
  - 개인정보 처리의 정지를 요구할 권리가 있다는 사실

- **법 제17조제1항에 따라 정보주체의 동의를 받아 제3자로부터 개인정보를 제공받은 경우 정보주체에게 수집출처, 처리목적, 처리정지 요구가 가능함을 고지하여야 함**
  ※ 단. 정보주체에게 알릴 수 있는 개인정보가 없다면 예외 가능

- **고지 대상**

  - 5만명 이상의 민감정보 또는 고유식별정보를 처리하는 자
  - 100만명 이상 정보주체에 대한 개인정보를 처리하는 자

- **고지 방법**

  - 서면, 전화, 문자전송, 전자우편 등 방법, 개인정보를 제공받은 날로 부터 3개월 이내
  - 정보주체의 동의를 받은 범위에서 연 2회 이상 주기적으로 제공받는 경우 제공받은 날로부터 3개월 이내 또는 동의를 받은 날로 부터 기산하여 연 1회 이상

- **고지하였다는 사실, 알린 시기, 알린 방법을 개인정보 파기할 때까지 보관 관리**

# 정보주체로부터 동의 받는 방법 (제 22조)

- **정보주체(법정대리인 포함)의 동의를 받을 때에는 각각의 동의사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 함**
- **정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분**
  - 제15조 제1항 제1호, 제17조 제1항 제1호, 제23조 제1항 제1호 및 제24조 제1항 제1호에서 정보주체의 동의 필요
  - 동의 없이 처리 가능한 개인정보라는 입증책임은 개인정보처리자에게 있음
- **홍보나 마케팅 등의 이유로 개인정보 처리 동의를 받으려 할 때는 정보주체가 이를 명확하게 인지하고 동의해야 함**
- **선택적으로 동의할 수 있는 사항을 동의하지 않는다는 이유로 재화 또는 서비스의 제공을 거부해서는 안됨**
- **만 14세 미만 아동의 개인정보를 처리하려면 법정대리인의 동의를 받아야 함**
  - 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 해당 아동으로부터 직접 수집할 수 있음

# 정보주체로부터 동의 받는 방법 (제 22조)

❖ 명확히 표시하여야 하는 사항-'17.4.18 개정, '17.10.19 시행(안)

· 재화나 서비스의 홍보 및 판매 권유, 기타 이와 관련된 목적으로 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실

· 개인정보 중 다음 각 목의 사항

- 민감정보
- 여권번호, 운전면허의 면허번호 및 외국인등록번호

· 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적

· 개인정보의 보유 및 이용 기간

❖ 표시 방법 - 시행규칙 개정(안)

· 글씨는 9포인트 이상의 크기로 하되 다른 내용보다 20% 이상 크게 할 것

· 다른 색의 글씨, 굵은 글씨 또는 밑줄 등을 사용하여 명확히 드러나게 할 것

· 중요한 내용이 많은 경우에는 별도로 요약하여 제시할 것

# 민감정보, 고유식별정보 처리제한(제 23조, 24조)

## 민감정보 및 고유식별정보는 원칙적으로 처리 금지

- 정보주체에게 **별도 동의**를 얻거나, **법령에서 구체적으로 처리를 요구하거나 허용하는** 경우에 한하여 처리

| | |
|---|---|
| 민감정보 | 사상, 신념, 노동조합·정당가입, 건강정보, 유전정보, 범죄경력 정보 |
| 고유식별정보 | 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 |

- 분실·도난·유출·위조·변조·훼손되지 않도록 **안전성 확보조치 의무**

위 규정에도 불구하고 주민등록번호는
법령에 구체적으로 처리근거가 있어야 처리가 가능함(제24조2)

# 고유식별정보 처리자에 대한 정기적 조사(제 24조)

행정안전부장관은 개인정보처리자가 고유식별정보에 대한 안전성 확보 조치를 이행하고 있는지를 **정기적으로 조사**

| | |
|---|---|
| **대 상** | • 공공기관<br>• 5만 명 이상 정보주체의 고유식별정보를 처리하는 자 |
| **주 기** | 2년마다 1회 이상 |
| **방 법** | 온라인 또는 서면을 통하여 필요한 자료 제출 |
| **전문기관** | 한국인터넷진흥원 또는 행안부장관이 고시하는 기관 |

# 주민등록번호의 처리제한(제 24조의2)

**주민등록번호는 정보주체의 동의를 받아도 처리 불가**

## 01 주민등록번호 처리가 가능한 경우

- 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙 · 중앙선거관리위원회 규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
- 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 보호
- 위의 사항에 준하는 경우로서 행정안전부령으로 정하는 경우

## 02 주민번호 암호화 의무

- 100만 명 **미만의 주민번호** 보관
  '16.12.31.까지 암호화

주민번호 보관
**100만 명**

- 100만 명 **이상의 주민번호** 보관
  '17.12.31.까지 암호화

## 03 인터넷으로 회원 가입시 주민번호 대체수단 제공

- ( 예 ) I - PIN, 공인인증서, 전자서명 등

# 영상정보처리기기 설치·운영(제 25조)

**누구든지 공개된 장소에서는 영상정보처리기기 설치 및 운영 원칙적 금지**

## 설치·운영이 가능한 경우

- 법령에서 구체적으로 허용하는 경우
- 범죄의 예방 및 수사
- 시설안전 및 화재 예방
- 교통단속
- 교통정보의 수집 · 분석 및 제공

## 설치·운영 금지 장소

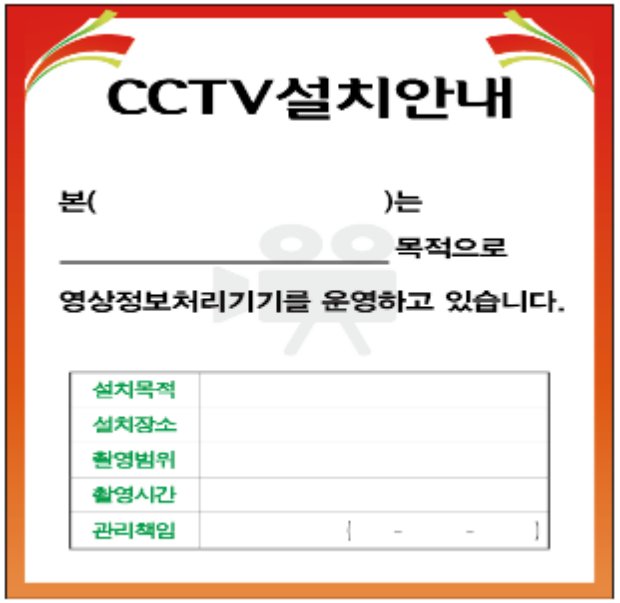
- 목욕탕·화장실·발한실(發汗室)·탈의실 등 사생활 침해 우려가 현저한 장소
- 교도소, 정신보건시설은 설치 가능

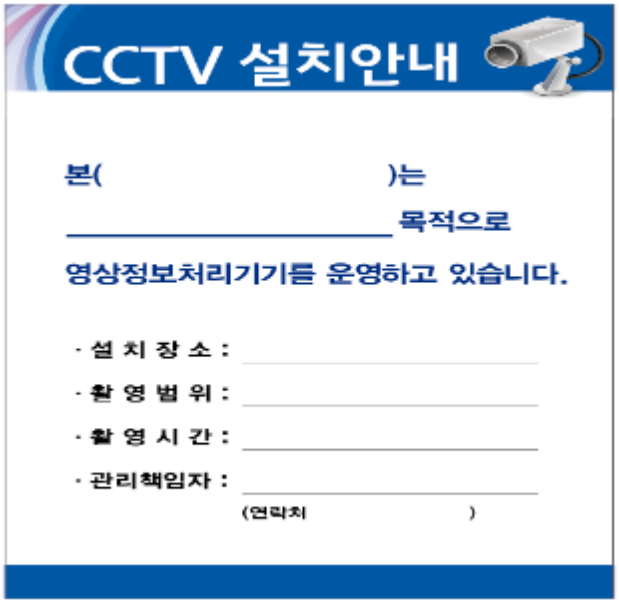
## 영상정보처리기기 운영·관리 방침

- 영상정보처리기기운영자는 영상정보처리기기 운영·관리 방침 마련

# 영상정보처리기기 설치·운영(제25조)

- 정보주체가 쉽게 인식할 수 있도록 다음 사항이 포함된 안내판을 설치




## 1 안내판 설치 의무가 없는 경우

군사시설, 국가중요시설, 국가보안시설

## 2 안내판 내용을 인터넷 홈페이지에 게재로 갈음할 수 있는 경우

1 . 공공기관이 원거리 촬영, 과속·신호위반 단속 또는 교통흐름조사 등의 목적으로 영상정보처리기기를 설치하는 경우로서 개인정보 침해 우려가 적은 경우

2 . 산불감시용 등 장소적 특성으로 인하여 안내판을 설치 하는 것이 불가능한 경우

# 업무위탁에 따른 개인정보 처리제한 (제26조)

- **처리위탁은 문서에 의해서 해야 함 (제1항)**
  - **문서에 포함될 내용**

    ① 위탁업무 수행 목적 외 개인정보의 처리 금지
    ② 개인정보의 기술적·관리적 보호조치
    ③ 위탁업무의 목적 및 범위
    ④ 재위탁 제한
    ⑤ 개인정보에 대한 접근 제한 등 안전성 확보 조치
    ⑥ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등의 감독
    ⑦ 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등의 책임
- **위탁하는 업무 내용, 수탁자를 인터넷 홈페이지에 공개**
- **홍보, 마케팅 업무 위탁시 업무 내용과 수탁자를 정보주체에게 고지**
- **수탁자가 개인정보를 안전하게 관리할 수 있도록 수탁자 교육, 감독**
- **수탁자의 이 법 위반으로 발생한 손해배상책임은 위탁자에게 있음**

# [참고] 개인정보 제3자 제공 vs 위탁

| | 제 3자 제공<br>(법 제17조, 제18조) | 위탁<br>(법 제26조) |
|---|---|---|
| 처리 목적 | **제공받는 자**의 이익 / 목적 | **제공하는 자**의 이익 / 목적 |
| 관리 범위 | **제공받는 자**의 책임 | **제공하는 자**의 책임 |
| 예시 | • 경찰에 수사자료로 제공<br>• 감사기관(감사 수행 목적) 등에 감사자료로 제출<br>• 마트 이벤트 고객정보를 보험회사 마케팅에 제공 | • 민원 처리 만족도 조사를 위해 리서치 업체에 직원 정보 제공<br>• 직원 교육을 위해 교육 위탁업체에 직원 명단 제공<br>• SMS를 통한 홍보를 위해 고객의 전화번호를 문자발송 업체에 전달 |

# 개인정보의 파기 (제 21조)

보유기간의 경과, 처리목적 달성 시 **지체 없이(5일 이내)** 파기
다만, 다른 법령에 규정이 있으면 보존 가능

개인정보 파기할 때에는 **복구 • 재생되지 않도록** 조치

파기 대상 개인정보의 보존 시 다른 개인정보와 분리하여 저장·관리

## 전부 파기

- **완전파괴**(소각, 파쇄 등)
- **전용 소자장비**를 이용하여 삭제
- 데이터가 복원되지 않도록 **초기화 또는 덮어쓰기** 수행

## 일부 파기

- 전자적 파일 형태
  : 개인정보 삭제 후 복구 • 재생되지 않도록 **관리 • 감독**
- 기록물, 인쇄물, 서면, 기록매체
  : 해당 부분을 **마스킹, 천공** 등으로 삭제

# Ⅳ 개인정보의 안전한 관리

(개인정보 보호법 제 4장)

# 개인정보의 안전한 관리

**민감정보·고유식별정보·개인정보가 분실·도난·유출·위조·변조·훼손되지 않도록 안전성 확보 조치를 해야 함**

## 개인정보의 안전성 확보조치 기준 (행정안전부 고시)

1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
5. 개인정보에 대한 보안프로그램의 설치 및 갱신
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

# 개인정보 처리방침의 수립 및 공개 (제 30조)

## 개인정보 처리방침의 주요 내용

1. 개인정보의 처리 목적
2. 처리하는 개인정보의 항목
3. 개인정보의 처리 및 보유 기간
4. 개인정보의 제3자 제공에 관한 사항(해당하는 경우에만 정한다)
5. 개인정보의 파기에 관한 사항
6. 개인정보 처리 수탁자 담당자 연락처, 수탁자의 관리 현황 점검 결과 등 개인정보처리 위탁에 관한 사항 (해당하는 경우에만 정한다)
7. 영 제30조제1항에 따른 개인정보의 안전성 확보조치에 관한 사항
8. 개인정보의 열람, 정정·삭제, 처리정지 요구권 등 정보주체의 권리·의무 및 그 행사방법에 관한 사항
9. 개인정보 처리방침의 변경에 관한 사항
10. 개인정보 보호책임자에 관한 사항
11. 개인정보의 열람청구를 접수·처리하는 부서
12. 정보주체의 권익침해에 대한 구제방법

# 개인정보 보호책임자의 지정 (제31조)

## 개인정보 보호책임자

**역할** 개인정보의 처리에 관한 업무를 총괄, 책임

**업무**

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오·남용 방지를 위한 내부통제시스템 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독
7. 개인정보 처리방침의 수립 · 변경 및 시행
8. 개인정보 보호 관련 자료의 관리
9. 처리 목적이 달성, 보유기간이 지난 개인정보의 파기

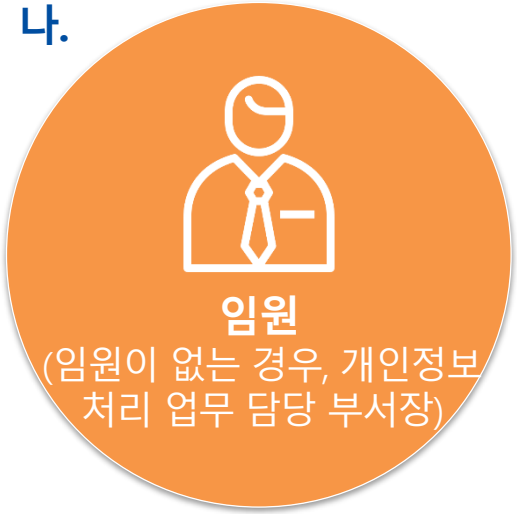
# 개인정보 보호책임자의 지정 (제31조)

- 개인정보 보호와 관련하여 이 법 및 다른 법령의 위반 사실을 알게 된 경우, 즉시 개선조치 시행, 필요 시 소속 기관의 장에게 보고
- 개인정보처리자는 보호책임자가 업무를 수행함에 있어서 정당한 이유없이 불이익을 줘서는 안됨

## 개인정보 보호책임자의 요건

가.


나.

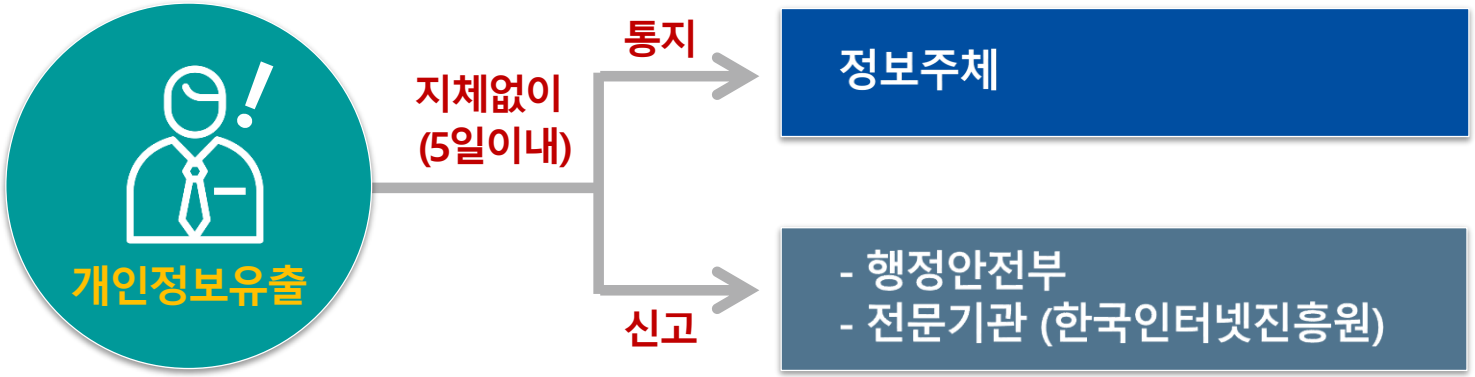


# [참고] 개인정보보호책임자의 지정 요건(공공)

| | |
|---|---|
| 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙 행정기관 | 고위공무원단에 속하는 공무원 |
| 정무직공무원을 장(長)으로 하는 국가기관 | 3급 이상 공무원 |
| 고위공무원, 3급 공무원을 장으로 하는 국가기관 | 4급 이상 공무원 |
| 기타 국가기관(소속 기관 포함) | 개인정보 처리 업무 부서장 |
| 시 · 도 및 시 · 도 교육청 | 3급 이상 공무원 |
| 각급 학교 | 행정사무 총괄자 |
| 기타 공공기관 | 개인정보 처리 업무 부서장 |

# 개인정보 유출 통지 등 (제 34조)

개인정보 유출 사실을 인지하였을 경우에는 지체없이 정보주체에게 관련 사실 통지 및 전문기관에 신고 등 조치를 취해야 함

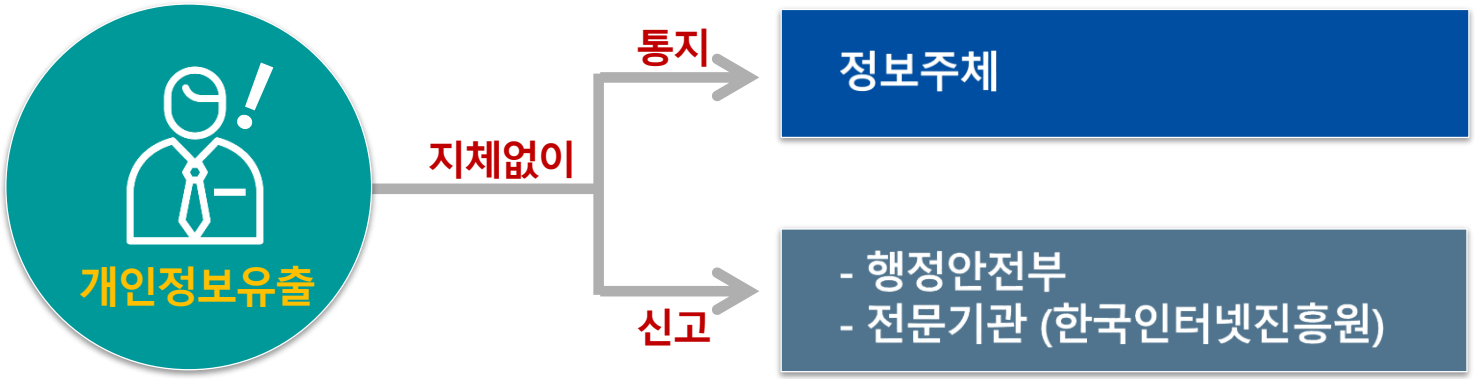



| 통지방법 | 신고방법 |
|---|---|

| | |
|---|---|
| 통지대상 | 1건이라도 개인정보 유출 시, 정보주체에게 유출관련 사실을 통지 |
| 통지시기 | 5일 이내 |
| 통지방법 | 개별 통지 - 서면, 전자우편, 전화, 팩스, 문자전송 등<br>※ 1만명 이상의 개인정보가 유출된 경우, 서면 등의 방법과 함께 인터넷 홈페이지에 7일 이상 게재 |
| 통지내용 | 유출된 개인정보의 항목, 유출된 시점과 그 경위, 정보주체의 피해 최소화 방법, 사업자의 대응조치 및 피해구제 절차, 담당부서 및 연락처 |

# 개인정보 유출 통지 등 (제34조)

개인정보 유출 사실을 인지하였을 경우에는 지체없이 정보주체에게 관련 사실 통지 및 전문기관에 신고 등 조치를 취해야 함




| 통지방법 | 신고방법 |
|---|---|
| 신고대상 | 1만명 이상('17.10.19부터는 1천명 이상)의 개인정보가 유출된 경우 |
| 신고기관 | 행정안전부, 전문기관(한국인터넷진흥원) |
| 신고시기 | 5일 이내 |
| 신고방법 | 전화, 전자우편, 팩스 |
| 신고내용 | 통지내용, 유출피해 최소화 대책 및 조치 결과 |

# 개인정보파일의 등록 (제32조) 공공기관만 해당

## 행정안전부장관에게 등록해야 하는 사항 (제1항)

- 개인정보파일의 명칭, 운영 근거 및 목적, 개인정보 항목,
- 개인정보의 처리방법 및 보유기간, 반복적인 제공의 경우 제공받는 자
- 공공기관의 명칭, 개인정보의 정보주체 수, 개인정보 처리 업무 담당 부서
- 개인정보의 열람 요구를 접수・처리하는 부서와 열람을 제한・거절할 수 있는 개인정보의 범위 및 사유

## 등록 예외 (제2항)

1. 국가 안전, 외교상 비밀 등 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
2. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호 집행, 교정처분, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항
3. 조세범처벌법, 관세법에 따른 범칙행위 조사에 관한 사항
4. 내부적 업무처리만을 위하여 사용되는 개인정보파일
5. 다른 법령에 따라 비밀로 분류된 개인정보파일

# 개인정보 보호 인증 (제32조의2)

**개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 법에 부합하는지 등에 관하여 인증**

- PIMS 인증의 기대효과
  - 체계적·지속적인 개인정보보호 활동 가능
  - 경영진 차원에서 상시 모니터링 체계 구축
  - 개인정보 침해사고에 효율적 대응 가능
  - 개인정보 보호에 대한 국민·고객의 신뢰 향상
- 인증전문기관 : 한국인터넷진흥원
- 인증 유효기간 : 3년
- 신청기관 유형 : 공공기관, 대기업, 중소기업, 소상공인
  * 정보통신서비스 제공자는 대기업 유형으로 인증
- 인증심사 기준 : 3개 분야 86개 항목
  ※ 인증기준 방법·절차 등은 고시 참조

**개인정보보호 관리체계(PIMS)**

# 개인정보 영향평가(제 33조)

공공기관만 해당

## ❖영향평가 수행대상

- 구축·운용 또는 변경하려는 개인정보파일로서 **5만명 이상의 정보주체**에 관한 **민감정보 또는 고유식별정보**의 처리가 수반되는 개인정보파일
- 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 **연계하려는 경우**로써 연계 결과 **50만명 이상의 정보주체**에 관한 개인정보가 포함되는 개인정보파일
- 구축·운용 또는 변경하려는 개인정보파일로서 **100만명 이상의 정보주체**에 관한 개인정보파일

## ❖ 개인정보 영향평가 기관 지정 신청 절차 등 간소화('17.10.19 시행 예정)

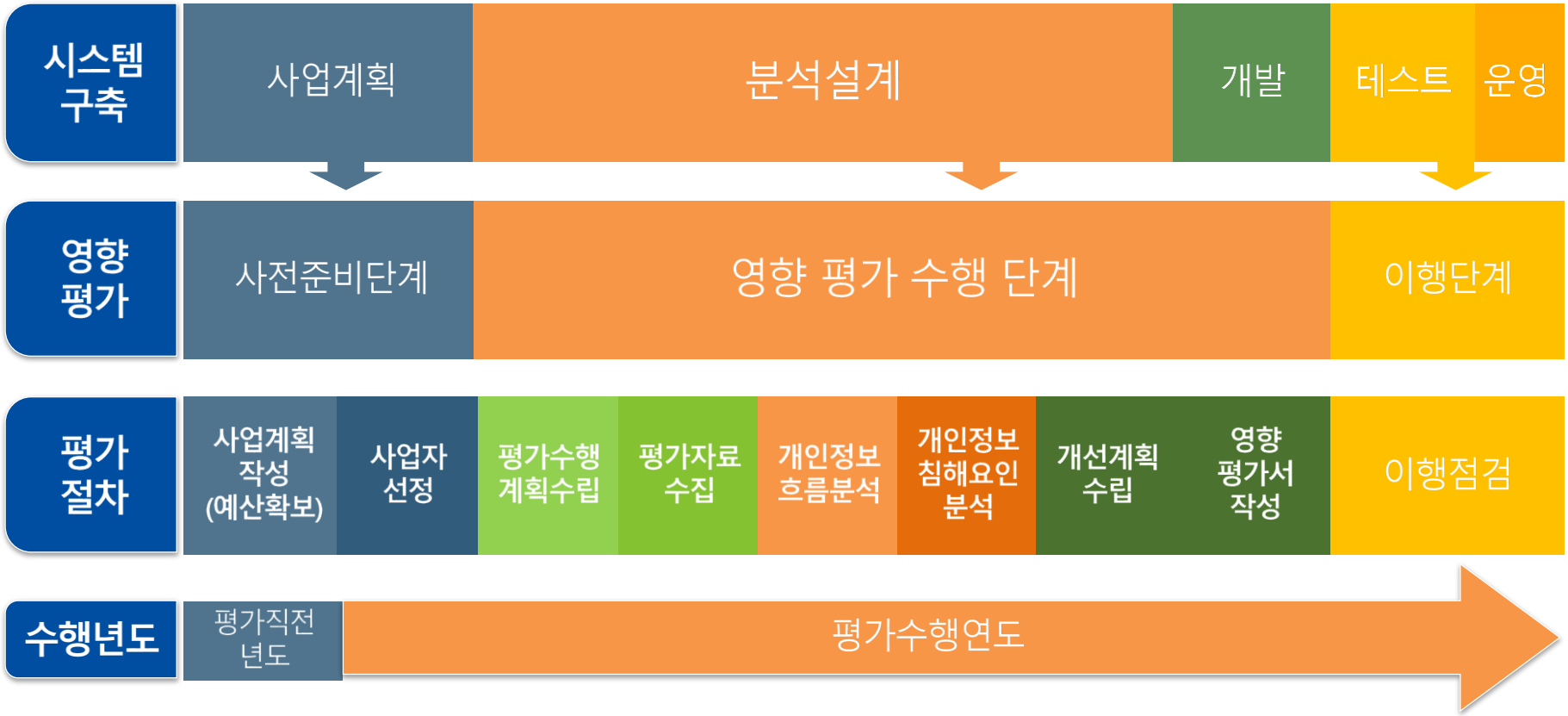
**· 개인정보 영향평가기관 지정 신청 시 제출 서류에 임원 성명을 삭제함.**

**· 평가기관 지정 이후,**

- 정관·대표자 등 기업 정보 변경신고 기간을 "7일"에서 "14일"로 변경
- 평가기관 양도·양수 또는 합병 시 신고 기간을 "30일"에서 "60일"로 변경

# [참고] 영향평가 수행시기

**정보시스템 구축·변경시 BPR/ISP(또는 분석 · 설계) 단계에서 영향평가를 수행**



# V 정보주체 권리보장과 피해구제

(개인정보 보호법 제5장, 제6장)

# 정보주체 권리 보장(제 35조 ~ 제 39조의2)

정보주체는 **자신의 개인정보에 대한 열람·정정·삭제 요구** 가능

- **개인정보의 항목 및 내용**
- **수집·이용 목적**
- **보유기간**
- **제3자 제공 현황**
- **개인정보 처리에 동의한 사실 및 내용**

※ 개인정보처리자가 공공기관인 경우에 **행정안전부장관을** 통해 열람요구 가능

**열람 요구시 10일 이내에 정보주체가 해당 개인정보를 열람할 수 있도록 조치**

1. 개인정보의 수집 출처
2. 개인정보의 처리 목적
3. 개인정보 처리의 정지를 요구 할 권리가 있다는 사실

**열람요청 기간 내에 열람할 수 없는 정당한 사유가 있을 때는,
정보주체에게 그 사유를 알리고 열람 연기 (사유 소멸 시 지체 없이 열람)**

❖ **정보주체의 열람, 정정·삭제, 처리정지 요구권의 행사 방법과 절차 간소화('17.10.19 시행)**

- **서면, 전화, 전자우편, 인터넷 등 정보주체가 쉽게 활용할 수 있는 방법 제공**
- **개인정보를 수집한 창구 또는 방법에 의해 개인정보의 열람을 요구할 수 있도록 할 것**
  (다만, 해당 창구의 지속적 운영이 곤란한 경우 등 정당한 사유가 있는 경우 예외)
- **대표 홈페이지에 열람 요구 방법과 절차를 공개**

# 개인정보 피해구제 제도 현황

## 개인정보침해신고상담


- 제도개선권고
- 행정처분 의뢰
- 수사 의뢰

»관련근거
(개인정보 보호법 제62조)

## 개인정보분쟁조정

Pico 개인정보분쟁조정위원회
Personal Information Dispute Mediation Committee

- 제도개선권고
- 손해배상 권고

»관련근거
(개인정보 보호법 제40조)

## 민사소송

- 손해배상 청구

»관련근거
(민법 제750조)

# 손해배상제도

- 징벌적 손해배상제도(제39조)와 법정 손해배상제도(제39조의2)

| 구분 | 징벌적 손해배상제도 | 법정 손해배상제도 |
|---|---|---|
| 적용 요건 | 기업의 고의·중과실로 개인정보 유출 또는 동의없이 활용하여 피해 발생 | 기업의 고의·과실로 개인정보가 분실·도난·유출된 경우 |
| 입증 책임 | 기업이 고의·중과실 없음을 입증 피해액은 피해자가 입증 | 기업이 고의·과실 없음을 입증 피해자에 대한 피해액 입증책임 면제 |
| 구제 범위 | 재산 및 정신적 피해 모두 포함 | 사실상 피해입증이 어려운 정신적 피해 |
| 배상 규모 | 실제 피해액의 3배 이내 배상 | 300만원 이하의 범위에서 상당한 금액 |
| 적용시기 | 2016년 7월 25일 이후 유출사고 | |

# VI 개인정보의 안전성 확보조치 기준

(행정안전부 고시)

# 법적 근거

**고시**

## 개인정보의 안전성 확보조치 기준

(행정안전부 고시 제2016-35호, 2016.9.1. 시행)

### 개인정보보호법

제29조
(안전조치의무)

### 개인정보보호법 시행령

제30조
(개인정보의 안전성 확보 조치)

# 목적과 용어의 정의

## ▪ [제1조] 안정성 확보조치 기준의 목적

개인정보가 분실·도난·유출·위조·변조·훼손되지 않도록 안전성 확보에 필요한
**기술적 · 관리적 · 물리적 안전조치에 관한 최소한의 기준**을 정하는 것

## ▪ [제2조] 사용하는 용어

- 정보주체
- 개인정보파일
- 개인정보처리자
- 대기업
- 중견기업
- 중소기업
- 소상공인

- 개인정보보호책임자
- 개인정보취급자
- 개인정보처리시스템
- 위험도분석
- 비밀번호

- 정보통신망
- 공개된 무선망
- 모바일 기기
- 바이오정보
- 보조저장매체
- 내부망
- 접속기록
- 관리용 단말기

※용어의 정의는 고시 참조

# 유형별 안전조치 적용

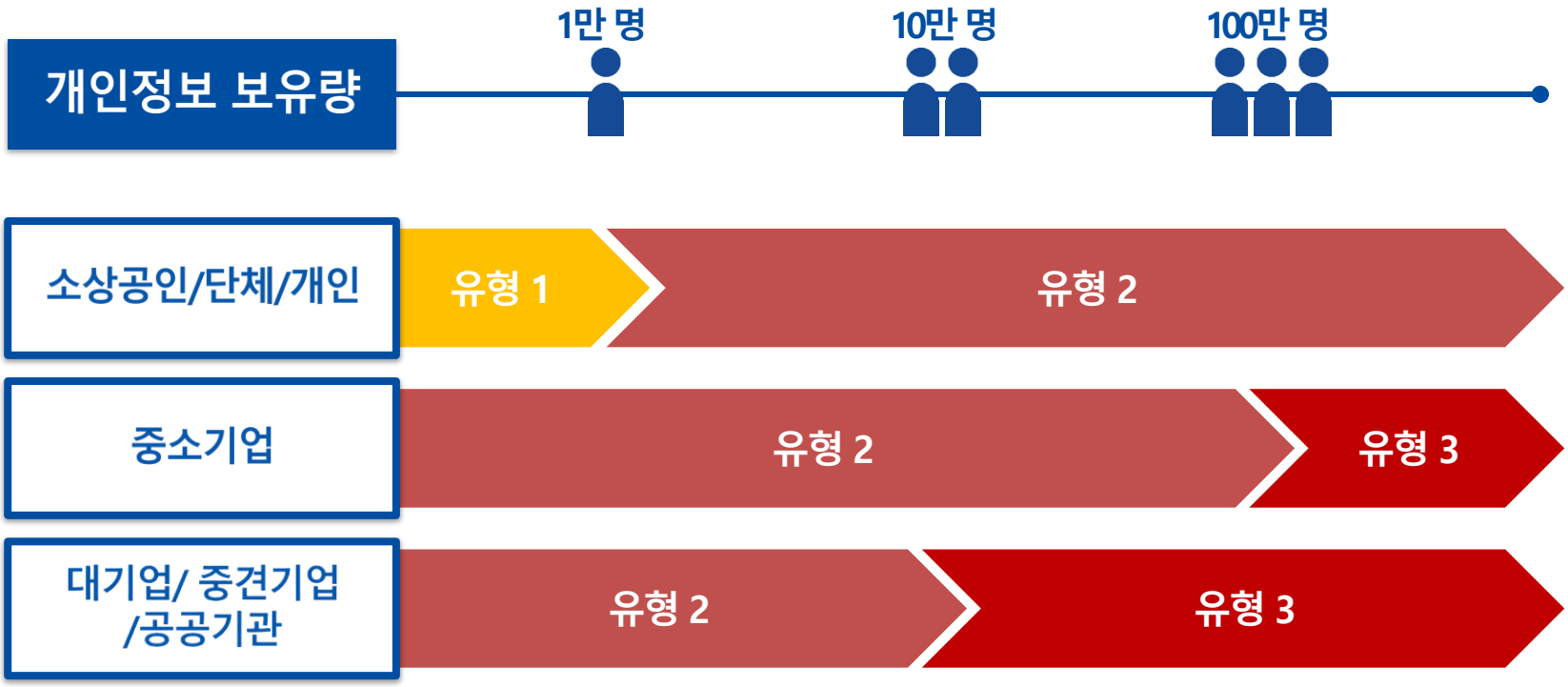
- [제3조] 안전조치 기준 차등 적용

**[ 별표 ] 개인정보처리자 유형에 따른 안전조치 기준 차등 적용**

| | |
|---|---|
| 유형1 (완화) | **1만 명 미만**의 개인정보를 보유한 **소상공인, 단체, 개인** |
| 유형2 (표준) | **1만 명 이상**의 개인정보를 보유한 **소상공인, 단체, 개인**<br>**10만 명 미만**의 개인정보를 보유한 **대기업, 중견기업, 공공기관**<br>**100만 명 미만**의 개인정보를 보유한 **중소기업** |
| 유형3 (강화) | **10만 명 이상**의 개인정보를 보유한 **대기업, 중견기업, 공공기관**<br>**100만 명 이상**의 개인정보를 보유한 **중소기업** |

# 유형별 안전조치 적용

▪ [제1조] 안정성 확보조치 기준의 목적




**유형1 (완화)**

- 제5조: 제2항~제5항
- 제6조: 제1항, 제3항, 제6항, 제7항
- 제7조: 제1항~제5항, 제7항
- 제8조, 제9조, 제10조, 제11조, 제13조

**유형2 (표준)**

- 제4조: 제1항 제1호~제10호, 제15호, 제3항, 제4항
- 제5조
- 제6조:제1항부터 제7항까지
- 제7조:제1항부터 제5항까지, 제7항
- 제8조, 제9조, 제10조, 제11조, 제13조

**유형3 (강화)**

- 제4조부터 제13조까지

# 내부 관리계획의 수립과 시행(제4조)

## 개인정보보호 내부 관리계획

1. 개인정보보호책임자(CPO) 지정
2. 개인정보취급자 및 보호책임자의 역할과 책임
3. 개인정보취급자 교육
4. 접근권한 관리
5. 접근통제
6. 개인정보 암호화
7. 접속기록 보관 및 점검
8. 악성프로그램 방지
9. 물리적 안전조치
10. 개인정보 보호조직 구성·운영
11. 유출사고 대응계획 수립 • 시행

☑ 12. 위험도 분석 및 대응방안 마련

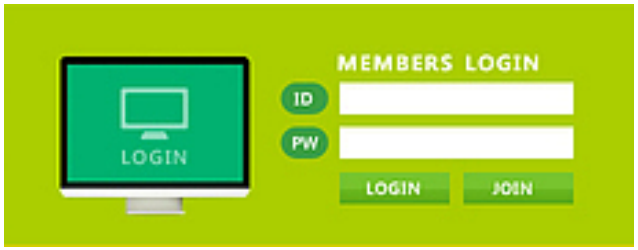
☑ 13. 재해 • 재난 대비 개인정보처리시스템의 물리적 안전조치

☑ 14. 개인정보처리 수탁자의 관리·감독

**유형1 선택조항**

15. 그 밖에 개인정보 보호를 위해 필요한 사항

# 접근권한의 관리(제5조)




① 개인정보처리시스템에 대한 접근 권한은 **업무 수행에 필요한 최소한의 범위**로 업무 담당자에 따라 차등 부여

**유형1 선택조항**

② 전보, 퇴직 등의 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 **접근 권한을 변경 또는 말소**

③ 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, **최소 3년간 보관**

④ 개인정보처리시스템의 사용자계정 발급시 **개인정보취급자 별로 발급**하며, 다른 개인정보취급자와 공유되지 않도록 함

⑤ 안전한 비밀번호를 설정하여 이행할 수 있도록 **비밀번호 작성규칙**을 수립하여 적용

⑥ 계정정보 또는 비밀번호를 **일정 횟수 이상 잘못 입력한 경우** 접근 제한 등 필요한 기술적 조치

**유형1 선택조항**

# 접근통제(제6조)

① **정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 기본 조치**

1. 접속 권한을 IP주소 등으로 제한 → 인가 받지 않은 접근 제한
2. 접속한 IP주소 등을 분석 → 불법적인 개인정보 유출 시도 탐지 및 대응

**→ 위 기능을 포함하여 조치해야 함**

IP(Internet Protocol)

② **외부에서 개인정보처리시스템에 접속하려는 경우 안전한 접속수단 또는 안전한 인증수단 적용**

**유형1 선택조항**

※ 가상사설망 (VPN : Virtual Private Network) 또는 전용선 등

③ **인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 개인정보가 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등 조치 수행**

# 접근통제 (제6조)

④ 인터넷 홈페이지를 통해 고유식별정보가 유출. 변조. 훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치 수행

**유형1 선택조항**

⑤ 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 해야 함

**유형1 선택조항**

⑥ 별도의 개인정보처리시스템이 아닌 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우

- 제1항 적용 안 함
- 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근 통제 기능 이용 가능

⑦ 업무용 모바일 기기의 분실. 도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치

# 개인정보의 암호화(제7조)

**암호화 필요 대상** 고유식별정보, 비밀번호, 바이오정보

**암호화 기준**

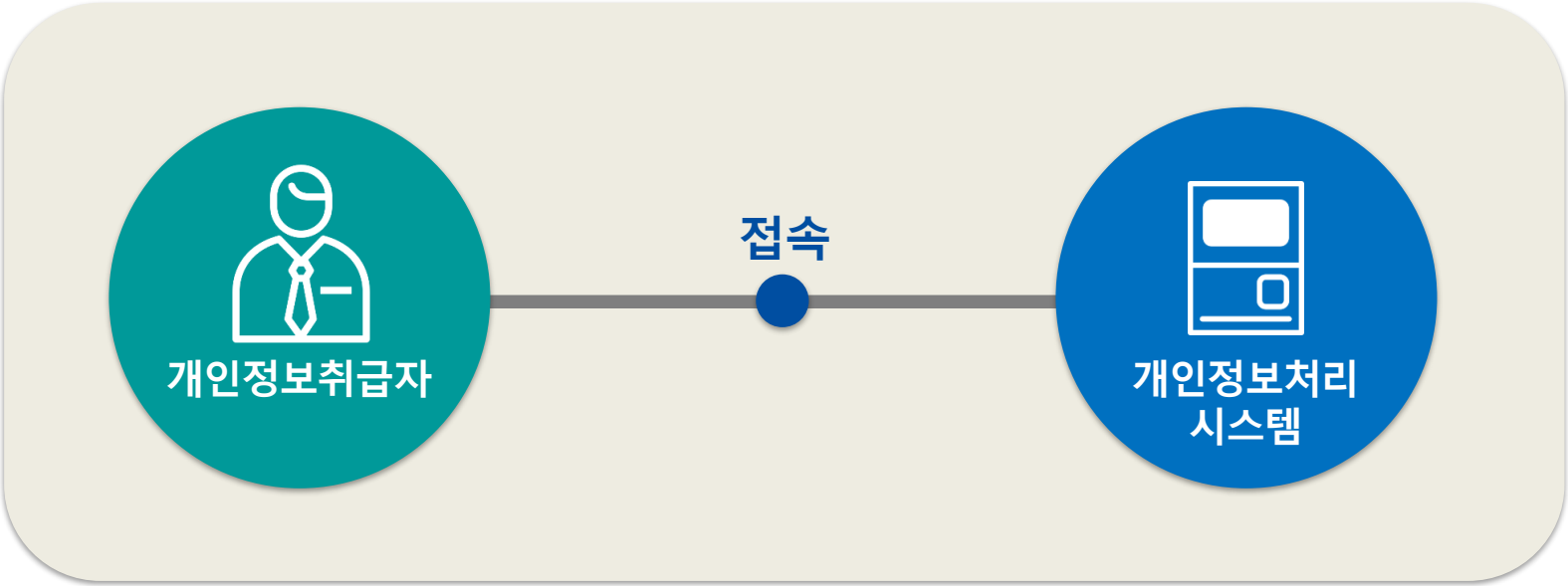
| 구 분 | | | | 암호화 기준 |
|---|---|---|---|---|
| 정보통신망, 보조저장매체를 통한 송, 수신 시 | 비밀번호, 바이오정보, 고유식별정보 | | | 암호화 송, 수신 ※제7조 ①항 TIP 참조 |
| 정보처리 시스템에 저장 시 | 비밀번호 | | | 일방향(해쉬 함수) 암호화 저장 |
| | 바이오정보 | | | 암호화 저장 |
| | 고유식별정보 | 주민등록번호 | | 암호화 저장 |
| | | 여권번호, 외국인등록번호, 운전면허번호 | 인터넷 구간, 인터넷 구간과 내부망의 중간 지점 (DMZ) | 암호화 저장 |
| | | | 내부망에 저장 | 암호화 저장 또는 다음 항목에 따라 암호화 적용여부. 적용범위를 정하여 시행<br>① 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과<br>② 암호화 미적용시 위험도 분석에 따른 결과 |
| 업무용 컴퓨터, 모바일 기기에 저장 시 | 비밀번호, 바이오정보, 고유식별정보 | | | 암호화 저장(비밀번호는 일방향 암호화 저장) |

- 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행

☑ 유형1,2 선택조항

- 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장

# 접속기록의 보관 및 점검(제8조)




① 접속한 기록을 **6개월 이상 보관. 관리**

② **반기별로 1회 이상** 점검 → 개인정보의 **분실. 도난. 유출. 위조. 변조 또는 훼손** 등에 대응하기 위하여

③ 개인정보취급자의 접속기록이 위. 변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관

# 악성프로그램 등 방지(제9조)

악성프로그램 등을 방지. 치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치. 운영해야 함

**1. 보안 프로그램은 항상 최신의 상태로 유지**

- 자동 업데이트 기능 사용
- 일 1회 이상 업데이트 실시

**2. 악성프로그램 관련 경보 발령 또는 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트 실시**

**3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치**

# 관리용 단말기의 안전조치(제10조)


개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로
개인정보처리시스템에 직접 접속하는 단말기

1 인가 받지 않은 사람이 임의로 조작하지 못하도록 조치

2 본래 목적 외로 사용되지 않도록 조치

3 악성프로그램 감염 방지 등을 위한 보안조치 적용

# 물리적 안전조치(제11조)

① 개인정보 보관을 위한 물리적 보관 장소(전산실, 자료보관실 등)는 출입통제 절차를 수립. 운영

② 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관

③ 개인정보가 포함된 보조저장매체의 반출. 입 통제를 위한 보안대책을 마련

다만, 별도의 개인정보처리시스템 없이 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우는 예외

# 재해·재난 대비 안전조치(제12조) ☑ 유형1,2 선택조항

## 화재, 홍수, 단전 등의 재해. 재난 발생 시

① 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검

② 개인정보처리시스템 백업 및 복구를 위한 계획 마련

# 개인정보의 파기(제13조)

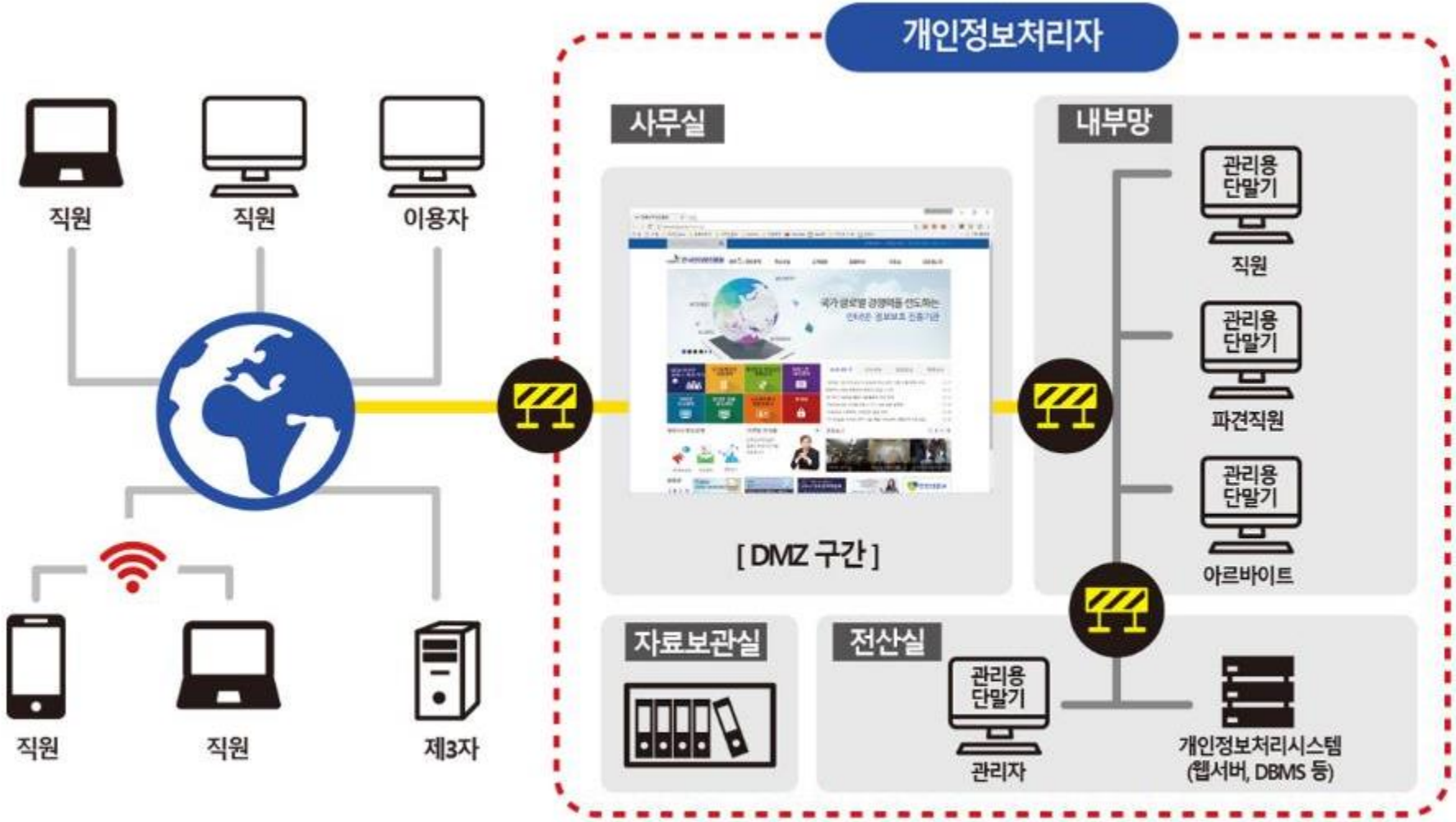
### ① 개인정보 파기 조치

1. 완전파괴(소각. 파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

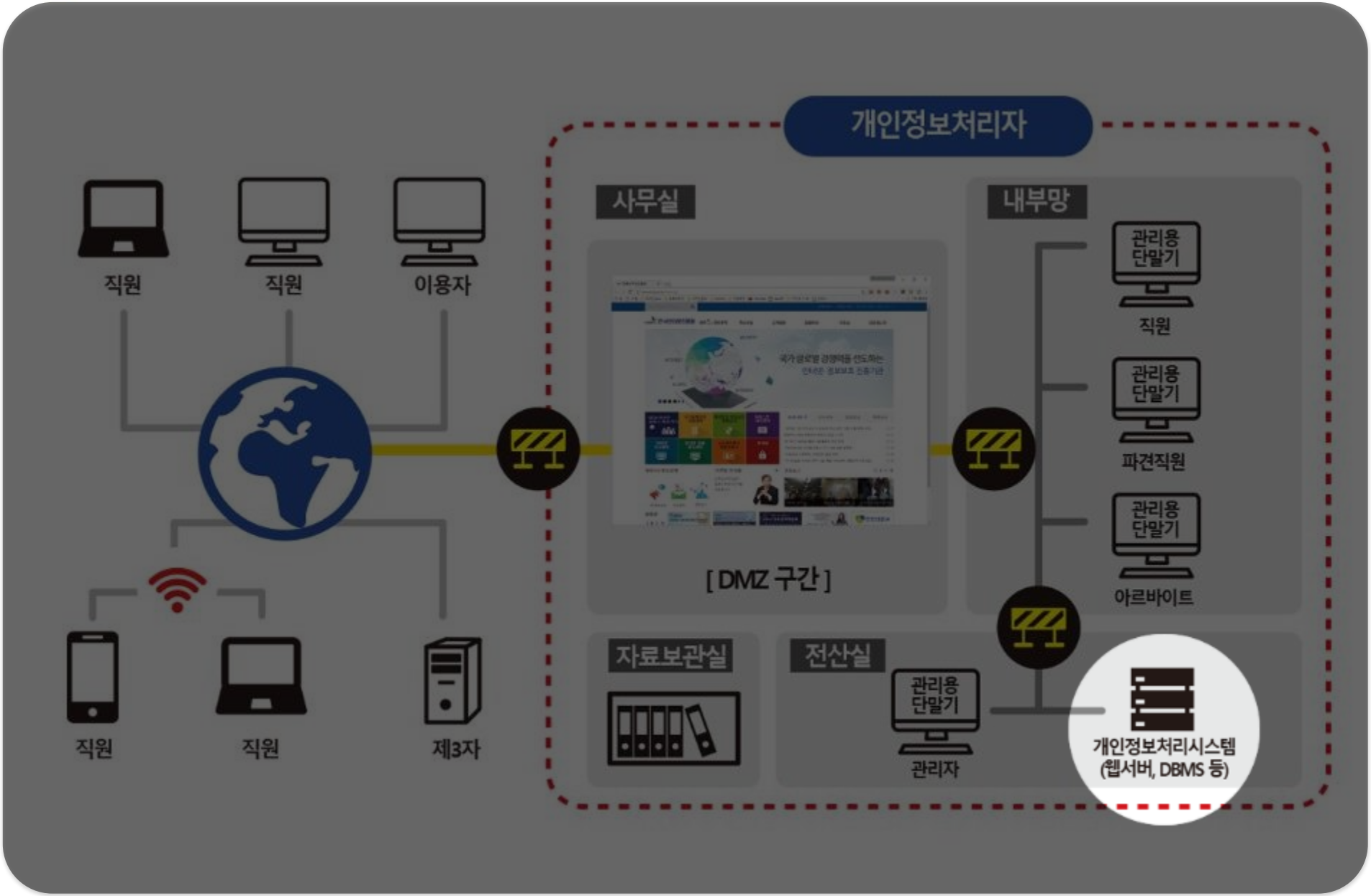
### ② 1항의 방법이 어려울 경우 일부 파기 조치

| | |
|---|---|
| **전자적 파일** | 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독 |
| **기록물, 인쇄물, 서면, 그 밖의 기록매체** | 해당 부분을 마스킹, 천공 등으로 삭제 |

# 고시에 따른 개인정보처리자의 업무처리 환경 개념도



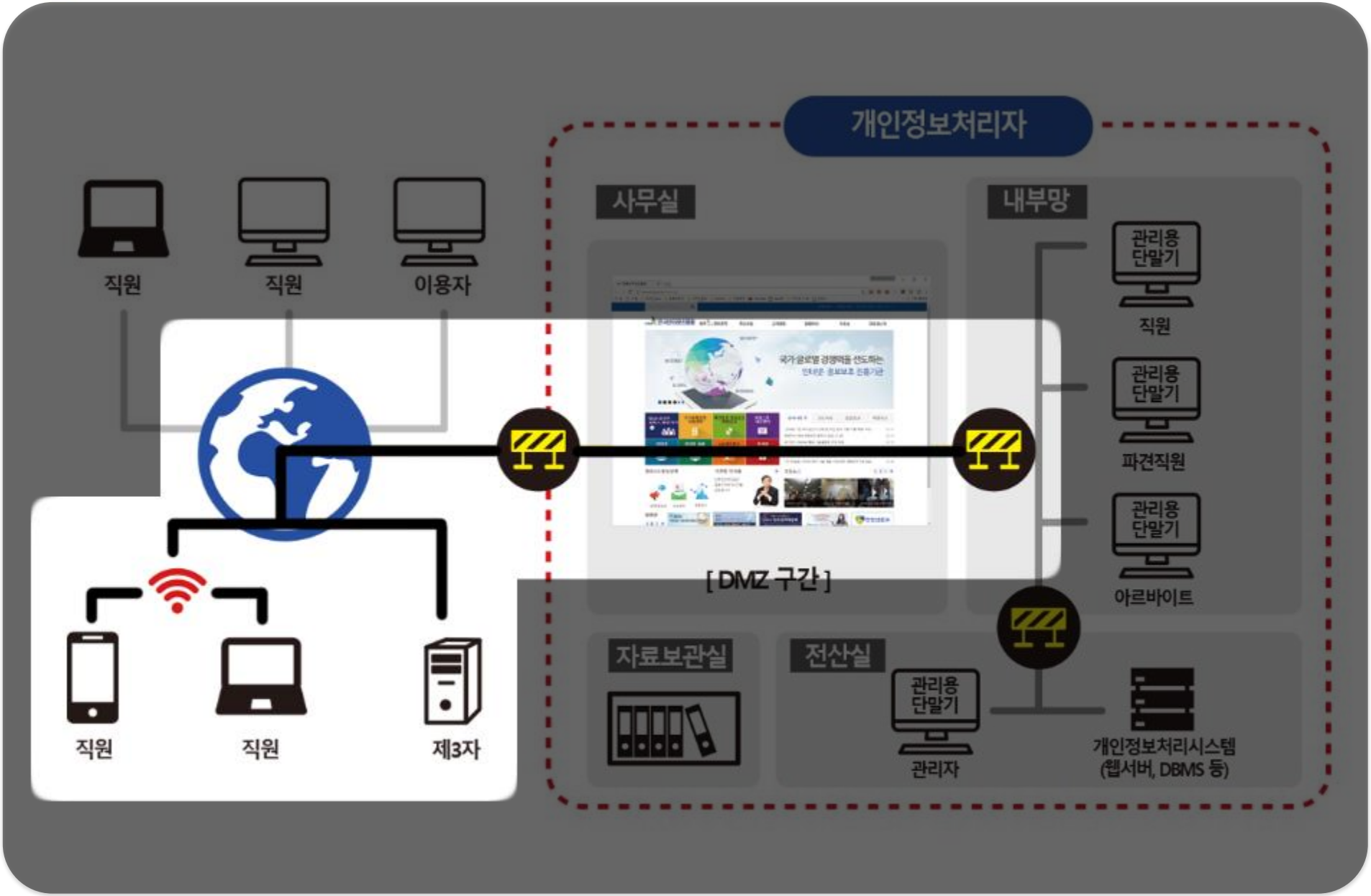
# 1. 개인정보처리시스템 측면



# 1. 개인정보처리시스템 측면

- 접근권한 관리 (권한 변경, 말소, 3년간 기록보관)
- 취급자(사용자)별 계정 발급, 비밀번호 작성규칙 수립・운영, 일정 횟수 이상 잘못 입력시 접근 제한
- 접근통제시스템  설치・운영, 일정시간 이후 개인정보처리시스템에서 자동 로그아웃
- 외부에서 처리시스템 접속시 VPN 등 안전한 접속수단 또는 안전한 인증수단 적용
- 고유식별정보, 비밀번호, 바이오 정보 저장, 송신시 암호화, 안전한 암호키 관리 (내부망에 고유식별정보 저장시에는 영향평가, 위험도 분석 결과에 따른 암호화)
- 개인정보 취급자 접속기록 6개월 이상 안전하게 보관 및 반기별 1회 이상 점검
- 보유기간이 경과한 개인정보 파기 (전부 또는 일부 파기)

# 2. 네트워크 측면


개인정보처리자
사무실
내부망
직원
직원
이용자
관리용 단말기
직원
관리용 단말기
파견직원
관리용 단말기
아르바이트
[ DMZ 구간 ]
자료보관실
전산실
관리용 단말기
관리자
개인정보처리시스템
(웹서버, DBMS 등)
직원
직원
제3자

# 2. 네트워크 측면

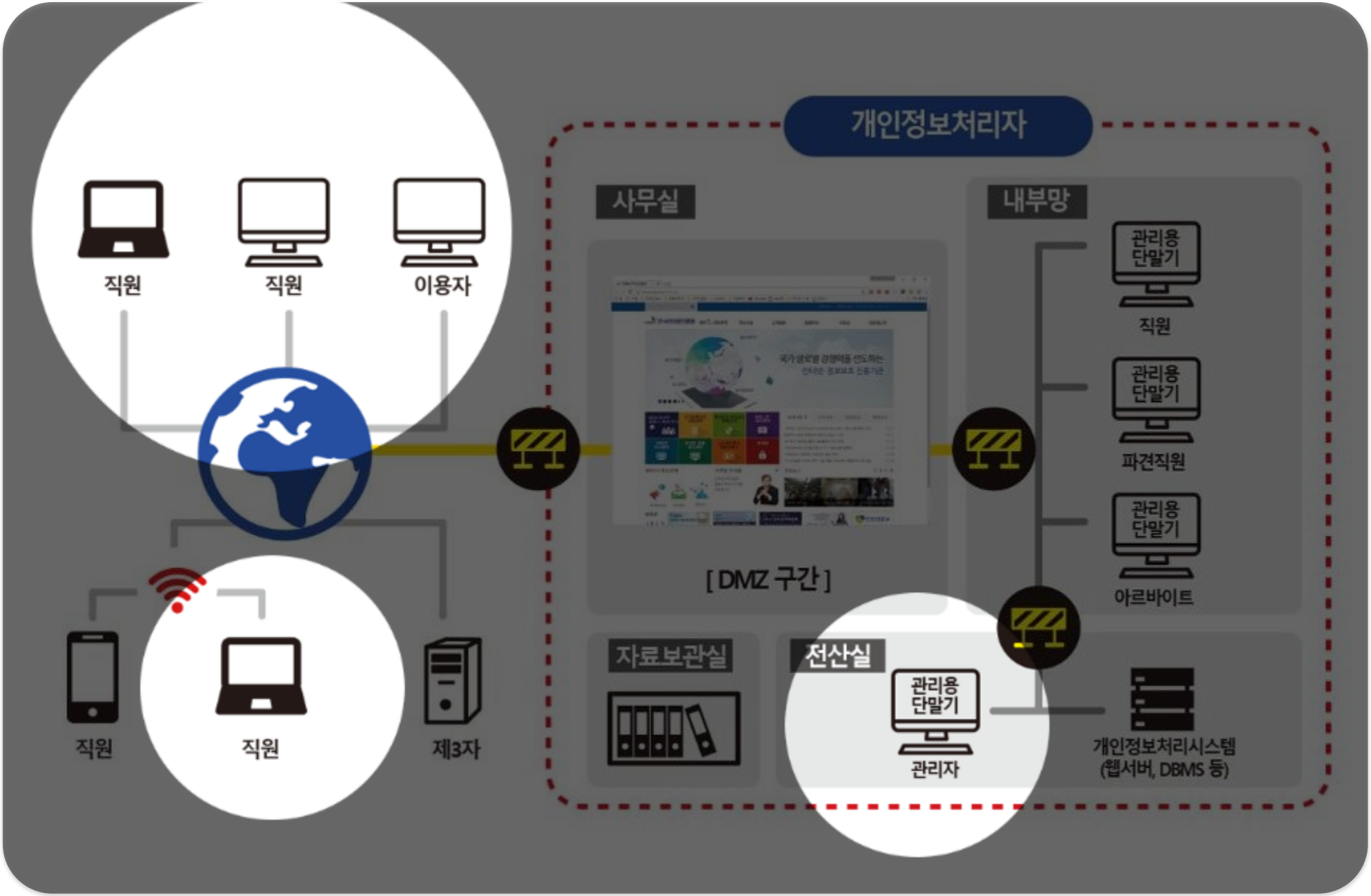
- 공개된 무선망 이용시 DBMS, 업무용 PC, 모바일 기기, 관리용 단말기에 개인정보 유출 방지조치 (TLS 적용, 콘텐츠 암호화, WPA2/보안업데이트/신뢰된 주체가 운영하는 AP 접속 등)

- 고유식별정보, 비밀번호, 바이오 정보 전송시 암호화

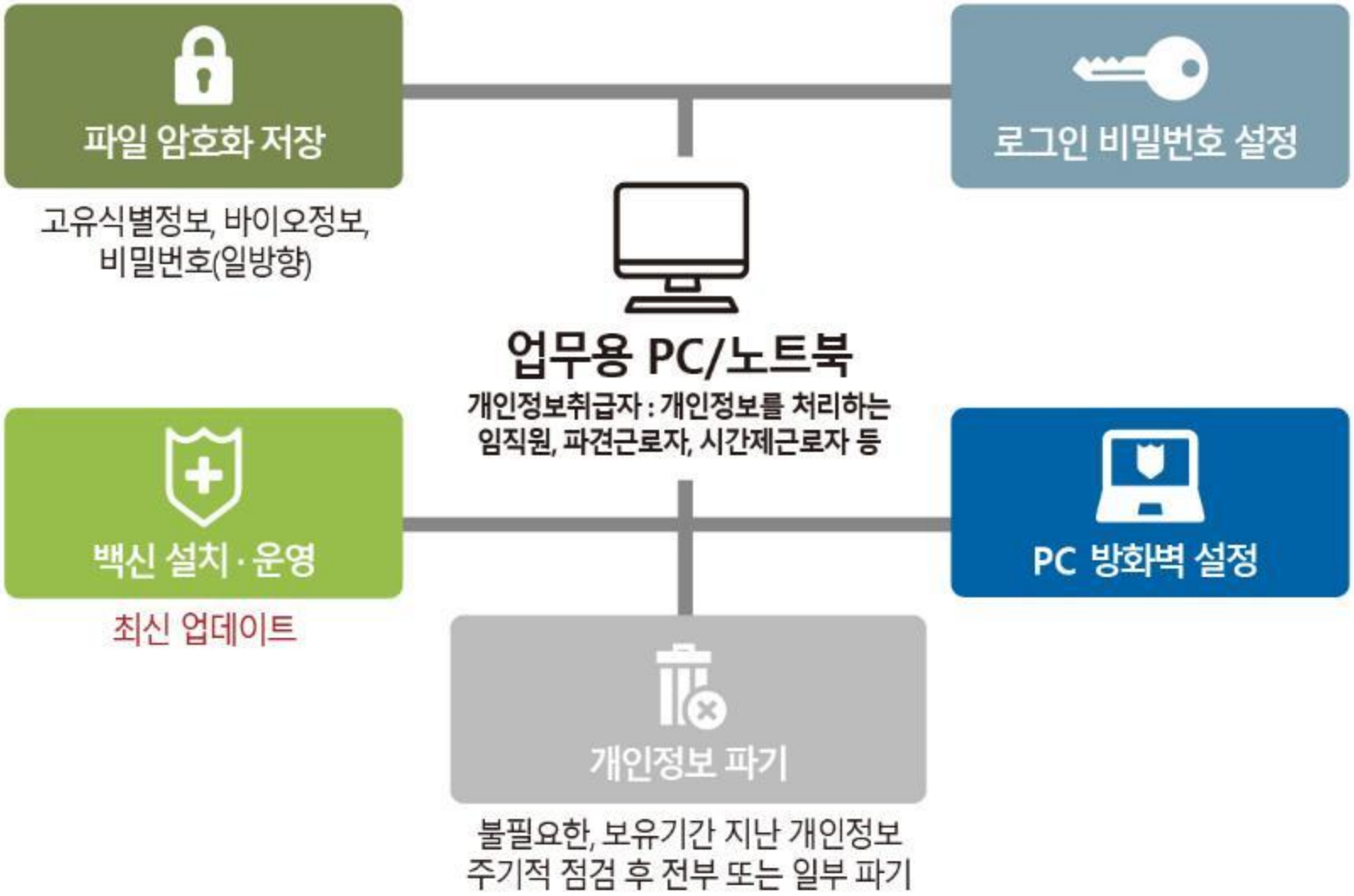

- 비인가자 접근통제, 유출시도 탐지 기능을 포함한 조치 (방화벽, 침입탐지/방지시스템, 데이터유출방지(DLP) 등 활용)

- 외부에서 개인정보처리시스템 접속시 VPN 등 안전한 접속수단 또는 2단계 인증 등 안전한 인증수단 적용

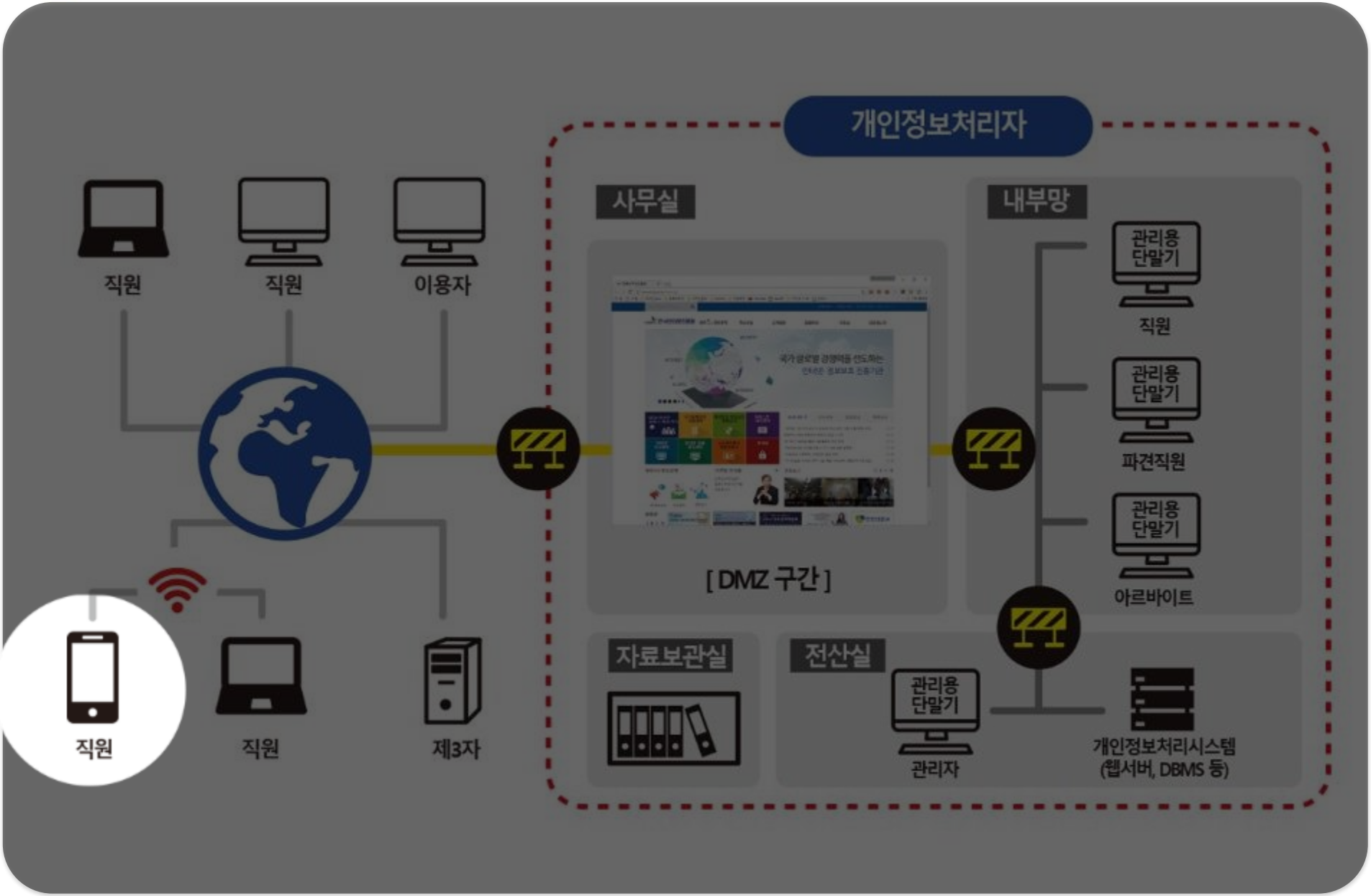
# 3. 업무용 PC 측면


개인정보처리자
사무실
내부망
직원
직원
이용자
관리용 단말기
직원
관리용 단말기
파견직원
관리용 단말기
아르바이트
[ DMZ 구간 ]
직원
직원
제3자
자료보관실
전산실
관리용 단말기
관리자
개인정보처리시스템
(웹서버, DBMS 등)

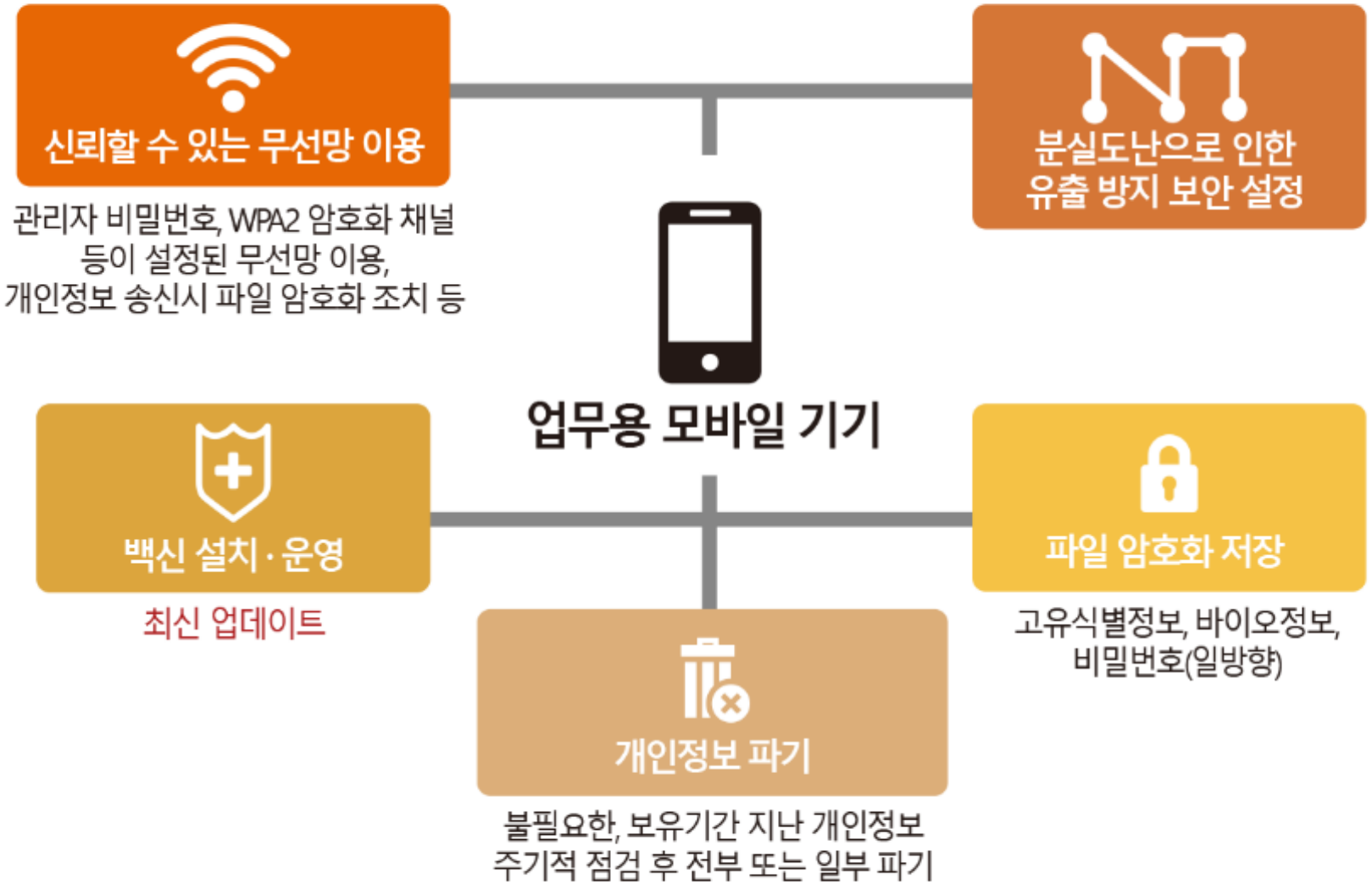
# 3. 업무용 PC 측면


파일 암호화 저장
고유식별정보, 바이오정보,
비밀번호(일방향)
로그인 비밀번호 설정
업무용 PC/노트북
개인정보취급자 : 개인정보를 처리하는
임직원, 파견근로자, 시간제근로자 등
백신 설치 · 운영
최신 업데이트
PC 방화벽 설정
개인정보 파기
불필요한, 보유기간 지난 개인정보
주기적 점검 후 전부 또는 일부 파기

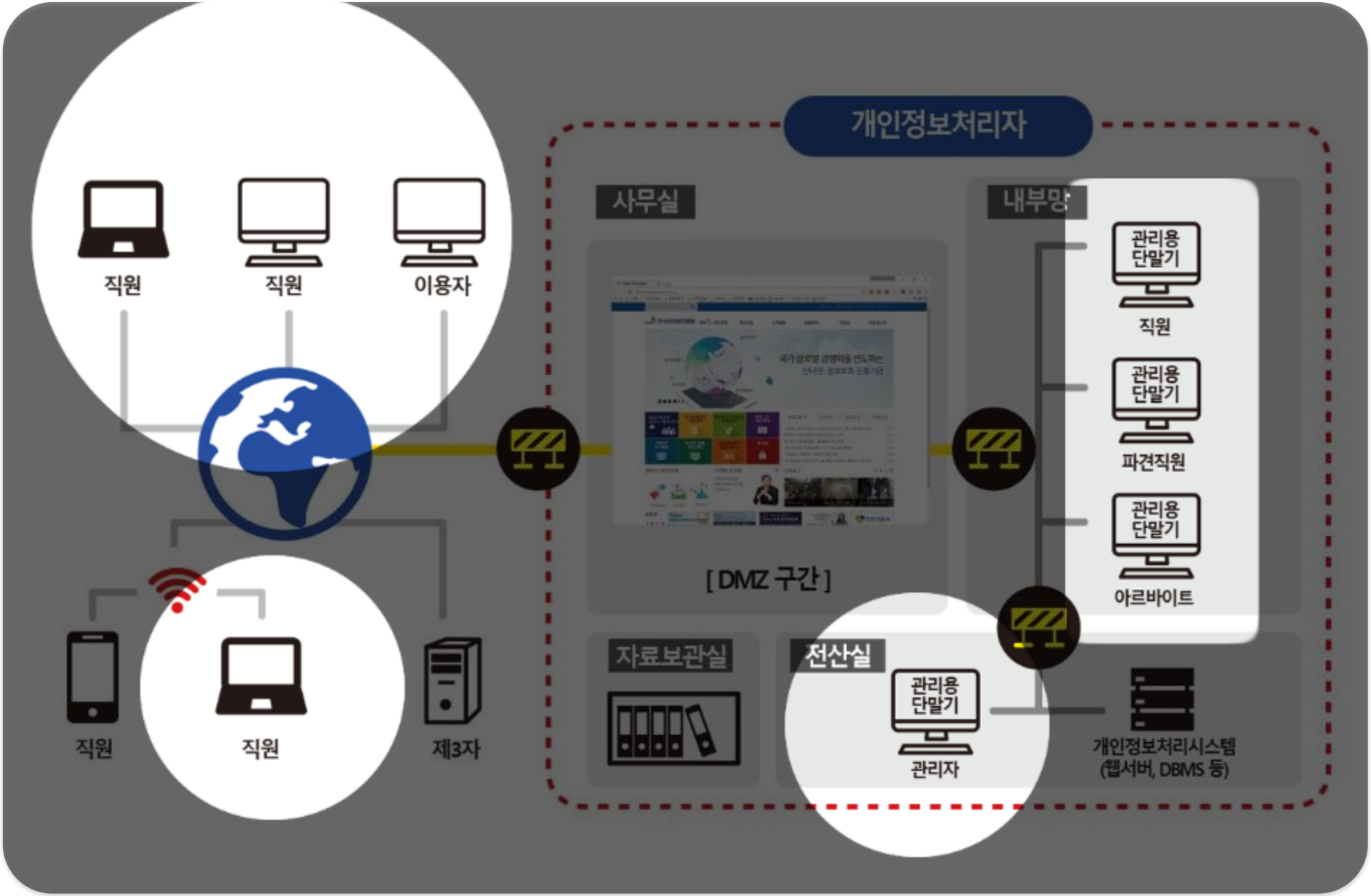
# 4. 모바일 기기 측면


개인정보처리자
사무실
내부망
직원
직원
이용자
[ DMZ 구간 ]
관리용 단말기
직원
관리용 단말기
파견직원
관리용 단말기
아르바이트
자료보관실
전산실
관리용 단말기
관리자
개인정보처리시스템
(웹서버, DBMS 등)
직원
직원
제3자

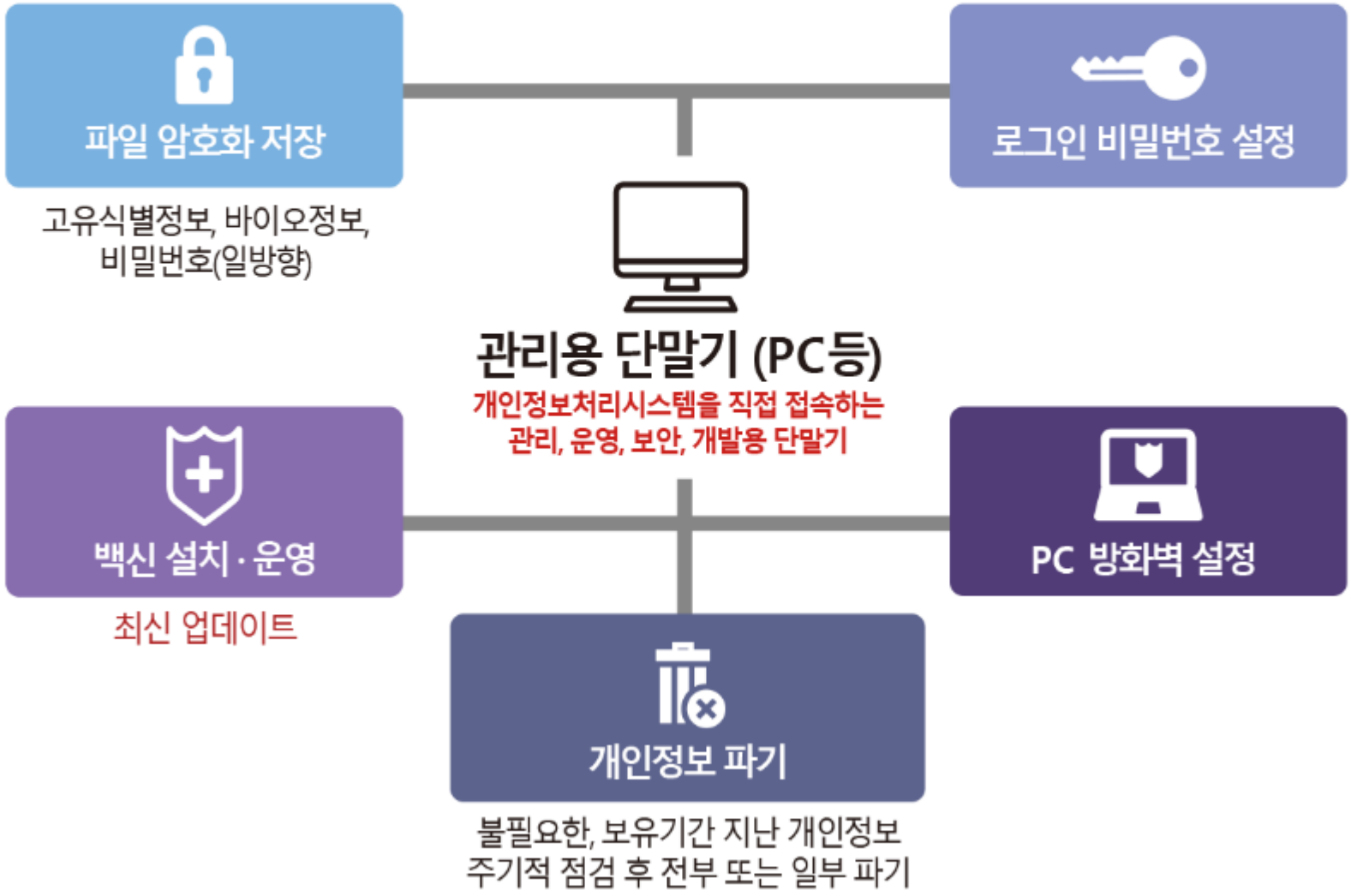
# 4. 모바일 기기 측면


신뢰할 수 있는 무선망 이용
관리자 비밀번호, WPA2 암호화 채널 등이 설정된 무선망 이용, 개인정보 송신시 파일 암호화 조치 등
분실도난으로 인한 유출 방지 보안 설정
업무용 모바일 기기
백신 설치·운영
최신 업데이트
파일 암호화 저장
고유식별정보, 바이오정보, 비밀번호(일방향)
개인정보 파기
불필요한, 보유기간 지난 개인정보 주기적 점검 후 전부 또는 일부 파기

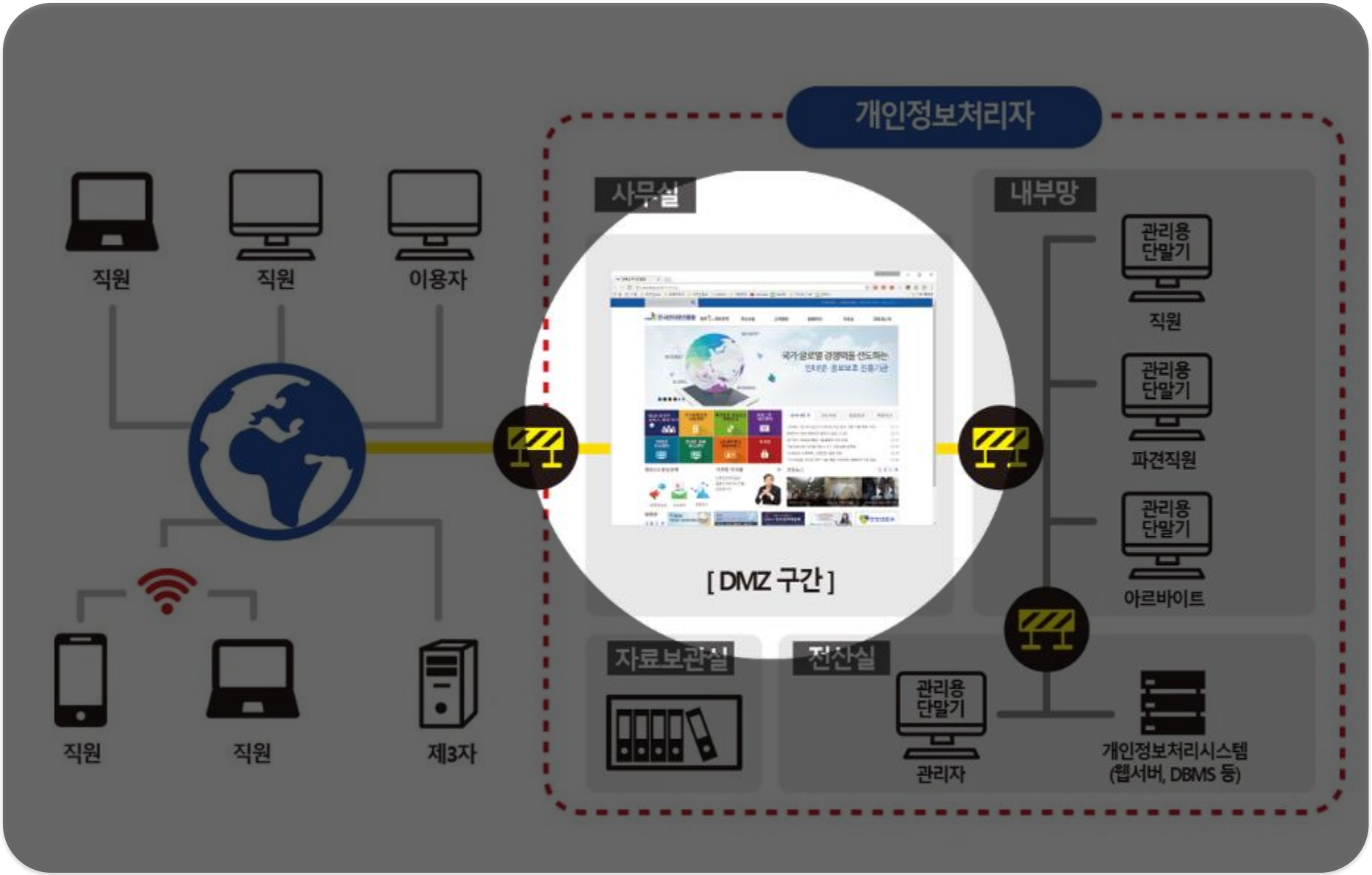
# 5. 관리용 단말기 측면


개인정보처리자
사무실
내부망
직원
직원
이용자
[ DMZ 구간 ]
관리용 단말기
직원
관리용 단말기
파견직원
관리용 단말기
아르바이트
직원
직원
제3자
자료보관실
전산실
관리용 단말기
관리자
개인정보처리시스템
(웹서버, DBMS 등)

# 5. 관리용 단말기 측면


파일 암호화 저장
고유식별정보, 바이오정보,
비밀번호(일방향)
로그인 비밀번호 설정
관리용 단말기 (PC등)
개인정보처리시스템을 직접 접속하는
관리, 운영, 보안, 개발용 단말기
백신 설치·운영
최신 업데이트
PC 방화벽 설정
개인정보 파기
불필요한, 보유기간 지난 개인정보
주기적 점검 후 전부 또는 일부 파기

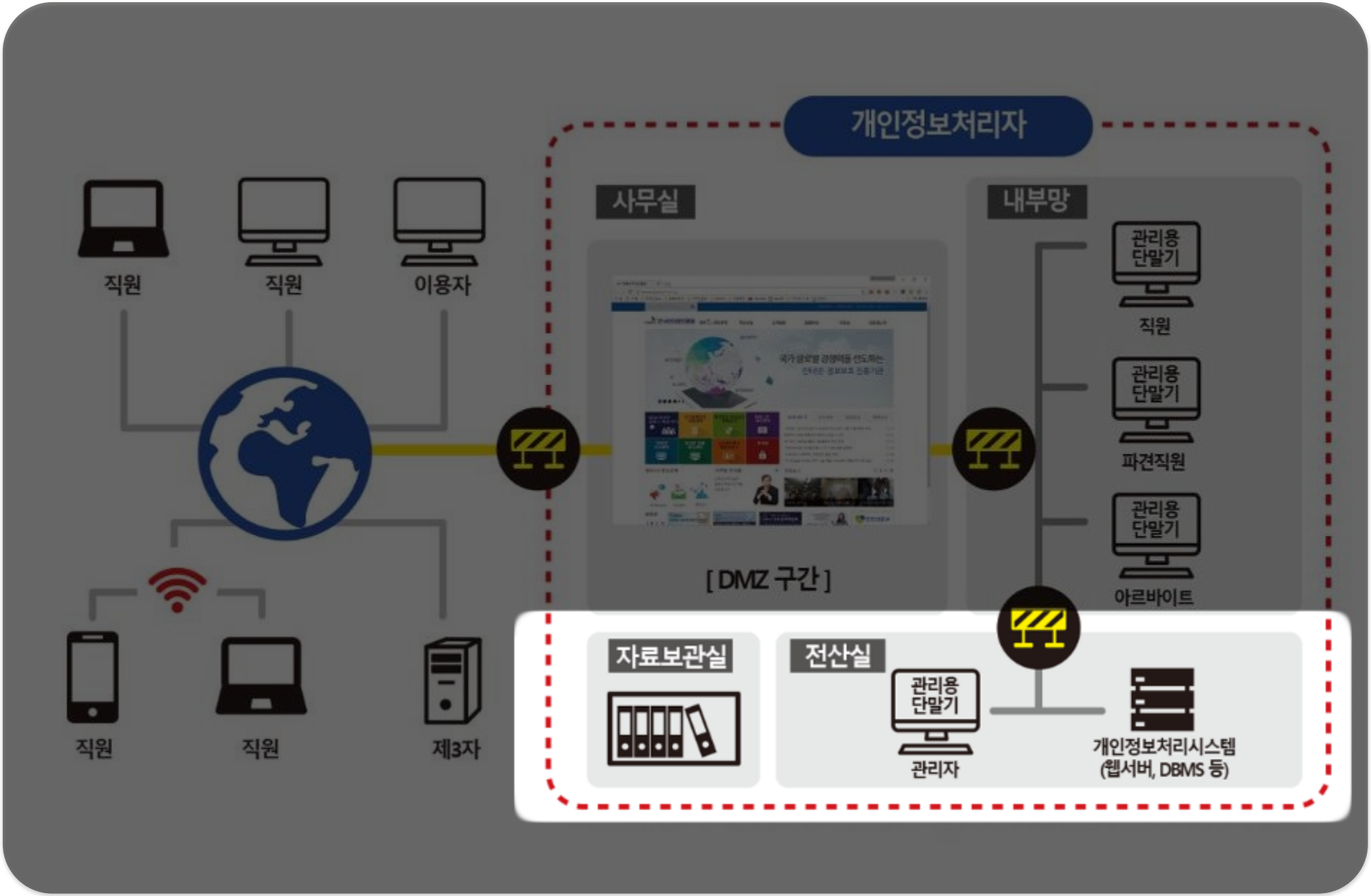
# 6. 홈페이지 측면


개인정보처리자
직원
직원
이용자
사무실
내부망
관리용 단말기
직원
관리용 단말기
파견직원
관리용 단말기
아르바이트
[ DMZ 구간 ]
직원
직원
제3자
자료보관실
전산실
관리용 단말기
관리자
개인정보처리시스템
(웹서버, DBMS 등)

# 6. 홈페이지 측면


- 개인정보 유·노출 방지조치 (홈페이지 Secure Coding, 취약점 점검, 웹 서버 보안설정 등)
- 고유식별정보 처리시, 연 1회 이상 취약점 점검 및 보완조치
- 비밀번호, 바이오정보, 고유식별정보 전송·저장시 암호화
- 비밀번호 작성규칙 수립·운영, 일정시간 이후 자동 로그아웃
- 홈페이지 웹 서버를 개인정보처리시스템으로 활용시
  - 업무별 권한 차등 부여, 변경시 권한 말소, 기록 3년 보관
  - 비인가자 접근통제, 개인정보취급자별 계정 발급
  - 홈페이지에서 직원의 업무처리 기록 6개월 이상 보관 및 반기별 점검
  - 보유기간 경과 개인정보 파기(전부, 일부) 등

# 7. 전산실, IDC, 자료보관실 측면



# 7. 전산실, IDC, 자료보관실 측면

- 출입통제 절차 수립 · 운영
- 서류, 보조저장매체는 잠금장치가 있는 곳에 보관
- 보조저장매체 반 · 출입 통제 보안대책 마련 및 운영
- 보유기간이 경과한 개인정보 파기 (전부 또는 일부 파기 방법 사용)

# [참고] 업무용 PC 개인정보 보호조치 점검도구 신청안내

**소상공인·중소사업자** 등을 대상으로 업무용 PC에 대한 개인정보 보호조치를 자율적으로 수행할 수 있도록 **프로그램 무료 제공**

| 업무용 PC 개인정보 보호조치 점검도구 주요 기능 | |
|---|---|
| 개인정보 암호화 점검 | 업무용 PC 내 개인정보 파일에 포함된 주민등록번호 등 고유식별정보 등 암호화 대상 정보에 대한 암호화 여부 점검 및 조치방법 안내 |
| 비밀번호 관리 | 비밀번호 작성규칙의 적절성, 비밀번호 유효기간 확인 등 점검 및 조치방법 안내 |
| 점근통제 시스템 설치·운영 점검 | 방화벽 설정, P2P·공유설정 여부에 대한 점검 및 조치방법 안내 |
| 보안프로그램 설치·운영 점검 | 백신 등 보안프로그램의 설치 및 업데이트 여부 등 점검 및 조치방법 안내 |

# [참고] 안전조치 기준 적용 유형

| 조 | 항 | 호 | 유형1 (완화) | 유형2 (표준) | 유형3 (강화) |
|---|---|---|---|---|---|
| 제4조 (내부 관리 계획의 수립 시행) | ① 개인정보처리자는 개인정보의 분실, 도난, 유출, 변조, 또는 훼손되지 아니하도록 내부의사 결정절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립시행하여야 한다 | 1. 개인정보 보호책임자의 지정에 관한 사항 | | O | O |
| | | 2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항 | | O | O |
| | | 3. 개인정보취급자에 대한 교육에 관한 사항 | | O | O |
| | | 4. 접근 권한의 권리에 관한 사항 | | O | O |
| | | 5. 접근 통제에 관한 사항 | | O | O |
| | | 6. 개인정보의 암호화 조치에 관한 사항 | | O | O |
| | | 7. 접속기록 보관 및 점검에 관한 사항 | | O | O |
| | | 8. 악성 프로그램 등 방지에 관한 사항 | | O | O |
| | | 9. 물리적 안전조치에 관한 사항 | | O | O |
| | | 10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항 | | O | O |
| | | 11. 개인정보 유출사고 대응 계획 수립시행에 관한 사항 | | O | O |
| | | 12. 위험도, 분석 및 대응방안 마련에 관한 사항 | | | O |
| | | 13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항 | | | O |
| | | 14. 개인정보 처리 업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항 | | | O |
| | | 15. 그 밖에 개인정보 보호를 위하여 필요한 사항 | | O | O |
| | ② [별표]의 유형1에 해당하는 개인정보 처리자는 제1항에 따른 내부 관리계획을 수립하지 아니할 수 있고, [별표]의 유형2에 해당하는 개인정보처리자는 제1항제12호부터 제14호까지를 내부 관리계획에 포함하지 아니할 수 있다. | | | | |
| | ③ 개인정보처리자는 제1항 각호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다. | | | O | O |
| | ④ 개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리 하여야 한다. | | | O | O |

# [참고] 안전조치 기준 적용 유형

| 조 | 항 | 호 | 유형1 (완화) | 유형2 (표준) | 유형3 (강화) |
|---|---|---|---|---|---|
| 제5조 (접근 권한의 관리) | ① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다. | | | O | O |
| | ② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다. | | O | O | O |
| | ③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다. | | O | O | O |
| | ④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우, 개인정보취급자별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. | | O | O | O |
| | ⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다. | | O | O | O |
| | ⑥ 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. | | | O | O |
| | ⑦ [별표]의 유형1에 해당하는 개인정보처리자는 제1항 및 제6항을 아니할 수 있다. | | | | |

# [참고] 안전조치 기준 적용 유형

| 조 | 항 | 호 | 유형1 (완화) | 유형2 (표준) | 유형3 (강화) |
|---|---|---|---|---|---|
| 제6조 (접근통제) | ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고방지를 위해 다음 각호의 기능을 포함한조치를 하여야 한다. | 1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한 | O | O | O |
| | | 2. 개인정보처리시스템에 접속한 IP (Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응 | O | O | O |
| | ② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. | | | O | O |
| | ③ 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. | | O | O | O |
| | ④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다. | | | O | O |
| | ⑤ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다. | | | O | O |
| | ⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근 통제 기능을 이용할 수 있다. | | O | O | O |
| | ⑦ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다. | | O | O | O |
| | ⑧ [별표]의 유형1에 해당하는 개인정보처리자는 제2항, 제4항부터 제5항까지의 조치를 아니할 수 있다. | | | | |

# [참고] 안전조치 기준 적용 유형

| 조 | 항 | 호 | 유형1 (완화) | 유형2 (표준) | 유형3 (강화) |
|---|---|---|---|---|---|
| 제7조 (개인정보의 암호화) | ① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다. | | O | O | O |
| | ② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다. | | O | O | O |
| | ③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다. | | O | O | O |
| | ④ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다. | 1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과 | O | O | O |
| | | 2 암호화 미적용시 위험도 분석에 따른 결과 | O | O | O |
| | 부칙 제2조(적용례) 영 제21조의2제2항에 따른 주민등록번호의 암호화 적용시기 이후에는 고유식별정보 중 주민등록번호는 제7조제4항을 적용하지 아니한다. | | | | |
| | ⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다. | | O | O | O |
| | ⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다. | | | | O |
| | ⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다. | | O | O | O |
| | ⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다. | | | | |

# [참고] 안전조치 기준 적용 유형

| 조 | 항 | 호 | 유형1 (완화) | 유형2 (표준) | 유형3 (강화) |
|---|---|---|---|---|---|
| 제8조 (접속기록의 보관 및 점검) | ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관관리하여야 한다. | | O | O | O |
| | ② 개인정보처리자는 개인정보의 분실. 도난. 유출. 위조. 변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다. | | O | O | O |
| | ③ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다. | | O | O | O |
| 제9조 (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 | O | O | O |
| | | 2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시 | O | O | O |
| | | 3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치 | O | O | O |
| 제10조 (관리용 단말기의 안전조치) | 개인정보처리자는 개인정보 유출 등 개인정보 침해 사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다. | 1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 | O | O | O |
| | | 2. 본래 목적 외로 사용되지 않도록 조치 | O | O | O |
| | | 3. 악성프로그램 감염 방지 등을 위한 보안조치 적용 | O | O | O |

# [참고] 안전조치 기준 적용 유형

| 조 | 항 | 호 | 유형1 (완화) | 유형2 (표준) | 유형3 (강화) |
|---|---|---|---|---|---|
| 제11조 (물리적 안전조치) | ① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립. 운영하여야 한다. | | O | O | O |
| | ② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다. | | O | O | O |
| | ③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출. 입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다. | | O | O | O |
| 제12조 (재해·재난 대비 안전조치) | ① 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다. | | | | O |
| | ② 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다. | | | | O |
| | ③ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제1항부터 제2항까지 조치를 이행하지 아니할 수 있다. | | | | |
| 제13조 (개인정보의 파기) | ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다. | 1. 완전파괴(소각. 파쇄 등) | O | O | O |
| | | 2. 전용 소자장비를 이용하여 삭제 | O | O | O |
| | | 3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행 | O | O | O |
| | ② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다. | 1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독 | O | O | O |
| | | 2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제 | O | O | O |

# [참고] 업무용 PC 개인정보 보호조치 점검도구 신청안내

## 점검도구 신청 대상

- 소상공인(상시종업원 5인 미만)
- 중소사업자(상시종업원 50인 미만 또는 중소기업확인서 등 발급받은 사업자)
- 수익사업을 하지 않는 비영리단체(상시종업원 수 상관없음)

## 점검도구 신청 대상

- ① 개인정보보호 종합포털(www.privacy.go.kr)에서 신청

  ※ 신청 경로 : 종합포털 →사업자→개인정보보호 기술지원→업무용 PC 보호조치 점검도구 신청

- ② 안내메일 확인
- ③ 증빙서류 등 제출(이메일, 팩스, 우편 등)
- ④ 이메일에 점검도구 프로그램 첨부하여 발송

  ※ 증빙서류 접수 후 점검도구 프로그램 발송까지 약 5일 정도 소요

Internet On, Security In !

# 감사합니다