



# PIMS 개인정보 관리체계

**작성자 : Eric Yoon**

# 목 차

- 1. PIMS 란 무엇인지 알아보기
- 2. 개인 정보 등급 분류시 고려해야할 요소
- 3. PDCA 는 무엇 ??
- 4. PIMS 의 인증체계
- 5. PIMS 인증 절차 1~4 단계
- 6. 인증심사 대상
- 7. 관리적, 물리적, 기술적 보호조치 보충설명
- 8. 인증항목 86개 관리과정16, 생명주기20, 보호조치50  
세부항목표 (중요하지 않으니 안봐도됨)

○ 현재 2018 년 11월 경에 ISMS인증과 PIMS인증이 합쳐져서 새로운 ISMS- P 인증이 통합되서 발표 된다고는 하지만, 현재는 통합전이기때문에 이제도를 따르고 있습니다. 차후에 통합이 되어도 기본적인틀은 크게 바뀌지 않을 것이기에 학습에 문제는 없을것입니다.

○ 보안기사나 cppg 등 많은 문제에도 출제가 되고있어, 정확히 짚어 학습 하고자 준비를 하였습니다. 부족하지만, 열심히 학습 하셔서 좋은 결과가 있길 바라며, 잘못된 부분에대해 피드백 주시면 즉시 수정 하도록 하겠습니다

○ 한국인터넷진흥원 KISA 의 자료를 참고하여 작성 하였습니다.

# PIMS 란 무엇인가요 ?

## 인증제도

- 기관 및 기업이 개인정보보호 관리체계를 갖추고 체계적·지속적으로 보호 업무를 수행하는지에 대해 객관적으로 심사하여 기준 만족 시 인증 부여
- 기대효과
- 개인정보보호 관리체계 구축을 통해 기업이 보유하고 있는 개인정보를 안전하게 관리하고 인증 기업의 대외 신뢰도 향상에 기여
- **PIMS 법적근거**
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조의 3
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제54조의 2
- 개인정보 보호법 제32조의 2
- 개인정보 보호법 시행령 제 34조의 2~제 34조의 8
- 개인정보보호 관리체계 인증 등에 관한 고시

# PIMS 란 무엇인가요 ?

## ○ 인증대상

- 개인정보보호 활동을 체계적이고 지속적으로 수행하기 위하여 필요한 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 개인정보 수집·취급 사업자

## ○ 인증심사 기준

- 인증기준은 국내·외의 표준과 '개인정보 보호법', '정보통신망 이용촉진 및 정보보호 등에 관한 법률', 국내환경을 고려하여 개발
- 개인정보 유관 컴플라이언스 대응을 위한 최소 구현 사항, 법적 준거성, 체계적 운영 측면을 보완  
개인정보보호 관련 조직 및 담당자가 해야 할 실제 활용 부분을 강조

# 개인정보 등급 분류시 고려할 요소

## 1. 개인정보 영향도 등급

자산가치	5점	1등급	비밀	주민번호, 신용카드정보, 금융정보, I D, 비밀번호, 지문, 홍채정보, 등등
자산가치	3점	2등급	대외비(조합정보)	성명+전화번호+주소+e-mail, 성명+생년월일+e-mail,.
자산가치	1점	3등급	대외비(식별어려운정보)	몸무게+키 , 주소, 학력

- 2. 법적통제 요구사항
- 3. 유출시 위험성 및 파급 영향
- 4. 정보 민감도
- 5. 정보의 고유성 및 식별성

## PDCA 사이클기반

- PDCA 가 무엇인지 짚고 넘어 가보자.
- Plan,Do,Check,Act 의 반복 사이클 로써,  
지속적이고 반복적인 개선 활동을 요구한다.
- 개인정보 보호 관리과정 이다
- 조직구성,위험관리,모니터링감사,정책
- 1.계획plan (①.정책수립,관리범위정함 ②.관리범위내의개인정보자산식별 ③.개인정보흐름파악및 흐름도 작성 ④.개인정보처리상에 문제점 파악.)
- 2.실행do (①.식별된 정보자산을 바탕으로 위험평가 실시 ②.정보보호대책의 수립과 이행)
- 3.검증check (①.정보보호대책의 효과성확인 ②.모니터링 정기적인점검,감사실시등으로 체크)
- 4. 개선 act (잔여 위험에 대한 추가적인 조치사항 반영 )**반영=순환 PDCA**

# PIMS 인증심사 기준

## PIMS 구성요소

### 관리과정 요구사항

관리체계 수립 (정책, 범위, 조직 등)
실행 및 운영 (개인정보 식별, 위험관리, 구현 등)
검토 및 모니터링 (사후관리)
교정 및 개선 (개선활동, 교육)

### 생명주기 및 권리보장 요구사항

생명주기 관리 (수집, 이용 및 제공, 보유, 파기)
정보주체 권리보장

### 보호대책 요구사항

관리적 (인적, 침해사고)
기술적 (접근권한, 접근통제, 운영보안, 암호화, 개발보안)
물리적 (영상정보처리기기, 물리적 보안, 매체)

- 총 86 개 항목
- 관리과정 (16)
- 생명주기 및 권리보장 (20)
- 보호대책 요구사항(50)
- 기업자율제도 이지만 인증획득후 차후 개인정보관련 과징금시 경감혜택 있음-100분의 50 까지!

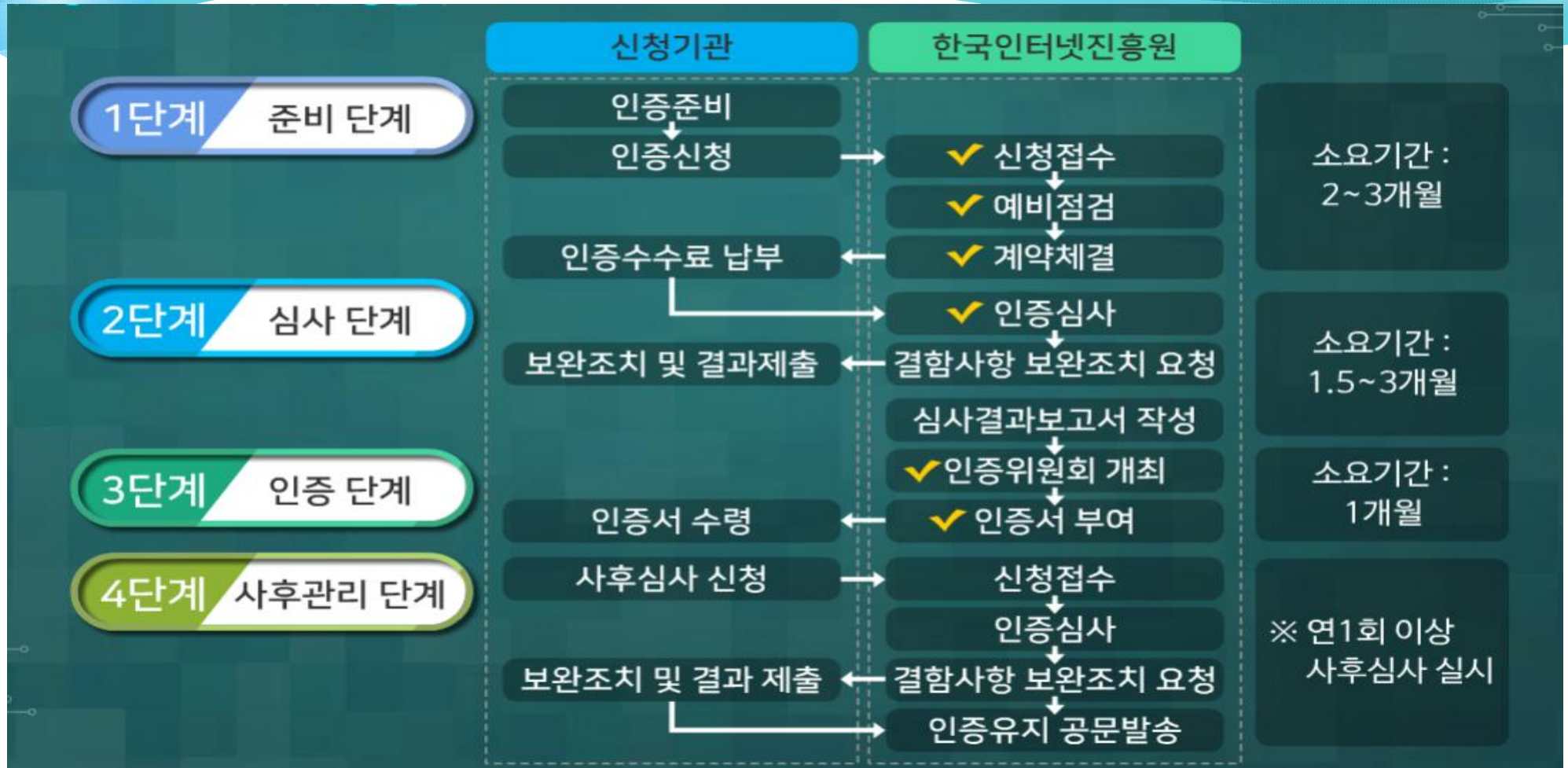


## ■ 인증체계



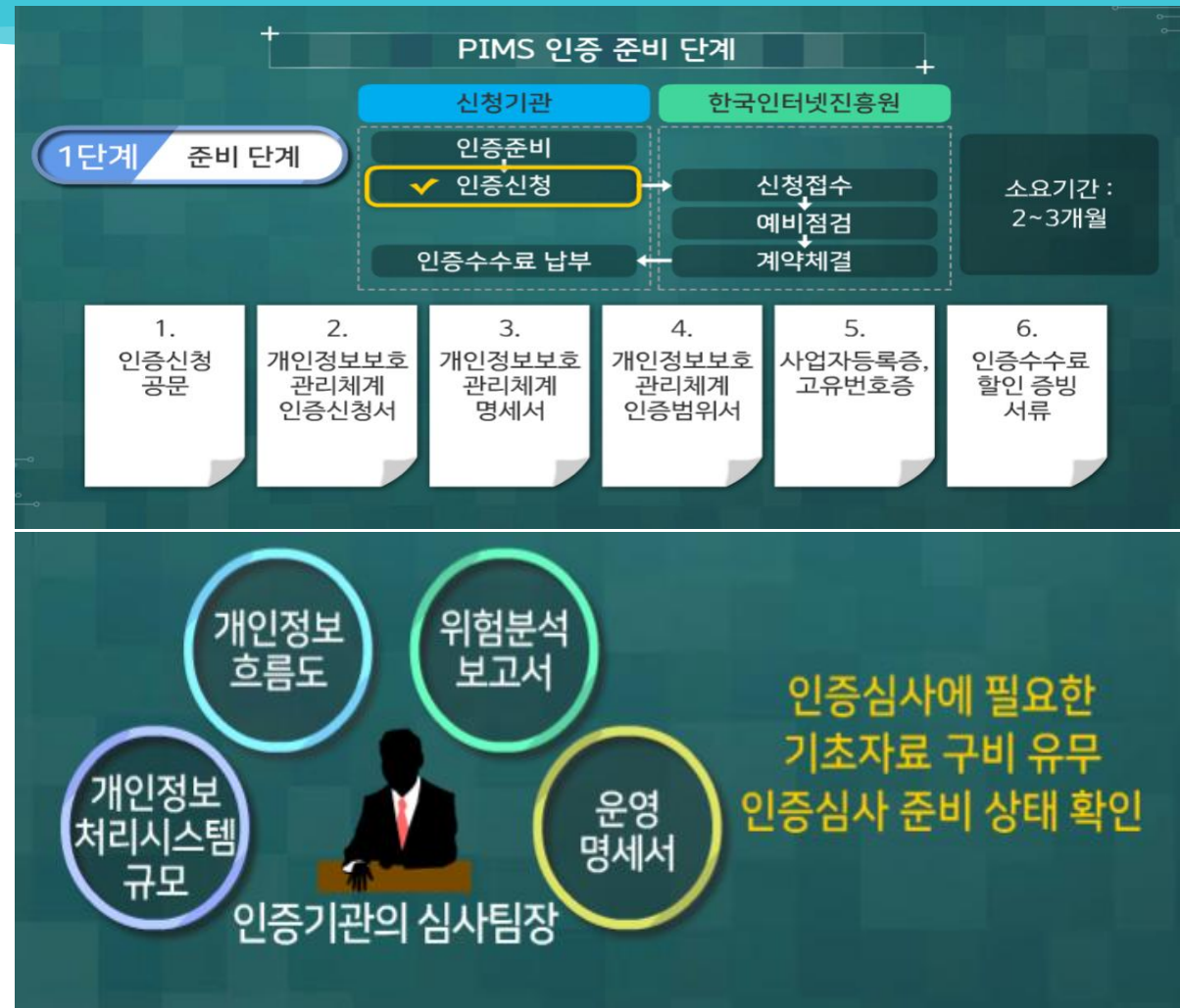
- 인증제도의 객관성 및 신뢰성 확보를 위해 정책기관, 인증기관, 인증위원회를 분리하여 운영
- 인증제도를 관리·감독하는 정책기관은 행정안전부/방송통신위원회가 직접수행
- 한국인터넷진흥원은 인증기관으로서 인증 제도 운영
- 산업계, 학계 등 관련 전문가 10명 이내로 인증위원회를 구성하여 인증결과 심의
- 인증심사팀은 인증심사원 양성교육을 수료하고, 자격 요건을 갖춘 자들로 구성

# 각각 인증 절차를 한번 보자



# 인증절차 1단계 - 준비단계

- 1. 준비 단계에서는 신청접수할 서류를 주목하자
- 2. 그후에 예비점검이 있는데 인증기관의 심사 팀장이 신청기관을 방문 하여 개인정보시스템규모,개인정보 흐름도,위험분석보고서,운영명세서등 기초자료를 확인한다.





## 1-1. 인증 신청 제출 서류 꼭 암기하자

### 인증 신청 제출 서류

1.  
개인정보보호  
관리체계  
인증신청서

2.  
개인정보보호  
관리체계  
명세서

3.  
사업자등록증,  
고유번호증

4.  
중소기업·  
소상공인  
증빙서류  
(해당 사업자)

- 개인정보보호 관리체계 명세서
- 개인정보처리시스템 및 관련 주요 정보통신설비(개인정보 처리 관련 정보자산 등)의 목록과 시스템 구성도
- 개인정보보호 관리체계 수립운영 방법 및 절차
- 개인정보보호 관리체계 관련 주요 문서 목록
- 국내외 품질경영체제 인증서 취득 명세서
- [별지] 개인정보보호 관리체계 운영명세서

# 이때 예비점검에 필요한 구비자료 목록

## 예비점검에 필요한 준비자료

※ 신청기관은 인증심사 예비점검 시 다음의 증적을 준비해야 한다.

- 상위 규정 및 정책(방침)서, 개인정보보호 정책/지침/절차서/메뉴얼
- 개인정보보호 관리체계 인증범위서, 개인정보 관련 자산목록, 위험분석보고서, 취약점 분석 결과 보고서
- 개인정보보호계획서, 직무기술서, 내부심사 결과 등 각종 계획서 및 보고서
- 각종 점검 및 관리대장 등 이행증적 자료
- 개인정보보호 관리체계 명세서
- 개인정보 흐름도
- 업무관련 조직도, 심사지원 담당자 연락처 등 기타 관련 문서

○ 이때 개인정보 흐름도는 반드시 신청접수 서류에 포함하지 않아도 된다 .!!!!

○ 심사위원이 심사할당시 현장 방문시 에 제출해도 된다

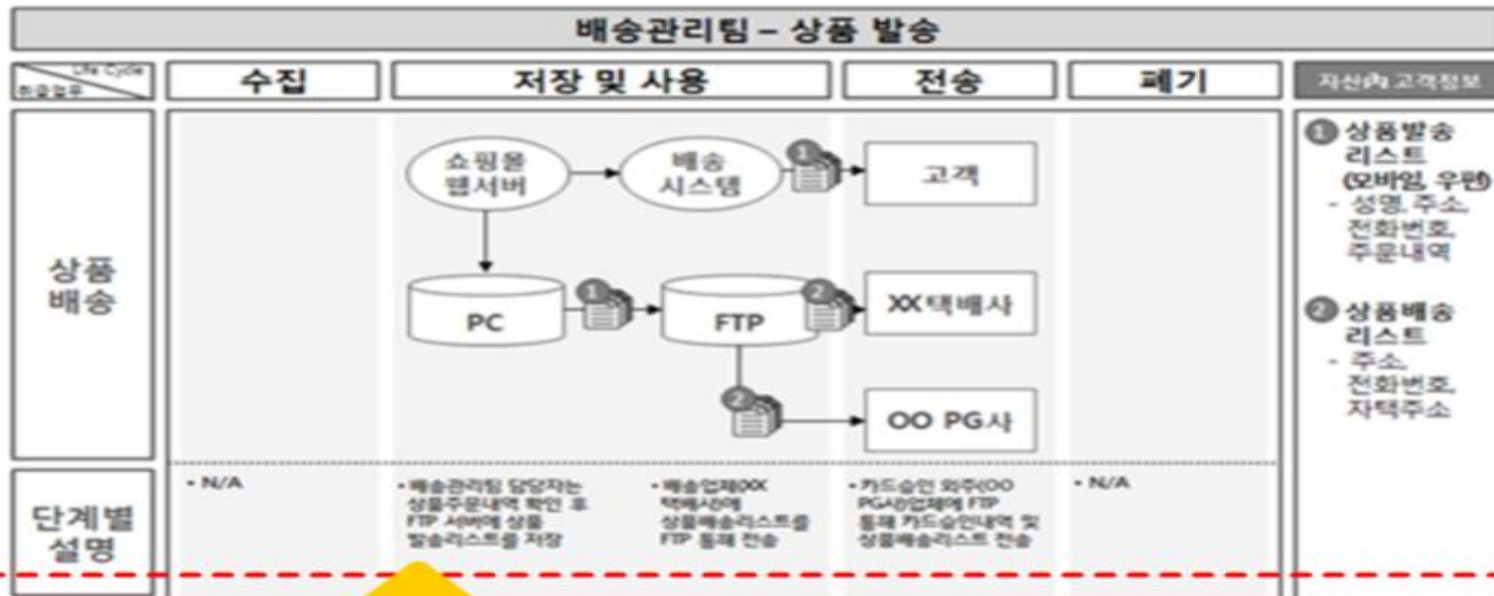
♥ 유형1 소상 공인의 경우 흐름도 작성 제외 !!

★ PIMS 인증 신청당시 최소 2월 이상 PIMS 를 구축 운영한적이 있어야한다

# 흐름도 예시

## 개인정보보호 관리체계 명세서

서비스 중 특정 업무의 개인정보 흐름도(업무별 흐름분석) 작성 예시



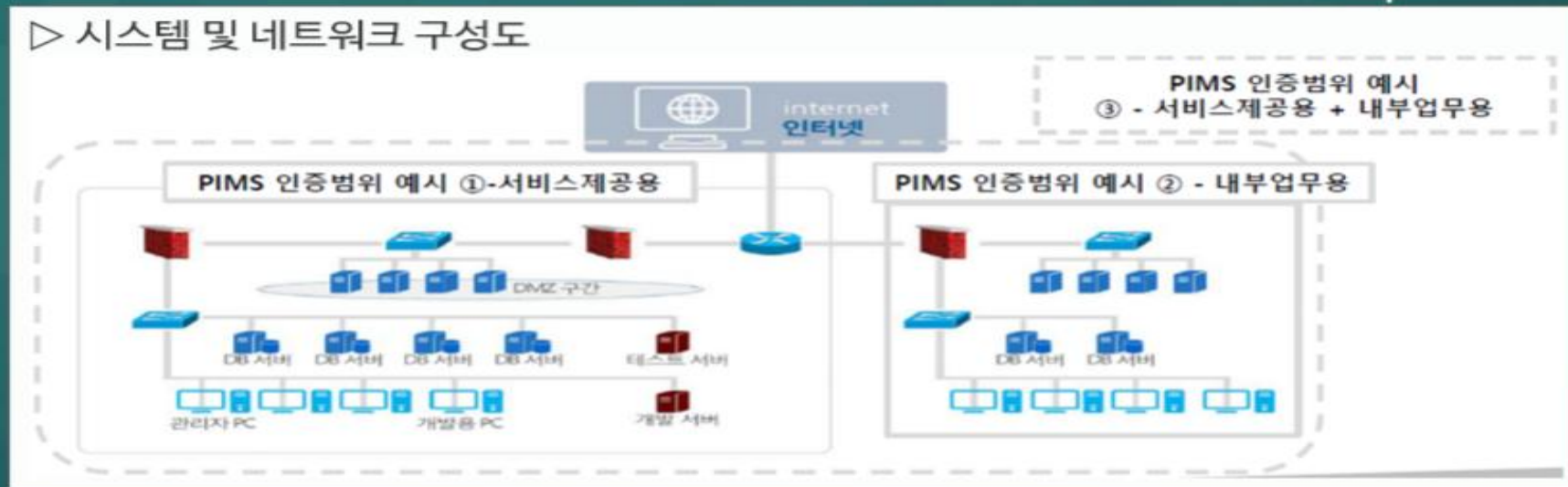
서비스 중 특정 업무의 개인정보 흐름을 파악할 수 있는 개인정보 취급업무별 개인정보 흐름도 작성



# 네트워크 구성도 예시

## 개인정보보호 관리체계 명세서

### ▷ 시스템 및 네트워크 구성도



- 인증 범위 서비스를 운영하는 **시스템을 중심으로 작성**(DB서버, 웹서버, 로그모니터링 시스템 등)
- IDC 및 물리적으로 구분된 경우 해당 사항과 시스템간의 네트워크 연결 명시
- **인증범위 서비스를 연결하는 네트워크 구성도를 작성할 때**  
네트워크 장비, 정보보호 관련 장비 및 DMZ 구간, VPN 구간 등 외부 연결 구간 표시
- 구성도에 네트워크와 시스템이 모두 표기되도록 작성, **인증심사 신청 시의 구성도를 현행화하여 표기**

## 인증절차 2단계 심사 단계

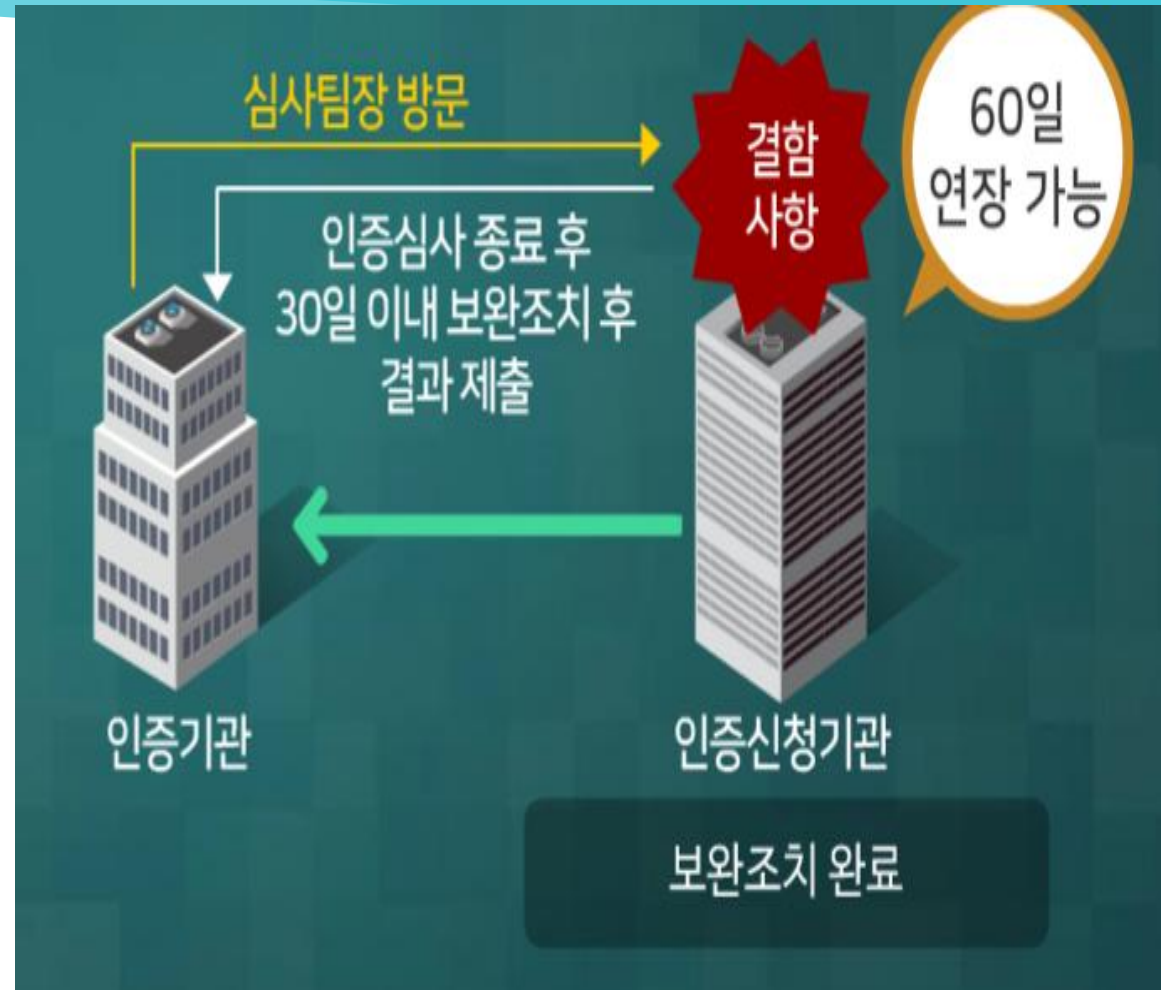


- 심사단계에서는 다음의 5가지의 순서로 진행된다.



## 인증절차 2단계 심사 단계

- 심사결과 결함사항이 발견시
- 심사종료 30일 이내에 보완조치를 한후 결과를 제출하여야한다.
- 만약 30일이 어려우면 60일 연장이 가능하다. ( 기간연장 서식에 따라 작성 해야됨, 구두상으로 불가 )=총90일.
- 이때 심사팀장이 재방문하여 조치여부를 확인한다.



## 인증절차 3단계 심사 단계

- 2단계의 심사단계를 거치면
- 인증위원회 에 결과를 보고 하고 심의 의결 결과 보완조치 확인,인증적합여부를 판단후 인증서를 발급 하게 된다.
- 신청기관은 인증기간동안 개인정보보호 관리체계를 유지해야한다.

## 인증절차 4단계 사후관리 단계



유효기간은 3년이며 매심사를 받지않을 경우  
인증 효력을 상실하게 된다.

◇인증 효력을 위해 매년 받아야 하는 것은 **사후 심사** 다  
갱신심사 아님 !!X

# PIMS 인증심사 대상

유형	관련근거
공공기관	<ul style="list-style-type: none"> <li>-[개인정보보호법]제2조6호에 따른 공공기관에 해당하는 개인정보처리자</li> <li>-국회,법원,헌법재판소,중앙선거관리위원회</li> <li>-중앙행정기관 및 그 소속기관</li> <li>-지방자치단체,지방공사및 지방공단</li> <li>-국가인권위원회,공공기관,각급학교</li> </ul>
대기업/정보통신 서비스 제공자	<ul style="list-style-type: none"> <li>-[대.중소기업 상생협력 촉진에 관한 법률]제2조2호에따른 대기업에 해당하는 사업자</li> <li>-[정보통신망 이용촉진및 정보보호 등에 관한 법률] 제2조3호에 따른 정보통신 제공자</li> </ul>
중소기업	<ul style="list-style-type: none"> <li>-[중소기업법]제2조에따른 중소기업에 해당하는 사업자</li> <li>1.다음각목의 요건을 모두 갖추고 영리를 목적으로 사업을 하는기업</li> <li>-업종별로 매출액 또는 자산총액 등이 대통령령으로 정하는 기준에 맞을것</li> <li>-지분소유나 출자관계등 소유와 경영의 실질적인 독립성이 대통령령으로 정하는 기준에 맞을것</li> <li>2.[사회적기업 육성법]제2조1호에 따른 사회적기업 중에서 대통령령으로 정하는 사회적 기억</li> <li>3.[협동조합 기본법]제2조1호에따른 협동조합중 대통령령으로 정하는 협동조합</li> <li>4.[협동조합기본법]제2조2호에따른 협동조합연합회 중 대통령령으로 정하는 협동조합연합회</li> </ul>
소상공인	<ul style="list-style-type: none"> <li>[소상공인 보호및 지원에 관한 법률]제2조1호및 2호에 따른 소상공인에 해당하는 사업자 및 그밖의 사업자 예시</li> <li>-상시 근로자 수가 10명 미만일것</li> <li>-광업,제조업,건설업,운수업=10명 미만</li> <li>-그밖의 업종=5명 미만</li> </ul>

# 구성요소 다시 확인 ! 관리적, 물리적, 기술적 보호대책 !!! 필수 !! 학습 하자 !!!

## PIMS 구성요소

### 관리과정 요구사항

관리체계 수립 (정책, 범위, 조직 등)
실행 및 운영 (개인정보 식별, 위험관리, 구현 등)
검토 및 모니터링 (사후관리)
교정 및 개선 (개선활동, 교육)

### 생명주기 및 권리보장 요구사항

생명주기 관리 (수집, 이용 및 제공, 보유, 파기)
정보주체 권리보장

### 보호대책 요구사항

관리적 (인적, 침해사고)
기술적 (접근권한, 접근통제, 운영보안, 암호화, 개발보안)
물리적 (영상정보처리기기, 물리적 보안, 매체)

- 지금껏 PIMS 의 절차 및 구성요소 86개를 확인했다.
- 다시 한번 보도록하자.
- 알고보면 보이고 모르고 보면 안보이기때문에 다시 보고 또 보도록 하자
- 보호대책 요구사항 (관리적, 기술적, 물리적 ) 이부분은 무려 50개의 심사항목이 있다 . 86개중 50개면 상당수다... 그만큼 중요하다.
- 보안인이라면 꼭 알아야될 보호대책 다시 짚어보자.

## 관리적 보호조치 는 무엇인가 ?

1. 교육 및 훈련 - 최소 연 1회 이상 !
2. 개인정보 취급자 관리-취급자 감독, 보안서약서, 퇴직자 등 직무변경관리
3. 위탁업무관리 및 침해사고관리-  
외부위탁계약, 정부주체고지. 위탁자관리감독  
(위탁계약서에 반드시 포함할 사항이 아닌것은 ?  
수탁자가 접근가능한 개인정보의 범위 및 유형은 반드시  
계약서에 포함하지 않아도 된다.)-시험문제 자주출제됨.
4. 침해사고관리- 침해사고 대응절차 및 체계구축, 침해사고  
훈련개선, 대응

## 물리적 보호조치 는 무엇인가 ?

- 1. 물리적 보안 – 보호구역지정 및 관리, 보호설비 설치, 출입 통제 등...
- 2. 영상 정보 처리기기 관리
- 3. 매체 관리- 저장매체파기, 재사용시....-데이터 복구 안되도록...



## 기술적 보호조치 는 무엇인가 ?

♡ 개인정보 처리시스템과 관련 시스템의 계정과 권한은 필요한 사람에게 최소한으로 부여 되어야하며, 권한부여 이력은 일정 기간 보관 - 개보3년, 망5년

♡ 개인정보 처리시스템 접속기록은 법령에 따라 일정기간 이상 보관하여야 하며 , 권한 없는자의 접근시도, 권한의 오남용, 시스템 오류등을 적발하기 위하여 주기적으로 접속 기록을 검토 하여야함.

♡ 계정의 비밀번호를 안전하게 관리 하기 위한 기준을 마련하여 이행하여야 하며 , 필요한경우 개인정보 취급자의 단말을 망분리 해야함.



# 기술적 보호조치 는 무엇인가 ?

♥망법에서 망분리대상자는

- 개인정보 처리시스템으로 부터 다운로드할수 있는 권한을 보유한자
- 개인정보처리시스템을 이용하는 개인정보 취급자의 권한을부여,변경할수 있는자
- 개인정보 처리시스템에 저장된 개인정보를 삭제할수 있는자

♥개인정보 처리업무에 사용하는 단말과 시스템은 악성코드감염에 수행해야하며,시스템과 단말기 보호를 위해 필요한 보안 시스템을 구축하여 운영해야함.

♥개인정보 처리시스템과 관련 시스템을 개발하는 경우 개발 보안 요구사항정의,개발과,운영환경의분리,실데이터의 테스트 환경사용금지,외주개발시 용역업체관리등의 사항을 준수하여야함.

# 기술적 보호조치 는 무엇인가 ?

## ○ 1. 접근통제

- 문서로 공식화 , - 인사이동에 따른 권한변경보관-개보법3년,망법 5년 - 비밀번호관리 , -접속기록,-전자적기록, 수기문서 X
- 철저한 네트워크 관리 - 물리적,논리적 분리

## ○ ①. 분리운영

- 외부접근가능한서버 =DMZ망
- DB서버들은 내부망
- 내부망도 DB서는 가급적 별도의 네트워크로구분
- 개발,테스트 서버등 별도 분리
- 내부망은 가급적 사설 ip 사용

## ○ ②. 원격접속관리 -VPN

- 개인정보처리시스템을 외부에서 접속하여 사용하는 경우 전용선,vpn 등 사용하여 통제
- Vpn 사용시 추가 인증수단, 단말기 보안등을 고려
- ♥-개보법vpn = 안전한접속수단=암호화통신방법
- 망법vpn=안전한 인증수단=otp,ip주소인증등

## ○ ③.무선 네트워크 사용

- 내부용,외부용(guest용) 구분
- 비밀번호 설정 ssid 숨김 등으로 내부 메의 외부노출 최소화
- 응용 프로그램 (- 계정관리처럼 권한제한및 관리 , 멀티 로그인금지 , 세션종료시간 설정등의 보안 대책 마련 )
- 데이터 베이스 관리
- 개인정보 망분리

# 기술적 보호조치 는 무엇인가 ?

## ○ 2. 운영보안

- 악성코드통제
- 취약점 점검
- 표시제한,마스킹, -비식별
- 보안시스템운영
- 노트북,모바일기기 접근관리
- 기타 운영보안-백업,복구

# 기술적 보호조치 는 무엇인가 ?

## 3. 암호화 및 개발보안등

- 암호정책 수립및 이행.
- 알고리즘 - ① 일방향암호화 -sha256 이상의 안전성 가진 방법 추천  
**(비밀번호 !! 무조건 일방향 !!!)** sha 중에서도 80 비트 는 전혀 권장사항 아님!!! 유효기간도 만료됨 !! 128 비트 이상 사용 할것 !!
  - ② 양방향암호화-aes128 알고리즘 등 권고
- 암호키 = 안전한곳 보관
- 개인정보 개발,유지보수

## 다음은 각 심사항목 세부사항 점검표이다.

- PIMS 심사항목 총 86개 이다

- 관리과정 16개
- 생명주기 및 권리보장 20개
- 개인정보 보호대책 50 개
- 이것만 기억하자.
- 다음장은 관련 업무를 하지않는 이상 지나치게 불필요한 내용입니다.
- 여기서 종료 하셔도 됩니다. ^^

# 개인 정보 관리 과정 -16개 세부 항목

인증기준				상세내용	적용 유형				세부점검항목
					유형4	유형3	유형2	유형1	
		1.1.1	정책의 수립	개인정보보호정책과 시행문서를 수립하여 조직의 개인정보보호 방침과 방향을 명확하게 제시하여야 한다. 또한, 개인정보보호(관리)책임자 등 경영진의 승인을 받고 임직원 및 관련자에게 공표하여야 한다.	○	○	○	○	<p>조직이 수행하는 모든 개인정보보호 활동의 근거를 포함하는 최상위 수준의 개인정보보호정책을 마련하였는가?</p> <p>개인정보보호정책의 시행을 위하여 필요한 세부적인 방법, 절차, 주기 등을 규정한 개인정보보호 지침, 절차, 매뉴얼 등을 수립하고 있는가?</p> <p>개인정보의 기술적, 관리적 및 물리적 보호조치 등의 세부 사항이 포함된 내부관리계획을 수립하고 있는가?</p> <p>개인정보보호정책 및 시행문서(지침, 절차 등)는 조직이 제공하고 있는 사업 등에 관련된 개인정보 보호 관련 법적 요구사항(법률, 시행령, 시행규칙, 하위 고시, 가이드)을 반영하고 있는가?</p> <p>개인정보보호정책 및 시행문서의 제·개정 시 이해 관계자의 검토를 받고 있는가?</p> <p>개인정보보호정책 제·개정 시 최고경영자의 승인을 받고 있는가?</p> <p>개인정보보호정책 및 시행문서의 제·개정 시 그 내용을 관련 임직원에게 공표하고 있는가?</p> <p>개인정보보호정책 및 시행문서를 관련 임직원에게 이해하기 쉬운 형태로 전달하고 최신본으로 제공하고 있는가?</p>

1.1	정책 및 범위	1.1.2	정책의 유지관리	개인정보보호정책 및 시행문서는 관련 법·규제를 준수하고, 상위 정책과 일관성을 유지하여야 한다. 또한, 정기적으로 검토하여 필요한 경우 제·개정 및 이력관리하고 운영기록을 생성·유지하여야 한다.	○	○	○	<p>개인정보보호정책 및 시행문서의 타당성 검토 절차를 수립하고 있으며, 정기적으로 검토하고 있는가?</p> <p>- 개인정보보호정책과 상위 조직 및 관련기관 정책의 일관성</p> <p>- 개인정보보호정책과 시행문서간 일관성</p> <p>관련 법규의 변화, 중대한 보안사고 발생, 새로운 위협 또는 취약성의 발견, 시스템 환경에 중대한 변화 등의 경우, 개인정보보호정책 및 시행 문서에 미치는 영향을 검토하여 제·개정하고 있는가?</p> <p>개인정보보호정책 및 시행문서의 제정, 개정, 배포, 폐기 등의 이력을 확인할 수 있도록 관리·관리를 수립·이행하고 있는가?</p> <p>개인정보보호정책 및 시행문서에서 정한 개인정보보호 활동 수행에 관한 운영 내역을 기록·관리하고 있는가?</p>
		1.1.3	범위설정	조직에 미치는 영향을 고려하여 중요한 업무, 서비스, 조직, 자산 등을 포함하는 개인정보보호 관리체계 범위를 설정하여야 한다.	○	○	○	<p>조직의 사업(서비스)을 위한 개인정보 처리에 영향을 줄 수 있는 핵심자산을 포함하도록 범위를 설정하고 있는가?</p> <p>개인정보보호 관리체계 범위를 설명하기 위하여 다음과 같은 내용이 포함된 문서를 작성하여 관리하고 있는가?</p> <p>- 주요 서비스 및 업무 현황</p> <p>- 서비스 제공과 관련된 조직</p> <p>- 개인정보보호 조직, 주요 설비 목록</p> <p>- 정보시스템 목록 및 네트워크 구성도</p> <p>- 개인정보 관련 자산식별 기준</p> <p>- 개인정보 흐름 파악(수집, 이용, 제공, 저장, 관리, 파기)</p> <p>- 인증 범위 내의 위험분석, 취약점 점검</p> <p>- 문서 목록 (예 : 정책, 지침, 매뉴얼, 대책 명세서 등)</p> <p>- 개인정보보호 관리체계 수립 방법 및 절차</p> <p>- 개인정보보호 관련 법적 준거성 검토, 내부감사</p> <p>- 고객센터 등 외주(위탁)업체 현황 등</p> <p>정의된 범위 내에서 예외사항이 있을 경우 명확한 이유 및 관련자 협의·승인 등 관련 근거를 관리하고 있는가?</p>



1.2	경영진의 책임	1.2.1	경영진의 참여	개인정보보호 관리체계 수립 및 운영 등 조직이 수행하는 개인정보보호 활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여야 한다.	○	○			개인정보 보호책임자를 포함한 경영진이 개인정보 보호활동에 관한 의사결정에 적극적으로 참여할 수 있는 보고, 검토 및 승인 절차를 수립·이행하고 있는가?
									개인정보 보호책임자를 포함한 경영진이 개인정보보호 활동에 관한 의사결정에 참여하고 있는가?
1.3	조직	1.3.1	개인정보보호(관리)책임자의 지정	지속적인 개인정보보호 관리체계 운영 활동을 위하여 개인정보보호(관리)책임자를 지정하여야 한다.	○	○	○	○	최고경영자는 개인정보 처리에 관한 업무를 총괄하여 책임질 개인정보 보호책임자를 공식적으로 지정하고 있는가?
									지정된 개인정보 보호책임자는 법령에 따른 자격 요건을 충족하는가?
		1.3.2	조직의 구성	조직 전반의 중요한 개인정보보호 관련 사항을 검토 및 의사결정할 수 있는 조직(협의체)을 구성하여야 한다. 또한 개인정보보호 관리체계 운영 활동을 수행하는데 필요한 자원(예산 및 인력)을 확보하여야 한다.	○	○	○		조직의 규모, 업무 중요도 등의 특성을 고려하여 개인정보보호 관리체계 구축·운영 활동을 지속적으로 수행할 수 있는 개인정보보호 조직(CPO, 실무조직, 개인정보보호위원회 등)을 구성하고 있는가?
									전사 개인정보보호 정책 등을 의사결정할 수 있는 기구의 조직 구성, 운영, 역할 및 책임 등을 규정하고 이에 따라 이행하고 있는가?
									최고경영자는 개인정보 보호책임자 역할을 지원하고 조직의 개인정보보호활동을 체계적으로 수행하기 위한 실무조직을 구성하여 운영하고 있는가?
									최고경영자는 개인정보보호 관리체계 구축·운영에 소요되는 자원을 평가하여 필요한 예산과 인력을 지원하고 있는가?





2. 실행 및 운영			2.1.2	개인정보 흐름 파악	조직의 개인정보 관련 서비스 및 업무에서 개인정보 흐름을 파악하여 개인정보 흐름도(표)를 작성하고 이를 주기적으로 검토하여 최신성을 유지하여야 한다.	○	○	○	개인정보 처리업무 식별, 개인정보 처리업무별 수집·저장·이용·제공·파기의 경로, 취급 상의 개인정보 흐름(관련 시스템, 취급자, 연계 인터페이스 포함)을 파악하고 개인정보 흐름도(표)를 작성하였는가?
									서비스 및 업무, 개인정보 자산 등의 변화에 따른 개인정보 취급 상의 흐름을 주기적으로 분석하여 필요시 재작성하는 등 개인정보 흐름도(표)의 최신성을 유지하고 있는가?
	2.2	위험관리	2.2.1	위험관리 방법 및 계획 수립	조직의 개인정보보호 전 영역에 대하여 위험식별 및 평가가 가능하도록 위험관리 방법을 선정하고 위험관리계획을 수립하여야 한다.	○	○	○	개인정보보호를 위한 다양한 측면에서 발생할 수 있는 위험을 식별하고 평가할 수 있는 방법을 정의하여 문서화하고 있는가?
									수행인력, 기간, 대상, 방법, 예산 등을 구체화한 위험관리계획을 수립하고 있는가?
			2.2.2	위험식별 및 평가	위험관리 방법 및 계획에 따라 위험 식별 및 평가를 연 1회 이상 수행하고 그 결과에 따라 조직에서 수용 가능한 위험 수준을 설정하여 관리하여야 한다.	○	○	○	개인정보보호 관리체계 범위 전 영역에 대한 위험식별 및 평가를 연 1회 이상 수행하고 결과를 경영진에게 보고하고 있는가?
									조직에서 수용 가능한 목표 위험수준을 정하고 그 수준을 초과하는 위험을 식별하고 있는가?
			2.2.3	이행계획 수립 및 보호대책 구현	위험을 수용 가능한 수준으로 감소시키기 위해 개인정보보호대책을 선정하고 이행계획을 수립하여 경영진의 승인을 받아야 한다. 또한, 수립된 이행계획에 따라 보호대책을 구현하여야 한다.	○	○	○	식별된 위험에 대한 처리 전략(감소, 회피, 전가, 수용 등)을 수립하고 위험처리를 위한 개인정보보호대책을 선정하였는가?
									개인정보보호대책의 우선순위를 고려하여 일정, 담당부서 및 담당자, 예산 등의 항목을 포함한 개인정보보호대책 이행계획을 수립하고, 개인정보 보호책임자 등 경영진에 보고하고 있는가?
	이행계획에 따라 개인정보보호대책을 구현하고 그 이행결과를 개인정보 보호책임자 등 경영진에게 보고하고 있는가?								

3. 검토 및 모니터링	3.1	개인정보 보호체계의 검토	3.1.1	법적요구사항 준수검토	조직이 준수해야 할 개인정보보호 관련 법적 요구 사항을 지속적으로 파악하여 최신성을 유지하고 준수여부를 지속적으로 검토하여야 한다.	○	○	○	조직이 준수해야 하는 개인정보보호 관련 법적 요구사항을 파악하여 최신성을 유지하고 있는가?	
			법적 요구사항의 준수여부를 연 1회 이상 주기적으로 검토하고 있는가?							
			3.1.2	내부 감사	개인정보보호 관리체계가 효과적으로 운영되고 있는지를 점검하기 위해 연 1회 이상 내부감사 계획을 수립하고 수행하여야 한다. 내부감사를 통해 발견된 문제점을 보완하여 경영진에게 보고하여야 한다.	○	○	○	법적 요구사항 및 수립된 정책에 따라 개인정보보호 관리체계의 효과적 운영을 점검하기 위한 감사기준, 범위, 주기, 감사인력 자격요건 등 내부감사 계획 등을 수립·보고하고 있는가?	
									내부감사 계획에 따라 연 1회 이상 내부감사를 수행하고 있는가?	
									내부감사에서 발견된 지적사항에 대해 보완조치 여부를 확인하여 개인정보 보호책임자 등 경영진에 보고하고 있는가?	
4. 교정 및 개선	4.1	교정 및 개선 활동	4.1.1	개인정보보호 개선 활동	주기적 또는 상시적으로 수행해야 하는 개인정보보호 활동을 문서화하여 그 운영현황을 지속적으로 점검·개선하는 등의 관리를 하여야 한다.	○	○	○	개인정보보호 관리체계 운영을 위해 주기적 또는 상시적으로 수행해야 하는 개인정보보호 활동을 문서화하고 있는가?	
									개인정보보호 운영현황을 주기적으로 검토하고 발견된 문제점에 대하여 개선하고 있는가?	
	4.2	내부 공유 및 교육	4.2.1	내부 공유 및 교육	개인정보 관리계획을 운영 또는 이행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여야 한다.	○	○	○	○	구현된 개인정보보호대책의 운영 및 시행부서 담당자를 대상으로 관련내용을 공유하고 교육을 수행하고 있는가?

# 생명주기 및 권리보장-20개 세부 항목

## 생명주기 및 권리보장

인증기준				상세내용	적용 유형				세부점검항목
					유형 4	유형 3	유형 2	유형 1	
	5.1.1	개인정보 수집 제한		서비스 제공을 위해 필요한 최소한의 정보만을 수집해야 한다. 개인정보 수집 시 필수와 선택 사항으로 구분하여 기재할 수 있도록 하여야 하며, 선택 사항의 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하여서는 아니된다.	○	○	○	○	서비스 제공을 위해 필요한 최소한의 정보만을 수집하고 있으며, 법령에 근거한 범위 내에서 수집하고 있는가?
									서비스 제공을 위해 필요한 최소한의 정보 이외의 정보를 수집할 경우, 정보주체(이용자)가 선택하여 제공할 수 있도록 하고 있는가?
									서비스 제공을 위해 필요한 최소한의 정보 이외의 개인정보를 제공하지 않는다는 이유로 해당 서비스의 제공을 거부하지 않도록 되어 있는가?
	5.1.2	정보주체의 동의		개인정보는 법령에 특별한 규정이 있는 경우를 제외하고는 정보주체(이용자)의 동의를 얻은 후에 수집해야 한다.	○	○	○	○	정보주체(이용자)의 개인정보를 수집하는 경우 법령에 근거하거나, 관련 사항을 모두 알리고 동의를 받고 있는가?
									동의를 받는 경우 동의를 얻어야 할 내용을 정보주체(이용자)가 명확히 인지하고 확인할 수 있도록 고지하고 있는가?
									정보주체의 개인정보를 이용하여 재화나 서비스를 홍보하거나 판매를 권유하는 경우 정보주체(이용자)가 이를 명확하게 인지할 수 있도록 고지하고 있는가?
									업무 여건의 변화 등으로 인하여 이미 수집·이용 중인 개인정보를 당초 수집 목적의 범위를 초과하여 이용하는 경우에는 해당 정보주체(이용자)에게 관련 내용을 알리고 동의를 받고 있는가?
									정보주체(이용자)가 해당 서비스의 이용 등을 위해 필요한 시점에 개인정보 수집 동의를 받고 있는가?
									정보주체(이용자)의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한이 필요한 경우 이용자의 동의를 받고 있는가?
									정보주체(이용자)에게서 동의를 받은 기록을 보관하는가?

5.1	개인정보 수집 시 보호조치	5.1.3	법정대리인 동의 및 고지	만14세 미만 아동의 개인정보를 수집할 경우 법정대리인에게 필요한 사항을 고지하고, 동의를 획득하여야 한다.	○	○	○	○	만14세 미만 아동의 개인정보를 수집·이용·제공 등의 동의를 받는 경우 법정 대리인에게 필요한 사항에 대하여 고지하고 동의를 얻고 있는가?
									법정대리인의 동의를 받기 위하여 개인정보 수집 시 최소한의 정보만을 수집하고 있는가?
									법정대리인이 자격 요건을 갖추고 있는지 확인하는 절차와 방법을 마련하고 있는가?
									법정대리인이 동의를 거부하거나 일정 기간 동의 의사가 확인되지 않은 경우 지체 없이 관련 개인정보를 파기하는가?
									법정대리인 동의에 대한 기록(동의자, 동의 여부, 동의 일시 등)은 사후에 확인이 가능하도록 개인정보처리시스템 등에 기록을 보존하는가?
		5.1.4	민감정보 및 고유식별정보의 수집 제한	고유식별정보와 민감정보는 정보주체(이용자)의 별도 동의를 받거나 다른 법령에서 처리를 요구하여 허용된 경우를 제외하고는 수집할 수 없다.	○	○	○	○	고유식별정보(주민등록번호 제외)를 수집하는 경우 정보주체(이용자)로부터 별도의 동의를 받거나 관련 법령에 근거하여서만 수집하고 있는가?
									민감정보를 수집하는 경우 정보주체(이용자)로부터 별도의 동의를 받거나 관련 법령에 근거하여야만 수집하고 있는가?
		5.1.5	주민등록번호 수집·이용 제한	법령에서 정보주체(이용자)의 주민등록번호 수집·이용을 허용한 경우를 제외하고 주민등록번호를 수집·이용할 수 없다.	○	○	○	○	법적 근거가 있는 경우를 제외하고는 주민등록번호를 수집·이용하지 않고 있는가?
									주민등록번호를 수집의 근거가 되는 법조항을 구체적으로 식별하고 있는가?
		5.1.6	주민등록번호 대체수단	법령에서 정보주체(이용자)의 주민등록번호 수집·이용을 허용한 경우에도 주민등록번호 대체수단을 제공해야 한다.	○	○	○	○	법적 근거에 따라 주민등록번호 수집이 가능한 경우에도 아이핀, 휴대폰 인증, 공인인증서 등 주민등록번호를 대체하는 수단을 제공하는가?

5.1.7	간접수집 보호조치	시스템에 의한 수집 또는 개인정보 처리를 통해 생성한 간접 수집 개인정보에 대하여 적절한 보호대책을 수립·이행해야 한다.	○	○	○	○	개인정보를 시스템에 의해 수집하거나 간접수집하는 경우 관련 내용을 개인정보처리방침에 공개하고 있는가?
							간접 수집된 개인정보를 제공받는 경우, 개인정보 수집에 대한 동의획득 책임이 개인정보 제공업체에 있음을 계약을 통해 명시하고 있는가?
							정보주체(이용자) 이외로부터 수집하는 개인정보에 대해 정보주체의 요구가 있는 경우 즉시 정보주체에게 이를 고지하고 있는가?
							SNS, 인터넷 홈페이지 등 공개된 매체 및 장소에서 개인정보를 수집하는 경우에는 정보주체(이용자)의 공개 목적·범위 및 사회 통념상 동의 의사가 있다고 인정되는 범위 내에서만 수집·이용하는가?
							서비스 계약 이행을 위해 필요한 경우로서, 사업자가 서비스 제공 과정에서 자동수집장치 등에 의해 수집·생성하는 개인정보(이용내역 등)의 경우에도 최소수집 원칙이 적용되고 있는가?
5.1.8	개인정보처리(취급)방침	개인정보처리(취급)방침을 수립하여 정보주체(이용자)가 언제든지 확인할 수 있도록 적절한 방법에 따라 공개하여야 한다.	○	○	○	○	개인정보처리방침이 법적 요구사항 및 운영에 필요한 사항을 포함하여 작성되었는가?
							개인정보처리방침을 정보주체(이용자)가 언제든지 쉽게 확인할 수 있도록 적절한 방법으로 공개하였는가?
							개인정보처리방침을 변경하는 경우에는 그 이유 및 변경 내용을 지정된 방법에 따라 지체 없이 공지하고, 정보주체(이용자)가 언제든지 변경된 사항을 쉽게 알아 볼 수 있도록 조치하는가?



5. 개인정보 생명주기 관리				5.2.1	개인정보 제3자 제공	개인정보를 제3자에게 제공 시, 관련내용을 고지하고 동의를 획득한 후 제공하여야 하며, 제3자에게 개인정보의 접근을 허용하는 경우 개인정보를 안전하게 보호하기 위한 보호절차에 따라 통제해야 한다.	○	○	○	○	정보주체(이용자)의 개인정보를 제3자에게 제공하는 경우 법령에 근거하거나, 관련 사항을 모두 알리고 동의를 받고 있는가?
											개인정보의 제3자 제공 동의는 수집·이용에 대한 동의와 구분하여 받아야 하고, 이에 동의하지 않는다는 이유로 해당 서비스의 제공을 거부하지 않도록 되어 있는가?
											개인정보를 제3자에게 제공하는 경우 제공 목적에 맞는 최소한의 개인정보 항목으로 제한하고 있는가?
											개인정보의 제3자 제공과 관련하여 기존에 정보주체(이용자)에게 고지한 사항 중 변경이 발생한 경우 정보주체(이용자)에게 관련 변경 내용을 알리고 동의를 받고 있는가?
											제3자에게 개인정보 제공 시 안전한 절차에 따르도록 하며, 제공 내역을 기록하여 보관하고 있는가?
				5.2.2	제공받은 개인정보의 관리	개인정보를 제공받은 경우 제공받은 목적 외의 용도로 이용하지 않고 제3자에게 제공하지 않아야 하며, 개인정보를 안전하게 관리하여야 한다.	○	○	○	○	개인정보를 제3자로부터 제공받은 경우 이를 제공받은 목적 외의 용도로 이용하지 않도록 하고 있는가?
											제공받은 개인정보를 제3자에게 제공할 경우 법령에 근거하거나, 관련 사항을 모두 알리고 동의를 받고 있는가?
											정보주체(이용자) 이외로부터 개인정보를 제공받을 시 법적 요건에 따라 통지 의무가 부과된 경우에는 제공받은 사실을 해당 정보주체에게 알리는가?

5.2	개인정보이용 및 제공	5.2.3	개인정보 목적 외 이용 및 제공	개인정보를 정보주체(이용자)에게 고지· 동의받은 범위에서 벗어나지 않도록 이 용하여야 하며, 만약 동의 범위를 벗어날 경우 정보주체(이용자)로부터 추가 동의 를 획득하고, 적절한 보호조치를 하여야 한다.	○	○	○	○	정보주체(이용자) 및 정보주체(이용자)의 법정대리인으로부터 수집한 개인정보를 동의받은 범위 또는 법에서 정한 목적 내에서만 이용하는가?
									개인정보를 수집 목적 또는 범위를 초과하여 이용하거나 제공하는 경우, 정보주체(이용자)로부 터 별도의 동의를 받거나 법적 근거가 있는 경우로 제한하고 있는가?
									개인정보를 목적 외의 용도로 제3자에게 제공하는 경우, 제공받는 자에게 이용목적·방법 등을 제한하거나 안전성 확보를 위해 필요한 조치를 마련하도록 요청하고 있는가?
									개인정보를 목적외의 용도로 제3자에게 제공하는 경우 제공 목적에 맞는 최소한의 개인정보 항 목으로 제한하고 있는가?
									개인정보를 비식별화하여 이용하거나 제공하는 경우, 재식별화의 위험을 최소화할 수 있도록 적절한 방법을 선정하여 비식별화 조치를 적용하고 이에 대한 적정성을 평가하고 있는가?
									공공기관이 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우, 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 관보 또는 인터넷 홈페이지 등 에 게재하고 있는가?
									공공기관이 개인정보를 목적 외의 용도로 이용하거나 목적 외의 용도로 제3자에게 제공하는 경 우, 목적외 이용 및 제3자 제공대장에 기록·관리하고 있는가?



			5.2.4	개인정보의 이전	<p>영업의 양도, 합병 등으로 개인정보를 이전하는 경우 적절한 보호대책을 수립·이행해야 한다. 또한, 개인정보를 해외로 이전하는 경우 개인정보에 대한 적절한 보호대책을 수립·이행해야 한다.</p>	○	○	○	○	<p>영업의 양도, 합병 등으로 개인정보를 타인에게 이전하려는 경우 미리 다음의 사항을 정보주체(이용자)에게 알리고 있는가?</p> <p>1. 개인정보를 이전하려는 사실</p> <p>2. 개인정보를 이전받는 자의 성명, 주소, 전화번호 및 그 밖의 연락처</p> <p>3. 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차</p> <p>정보주체가 안전한 처리를 증명하지 않고 영업의 양도, 합병 등으로 개인정보를 이전하겠다고, 자체없이 그 사실을 정보주체(이용자)에게 통지하는가? 다만, 정보통신서비스제공자인 경우에는 양도자의 이전 사실 통지 여부와 무관하게 개인정보를 이전받은 사실을 이용자에게 통지하는가?</p> <p>영업의 양도, 합병 등으로 개인정보를 이전받은 경우 양도자가 이용자의 개인정보를 이용하거나 제공할 수 있는 당초의 목적 범위 내에서만 개인정보를 이용하거나 제공하는가?</p> <p>영업의 양도, 합병 등으로 개인정보를 이전받아 양도자가 정보주체(이용자)의 개인정보를 이용하거나 제공할 수 있는 당초의 목적 범위 외로 개인정보를 이용하거나 제공하고자 하는 경우, 별도로 이용자의 동의를 받고 있는가?</p> <p>개인정보의 국외 이전시 국내법 및 해당 국가의 법을 만족하는 공식적인 계약을 체결하였는가?</p> <p>개인정보의 국외 이전시 관련 사항을 모두 알리고 동의를 받고 있는가? 다만, 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 이용자의 개인정보를 국외에 처리위탁 또는 보관하는 경우에는 동의에 갈음하여 관련 사항을 이용자에게 알리고 있는가?</p> <p>개인정보의 국외 이전 시 분실, 도난, 유출, 변조, 훼손을 막을 수 있는 안전한 방법으로 이전하고, 국외 이전된 개인정보에 대하여 기술적, 관리적 보호조치를 취하고 있는가?</p>
--	--	--	-------	----------	--	---	---	---	---	---

5.3	개인정보 보호 시 보호조치	5.3.1	개인정보 품질 보장	수집된 개인정보는 안전하게 저장 및 관리 하여야 하며 정확성, 완전성, 최신성을 유지 하여야 한다.	○	○	○	○	수집된 개인정보를 안전하게 처리하여 관리할 수 있도록 내부 절차를 수립하고 있는가?
									수집된 개인정보는 안전하게 처리하도록 관리하며 정확하고 최신의 상태로 유지되는가?
									정보주체(이용자)가 최신성을 유지할 수 있는 방법을 제공하고 있는가?
		5.3.2	개인정보 파일관리	개인정보파일을 운용하는 공공기관은 그 현황을 행정자치부에 등록하여야 하고, 변경사항 발생 시, 이를 고지하여야 한다.	○				공공기관이 개인정보파일을 신규로 운용하거나 변경하는 경우, 관련된 사항을 행정자치부장관에게 등록하고 있는가?
									공공기관은 개인정보파일의 보유 현황을 개인정보처리방침에 공개하고 있는가?
		5.4.1	개인정보 파기 규정 및 절차	개인정보의 보유기간 및 파기와 관련한 내부 규정을 수립하고, 파기 관련 보호조치를 마련하여야 한다. 또한, 개인정보 수집 동의 등에 대한 기록은 탈퇴 전까지 안전하게 보관하여야 한다.	○	○	○	○	수집 및 취급하는 개인정보의 보유기간 및 파기 관련 내부 규정이 존재 하는가? - 수집항목별, 수집목적별, 수집경로별 - 보관장소(DB, 백업데이터 등) - 파기방법 - 법령근거 등
									휴면 이용자의 개인정보가 파기 또는 분리하여 저장·관리되는 사실, 일시 및 해당 개인정보 항목을 통지하는가?
									공공기관이 개인정보파일 파기시 파기관리대장을 기록·관리하고 있는가?

5.4	개인정보 파 기 시 보호조 치	5.4.2	개인정보의 파기	개인정보의 수집 목적이 달성된 경우, 안전한 방법으로 지체없이 파기하고 관련 사항은 기록 관리하여야 한다. 개인정보의 수집목적 달성 후에도 관련 법령 등에 의해 보유가 필요하다면 정보주체(이용자)에게 고지하고 최소한의 항목을 보유해야 한다.	○	○	○	○	개인정보의 보유기간이 경과되거나 수집 및 이용목적이 달성된 경우 지체없이 개인정보(위탁 또는 제3자 제공 포함)를 파기하는가?
									개인정보의 파기 방법은 복구 불가능한 수준의 안전한 방법으로 파기하고 있는가?
									개인정보 파기에 대한 기록을 남기고 파기일자, 파기사실 등에 대해 정기적으로 확인하고 검토하는가?
									개인정보의 수집목적이 달성된 후에도 타 법령 등에 근거하여 개인정보의 전부 또는 일부를 보유해야 하는 경우 필요한 조치를 취하고 있는가? - 보유근거, 보유목적, 보유기간 및 보유항목에 대해서 정보주체(이용자)에게 고지 - 개인정보의 항목을 보유목적에 맞는 최소한의 항목으로 제한 - 다른 개인정보와 분리하여 보존 등
									정보통신서비스제공자는 법에서 정한 기간 이상 정보통신서비스를 미이용한 이용자의 개인정보를 해당 기간 경과 시 지체없이 파기하거나 다른 개인정보와 별도로 분리하여 저장·관리하고 있는가?
									분리 보존된 개인정보에 대해서는 접근권한을 최소한의 인원으로 제한하고 분리 보존된 목적 외에 이용되지 않도록 제한하고 있는가?
		6.1.1	개인정보 열람	개인정보에 대한 열람·정정·삭제 방법 및 절차를 제공하고, 정보주체(이용자)가 요구 시 열람하게 하여야 한다.	○	○	○	○	정보주체(이용자) 및 정보주체(이용자)의 법정대리인으로부터 이용자 개인정보에 대한 열람을 요구할 수 있는 방법 또는 절차를 제공하는가? - 요청 방법 및 접수 담당자 - 처리 절차 - 기록 대장 관리 등
									개인정보처리자가 개인정보에 대한 열람을 요구받을 경우 기간 내에 열람 가능하도록 처리하고, 열람할 수 없는 정당한 사유가 있을 때에는 열람 요구자에게 그 사유를 알리는가?
									개인정보에 대한 열람 요청을 받은 경우 본인 여부를 확인하는 절차가 있는가?



6.1.3	개인정보 처리 정지	정보주체(이용자)에게 개인정보에 대한 처리정지 방법 및 절차를 제공하고, 처리정지 요구 시 지체없이 처리하고, 기록을 남겨야 한다.	○	○	○	○	정보주체(이용자) 및 정보주체(이용자)의 법정대리인이 개인정보 처리정지를 요청할 수 있는 방법 및 절차가 있는가? - 요청 방법 및 접수 담당자 - 처리 절차 기록 대장 관리 등
							정보주체(이용자) 및 정보주체(이용자)의 법정대리인이 이용자의 개인정보 처리정지를 요청할 경우 지체없이 필요한 조치를 취하는가?
							정보주체(이용자) 및 정보주체(이용자)의 법정대리인에 의한 처리정지 요구를 거절하는 정당한 사유가 있을 때, 그 내용을 처리정지 요구자에게 알리는가?
							정보주체(이용자) 및 정보주체(이용자)의 법정대리인으로부터 개인정보 처리정지 요청을 받은 경우 본인 여부를 확인하는 절차가 존재하는가?
6.1.4	권리행사의 방법 및 절차	정보주체(이용자)가 열람 등 요구에 대한 거절 등 조치에 이의를 제기할 수 있도록 상담창구 등 필요한 절차를 마련하여야 한다.	○	○	○	○	정보주체(이용자)로부터의 개인정보에 관한 의견과 불만을 접수하고 처리하는 상담창구를 운영하고 있는가?
							개인정보 처리와 관련하여 정보주체(이용자)의 불만처리 결과를 검토하는 절차가 존재하는가?
							정보주체(이용자)의 요구에 대한 개인정보처리자의 조치에 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하고 있는가?

# 개인정보보호조치-50개 세부항목

## 개인정보 보호대책

인증기준				상세내용	적용 유형				세부점검항목
					유형 4	유형 3	유형 2	유형 1	
7.1	교육 및 훈련	7.1.1	교육 및 훈련 시행·평가	연간 개인정보보호 교육 계획을 수립하고, 관련 임직원 및 외부자를 대상으로 주기적인 교육을 시행하여야 한다. 또한, 교육 시행에 대한 기록을 남기고 결과를 평가하여 다음 교육에 반영하여야 한다.	○	○	○	○	<p>개인정보보호 교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 개인정보보호교육 계획을 수립하고 있는가?</p> <p>개인정보 보호책임자가 개인정보보호 교육 계획을 검토하여 승인하고 있는가?</p> <p>교육대상에 개인정보보호 관리체계 범위 내 개인정보자산에 접근하는 관련 임직원 및 외부자를 모두 포함하고 있는가?</p> <p>교육시 다음과 같은 내용을 포함하고 있는가?</p> <ul style="list-style-type: none"> <li>- 개인정보보호 및 개인정보보호 관리체계 개요</li> <li>- 개인정보보호 관련 법률</li> <li>- 개인정보보호 정책, 지침, 절차 등 개인정보보호 관련 내부규정</li> <li>- 관리적·기술적 조치사항 및 이를 수행하기 위한 방법</li> <li>- 개인정보 침해(유출)사고 사례 및 대응방안</li> <li>- 개인정보보호 규정 위반 시 법적 책임 등 개인정보취급자가 필수적으로 알아야 하는 사항 등</li> </ul> <p>개인정보취급자 및 개인정보보호 조직 내 임직원은 개인정보보호와 관련하여 직무특성에 따른 전문성 제고를 위하여 필요한 별도의 교육을 받고 있는가?</p> <p>개인정보보호 정책 및 절차의 중대한 변경, 조직 내·외부 개인정보 침해사고 발생, 개인정보보호 관련 법률 변경 등 발생 시 이에 대한 추가 교육(예 : 게시판 공지, 이메일 안내, 책자 안내 등)을 수행하고 있는가?</p> <p>출장, 휴가 등의 사정으로 정기 개인정보보호 교육을 받지 못한 인력에 대한 교육 방법을 마련하고 시행하고 있는가?</p> <p>교육 계획에 따라 주기적으로 시행하여 이에 대한 기록을 남기고 결과를 평가하여 다음 교육에 반영하고 있는가 ?</p>
				개인정보를 취급하는 임직원 및 외부자를 최소한으로 제한하고 개인정보취급자 목록을 관리하여야 한다. 또한 개인정보 보호 책임의 충실한 이행 여부에 대해 상 별 규정을 마련하여야 한다.	○	○	○	○	<p>임직원 및 계약에 따라 개인정보를 취급하는 자 등을 업무상 개인정보를 취급하는 자를 개인정보 취급자로 지정하고 목록을 관리하고 있는가?</p> <p>개인정보를 취급하는 임직원 및 외부자를 최소한으로 지정하고 있는가?</p> <p>개인정보 업무를 취급함에 있어 충실히 이행하는지에 대한 상별규정을 마련하고 있는가?</p>



7. 관리적 보호조치	7.2	개인정보 취급자 관리	7.2.2	보안 서약서	개인정보를 취급하는 개인정보취급자, 임직원, 외부자 등에게 보안서약서를 받아야 한다.	○	○	○	○	개인정보 업무를 취급하는 개인정보취급자에게 개인정보취급에 대한 보안서약서를 받고 있는가? 임직원 혹은 외주용역과 같은 제3자에게 개인정보에 대한 접근권한을 부여할 경우, 개인정보취급에 대한 준수사항과 책임이 명시된 보안서약서를 받고 있는가? 개인정보취급에 대한 보안서약서는 안전하게 보존·관리하고 있는가?
			7.2.3	퇴직 및 직무변경 관리	개인정보취급자의 퇴직 및 직무변경 시 자산반납, 계정 및 권한 회수, 조정, 결과 확인 등의 개인정보취급자 인사 관리 절차를 수립하고 이행하여야 한다.	○	○	○	○	조직 내 인력(임직원, 파견근로자, 시간제근로자, 외주용역직원 등)의 퇴직 및 직무변경 시 자산 반납, 접근권한 회수·조정, 결과 확인 등 절차를 수립하고, 관련 절차에 따라 지체 없이 이행하고 있는가? 휴직, 퇴직, 직무변경 등의 인사변경 내용이 인사부와 개인정보보호부서, 시스템 운영부서 등 관련 부서 간에 공유되고 있는가?
			7.3.1	외부 위탁 계약	개인정보 처리업무를 외부에 위탁하는 경우 개인정보보호에 관한 요구사항, 관리감독, 법규정 위반의 배상책임 등에 관한 사항을 계약서 등에 문서화하여야 한다.	○	○	○	○	개인정보 처리 위탁 계약시 해당 계약서에는 다음의 내용을 포함하는가? - 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항 - 개인정보의 기술적·관리적 보호조치에 관한 사항 - 위탁업무의 목적 및 범위 - 재위탁 제한에 관한 사항 - 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항 - 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항 - 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항 등 위탁자는 개인정보 처리위탁을 위한 수탁자를 선정할 때 인력과 물적 시설, 재정 부담능력, 기술 보유의 정도, 책임능력 등 개인정보 처리 및 보호 역량을 종합적으로 고려하는가?
	7.3	위탁업무 관리	7.3.2	정보주체 고지	개인정보 처리업무 위탁시 수탁자, 수탁 목적 등 관련사항을 정보주체(이용자)에게 고지하고 필요한 경우 동의를 받아야 한다.	○	○	○	○	제3자에게 정보주체(이용자)의 개인정보 처리업무를 위탁하는 경우 관련 사항을 이용자에게 알리는가? 개인정보 처리 위탁에 대한 동의가 필요한 경우, 법령에 따라 필요한 사항을 알리고 동의를 받고 있는가? 개인정보 처리 위탁 시 수탁자 변동 또는 위탁업무 범위 및 계약상의 변동사항이 발생할 경우 정보주체(이용자)로부터 별도의 동의 또는 고지 절차를 거치고 있는가? 위탁자는 정보주체가 언제든지 수탁자의 정보를 확인할 수 있도록 관보 또는 인터넷 홈페이지에 게재하는 등의 방법으로 공개하고 있는가?

									수탁자로부터 개인정보보호의 관리상황을 주기적으로 보고 받고, 정기 또는 수시점검을 통해 관리·감독하고 있는가?
									개인정보 처리 위탁 시 수탁자 직원에 대한 개인정보보호 교육을 직접 수행하거나 요청하여 관리하고 있는가?
		7.3.3	위탁자 관리·감독	위탁 업체가 계약서 및 서비스 수준 협약, 관련 법·규정 등에 명시된 사항을 충분히 이행하는지 주기적으로 관리·감독해야 한다.	○	○	○	○	수탁자 및 외부로부터의 개인정보처리시스템 접근내역을 기록하여 남기고 있는가?
									개인정보 위탁계약 종료 시 수탁자에 대한 개인정보 파기 확인 절차가 마련되어 있고 이에 대한 관리가 이루어지고 있는가 ?
									수탁자가 개인정보 처리업무를 제3자에게 재위탁하는 경우, 위탁자의 동의를 받은 경우에 한하여 재위탁하고, 위탁자가 수탁자에게 요구하는 동일한 수준의 기술적·관리적 보호조치를 재위탁자가 이행하도록 관리·감독 하는가?
		7.4.1	침해사고 대응절차 및 체계구축	개인정보 침해사고 대응절차를 수립하고, 개인정보 침해사고 대응이 신속하게 이루어질 수 있도록 대응체계를 구축하며 외부기관 및 전문가들과의 협조체계를 수립하여야 한다.	○	○	○		개인정보 침해사고 대응절차가 수립되어 있고 대응절차에는 다음과 같은 내용을 포함하고 있는가? - 개인정보 침해사고의 정의 및 범위 (중요도 및 유형 포함) - 개인정보 침해사고 선포절차 및 방법 - 비상연락망 등의 연락체계 - 개인정보 침해사고 발생시 기록, 보고절차 - 개인정보 침해사고 신고 및 통지 절차 (관계기관, 이용자 등) - 개인정보 침해사고 보고서 작성 - 개인정보 침해사고 중요도 및 유형에 따른 대응 및 복구 절차 - 개인정보 침해사고 복구조직의 구성, 책임 및 역할 - 개인정보 침해사고 복구장비 및 자원조달 - 개인정보 침해사고 대응 및 복구 훈련, 훈련 시나리오 - 외부 전문가나 전문기관의 활용방안 - 기타 보안사고 예방 및 복구를 위하여 필요한 사항 등
									외부 관제시스템 등 외부 기관을 통해 개인정보 침해사고 대응체계를 구축·운영하는 경우 개인정보 침해사고 대응절차의 세부사항을 계약서(SLA 등), 계획서 등에 반영하고 있는가?
									개인정보 침해사고의 모니터링, 대응 및 처리와 관련된 외부전문가, 전문업체, 전문기관(KISA) 등과의 협조체계를 수립하고 있는가?
									침해사고 대응절차는 관련자들이 인지할 수 있도록 공유 및 교육하고 있는가?

7.4	침해사고 관리	7.4.2	침해사고 훈련 및 개선	침해사고 대응절차를 임직원들이 숙지할 수 있도록 시나리오에 따른 모의훈련을 실시하여야 한다. 모의훈련 결과는 침해사고 대응절차에 반영하여 주기적으로 개선하여야 한다.	○	○	○	<p>개인정보 침해사고 대응에 관한 모의훈련 계획을 수립하고, 이에 따라 주기적으로 교육 및 훈련을 실시하고 있는가?</p> <p>모의훈련 결과는 침해사고 대응절차에 반영하여 주기적으로 개선하고 있는가?</p>
		7.4.3	침해사고 대응	개인정보 침해사고 발생 시 절차에 따라 신속히 복구를 수행하고, 사고분석 후 발견된 취약점은 관련 조직 및 임직원과 공유하며, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하여 침해사고 대응 체계에 반영하여야 한다.	○	○	○	<p>개인정보 침해사고의 징후 또는 발생을 인지한 경우 개인정보 침해사고 대응절차에 따라 신속하게 대응 및 보고가 이루어지고 있는가?</p> <p>개인정보 침해사고 발생 시 관련 법률 및 규정에 따라 정보주체(이용자)에게 통지하고 필요 시 관계 기관에 신고하는 절차를 수립·이행하고 있는가?</p> <p>개인정보 침해사고가 발생한 경우 절차에 따라 적대적 공격자를 추적하고 그 기록을 감시하고 있는가?</p> <ul style="list-style-type: none"> <li>- 사고날짜, 내용 등</li> <li>- 처리 및 복구 일시</li> <li>- 담당자</li> <li>- 처리 및 복구 방법</li> </ul> <p>처리 및 복구 수행 결과 내용 등</p> <p>개인정보 침해사고 정보와 발견된 취약점 및 보호대책에 대해 관련 조직 및 임직원에게 공유하고 있는가?</p> <p>개인정보 침해사고 분석을 통하여 재발방지 대책을 수립하고, 필요시 개인정보 침해사고 대응절차 등을 변경하는가?</p> <p>통지를 할 수 없는 경우 법령상 정하는 방법에 따라 알릴 수 있는 절차를 수립하고 발생 시 이행하는가?</p>
		8.1.1	접근통제 정책 수립	개인정보보호 요구사항을 기반으로 비인가자의 접근을 통제할 수 있도록 개인정보취급자의 접근통제 정책을 수립하여야 한다.	○	○		<p>개인정보취급자 등 사용자의 접근 통제영역을 정의하고 접근 통제영역별로 접근통제 정책을 수립하고 있는가?</p> <ul style="list-style-type: none"> <li>- 개인정보취급자 계정 관리 절차</li> <li>- 네트워크, 서버, 응용프로그램, 데이터베이스 등 영역별 접근통제 규칙, 방법, 절차</li> <li>- 예외사항에 대한 안전한 관리절차 등</li> </ul>
		8.1.2	개인정보취급자 등록	개인정보 및 개인정보처리시스템의 접근을 통제하기 위한 개인정보취급자 등록 및 해지 절차를 마련하여야 한다. 또한, 개인정보 취급 PC의 보안책임이 본인에게 있음을 규정하고 인식시켜야 한다.	○	○	○	<p>개인정보취급자 등의 사용자 계정 등록·삭제(비활성화) 및 접근권한 등록·변경·삭제에 관한 공식적인 절차를 수립·이행하고 있는가?</p> <p>개인정보취급자에게 개인정보 취급 PC의 보안책임이 본인에게 있음을 규정하고, 이에 대해 인식교육을 수행하고 있는가?</p>

8.1	접근권한 관리	8.1.3	개인정보취급자 권한관리	개인정보처리시스템의 접근권한은 최소한의 업무수행자에게만 부여하고 권한변경 내역을 보관하여야 한다.	○	○	○	○	개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 최소한의 인원에게 부여하고 있는가?
									개인정보취급자 등 사용자의 업무 내용에 따라 접근 권한을 차등 부여하고 있는가?
									개인정보처리시스템의 접근 권한 부여 현황, 변경 또는 말소 내역 등을 기록하고 관련 법령에 따라 보관하고 있는가?
									개인정보취급자의 퇴직, 계약 종결 또는 직무 변경 시 접근권한을 제거 또는 변경하고 있는가?
		8.1.4	특수권한 관리	개인정보 및 개인정보처리시스템에 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.	○	○	○	○	개인정보 및 개인정보처리시스템 관리자 및 특수 권한은 최소한의 인원에게만 부여하고 권한 부여 시 책임자 승인 절차를 수립하고 있는가?
									개인정보 및 개인정보처리시스템 관리자 권한 및 특수 권한을 식별하여 별도 목록으로 관리하고 있는가?
									외부자에게 부여한 특수 목적의 계정은 한시적으로 부여하고 사용이 끝난 후에는 즉시 삭제 또는 정지하고 있는가?
									특수 권한의 할당이나 사용을 최소한으로 제한하고 사용 현황을 주기적으로 점검하고 있는가?
		8.1.5	개인정보취급자 접근 권한 검토	개인정보 및 개인정보처리시스템 등을 사용하는 개인정보취급자의 접근권한 현황을 정기적으로 점검해야 한다.	○	○	○		개인정보취급자 직무별 또는 역할별 개인정보처리시스템 접근권한을 정의한 개인정보 접근권한 분류 체계를 수립하고 있는가?
									개인정보처리시스템 및 개인정보에 대한 접근권한 검토 기준, 검토주체, 검토방법, 주기 등을 정하여 정기적 검토를 이행하고 있는가?
									개인정보취급자 접근권한의 검토 결과 접근권한 오남용 등의 이상징후가 발견된 경우 그에 따른 조치절차를 수립·이행하고 있는가?

8.2	접속기록 관리	8.1.6	개인정보취급자 인증 및 식별	개인정보처리시스템 접근 시 안전한 인증 절차에 따라 통제하고, 필요한 경우 법적요구사항 등을 고려하여 강화된 인증 방식을 적용해야 한다.	○	○	○	○	<p>개인정보처리시스템에 대한 접근은 개인정보취급자만 접속할 수 있도록 내부 기준과 통제 방안을 마련하고, 개인정보취급자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고, 동시접속 제한 등 안전한 개인정보취급자 인증 절차 등을 통해 통제하고 있는가?</p> <p>동일한 식별자를 공유하여 사용하는 경우 그 이유와 타당성을 검토하고 책임자의 승인을 받고 있는가?</p> <p>개인정보취급자가 불가피하게 외부에서 개인정보처리시스템에 접속하는 경우 강화된 인증 방식과 개인 식별이 가능한 방법을 사용하고 있는가 ?</p>
		8.1.7	비밀번호 관리	법적요구사항, 외부 위협요인 등을 고려하여 개인정보취급자 및 사용자, 정보주체(이용자)의 비밀번호 관리절차를 수립하고 이행하여야 한다.	○	○	○	○	<p>개인정보취급자, 사용자의 비밀번호 관리절차를 수립·이행하고 있는가?</p> <ul style="list-style-type: none"> <li>- 비밀번호의 변경 주기 및 복잡도</li> <li>- 유추하기 쉬운 비밀번호 사용 금지</li> <li>- 이전 사용한 비밀번호의 재사용 금지 등</li> </ul> <p>정보주체(이용자)가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성 규칙을 수립·이행하고 있는가?</p> <p>비밀번호 관리 책임이 본인에게 있음을 주지시키고 있는가?</p>
		8.2.1	개인정보처리시스템 접속기록 관리	개인정보처리시스템의 접속기록을 보관하고, 접속기록의 정확성을 보장하기 위해 관련 장비 및 시스템을 표준시간으로 동기화하여 해야 한다.	○	○	○	○	<p>개인정보처리시스템 접속기록 관리절차를 수립하고 이에 따라 접속기록을 관리하고 있는가?</p> <ul style="list-style-type: none"> <li>- 보존이 필요한 접속기록과 대상시스템의 식별</li> <li>- 각 시스템 및 장비별 접속기록 형태 및 보존기간 정의</li> <li>- 접속기록 보존(백업) 방법 등</li> </ul> <p>개인정보처리시스템 및 개인정보 처리와 연관된 주요 자산에 대한 개인정보취급자의 접속기록(식별자, 접속일시, 개인정보 열람·수정·삭제·출력 등의 작업내역)을 저장하고 있는가?</p> <p>개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관·관리하고 있는가?</p> <p>각 개인정보처리시스템 시간을 표준시간으로 동기화하고 있는가?</p>

		다	8.2.2	접속기록 모니터링	접속기록은 위·변조되지 않도록 보호대책을 적용하여야 하며, 개인정보의 오남용이 발생되지 않도록 모니터링을 수행하여야 한다. 또한 문제 발생 시 적절한 사후조치가 적시에 이루어져야 한다.	○	○	○	<p>개인정보처리시스템의 접속기록이 위·변조되지 않도록 해당 접속기록을 안전하게 보관하고 그에 대한 접근권한 부여를 최소화 하고 있는가?</p> <p>개인정보보호 업무의 수행과 관련하여 오류 및 부정행위가 발생하지 하지 않도록 개인정보처리 활동에 대한 모니터링 및 정기적인 점검활동을 수행해야 하며, 이를 위한 지침, 절차를 수립·이행하고 있는가?</p> <ul style="list-style-type: none"> <li>- 검토대상 및 주기</li> <li>- 검토기준 및 방법</li> <li>- 검토 담당자 및 책임자 지정</li> <li>- 이상징후 대응절차 등</li> </ul> <p>사용자 접속기록 검토결과를 개인정보 보호책임자에게 보고하고 이상징후 발견 시 절차에 따라 대응하고 있는가?</p>
			8.3.1	네트워크 접근	유·무선 네트워크에 대한 비인가 접근을 통제하기 위해 네트워크 접근통제 관리 절차를 수립하고 서비스, 사용자 그룹, 개인정보 자산의 중요도, 법적요구사항에 따라 네트워크를 분리하여야 한다.	○	○	○	○ <p>접근통제 정책에 따라 인가된 사용자만이 네트워크에 접근할 수 있도록 네트워크 식별자(IP) 할당 등을 통제하고 있는가?</p> <p>네트워크 구성 변경 시에는 공식적인 변경 관리 절차를 준수하고 자체적인 보안성 검토를 수행하고 있는가?</p> <p>네트워크 대역별 IP 주소 부여 기준을 마련하여 DB서버 등 외부 연결이 필요하지 않은 경우 사설 IP로 할당하는 등의 대책을 적용하고 있는가 ?</p> <p>서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 망을 분리하고 있는가?</p> <p>물리적으로 떨어진 IDC 센터, 지사, 대리점, 협력업체, 고객센터 등과의 네트워크 연결 시 전용회선을 구축 또는 VPN(가상사설망) 등을 활용하고 있는가 ?</p> <p>네트워크 장비(라우터, 스위치 등)별로 접근이 허용된 사용자를 명확하게 식별·인증하고 안전한 접근수단을 적용하고 있는가?</p> <p>조직 내 무선네트워크 환경을 구축(AP 설치)할 경우 내부 승인, 보안성 검토 등 절차를 마련하고 구축에 따른 다음 사항을 보호대책에 적용하고 있는가?</p> <ul style="list-style-type: none"> <li>- 접속 단말 인증 방안(MAC 인증 등)</li> <li>- 정보 송수신 시 암호화 기능 설정(WPA2 이상 권고)</li> <li>- SSID 숨김(브로드캐스팅 중지) 기능 설정</li> <li>- 무선 AP의 관리자 접근 통제 (IP 등)</li> <li>- 무선 AP의 관리자 패스워드 주기적 변경 등</li> </ul> <p>정상적인 절차에 따라 무선네트워크 사용을 허가한 경우 인가된 임직원만 무선네트워크를 사용할 수 있도록 사용 신청 및 해지 절차를 수립하여 운영하고 있는가?</p>



8.3	접근통제영역 관리	8.3.2	서버 접근	서버별로 접근이 허용되는 사용자, 접근 제한 방식, 안전한 접근수단 등을 정의하여 적용하여야 한다.	○	○	○	○	개인정보처리시스템 등 서버별로 접근이 허용된 사용자를 명확하게 식별·인증하고 안전한 접근수단을 적용하고 있는가?
									개인정보처리시스템 등 중요 서버의 연결시간을 제한하고 있는가?
									개인정보처리시스템 등 서버의 사용목적과 관계없는 서비스를 제거하고 있는가?
		8.3.3	응용 프로그램 접근	사용자의 업무 또는 직무에 따라 개인정보를 취급하는 응용프로그램 접근권한을 제한하여야 한다.	○	○	○	○	개인정보 및 개인정보 관련 응용프로그램 접근을 통제하기 위하여 사용자의 업무에 따라 접근권한을 차등 부여하고 있는가?
									개인정보의 노출(조회, 출력, 다운로드 등)을 최소화 하도록 응용 프로그램을 구현하고 있는가?
									일정 시간동안 입력이 없는 세션은 자동 차단하고, 동일 사용자의 동시 세션 수를 제한하고 있는가?
									관리자 전용 응용프로그램(관리자 웹페이지, 관리콘솔 등)을 외부에 오픈되지 않도록 접근통제하고 있는가?
									주요 응용 프로그램에 대한 관리자(사용자) 접속 로그 및 이벤트 로그에 대한 모니터링을 정기적으로 수행하고 있는가 ?
									개인정보 검색 시 조회가 필요한 정보 이외의 정보가 조회되지 않도록 일치검색(equal검색)이나 두가지 조건 이상의 검색조건을 요구하는가?

8.3.4	데이터 베이스 접근	데이터베이스 접근을 허용하는 응용프로그램 및 사용자 직무를 명확하게 정의하고 응용프로그램 및 직무별 접근통제 정책을 수립·이행하여야 한다.	○	○	○	○	<p>데이터베이스 관리자 및 사용자의 직무를 접근 통제 영역을 구별하고 이에 따라 운영하고 있는가?</p> <ul style="list-style-type: none"> <li>- 데이터베이스 계정 또는 오브젝트(테이블, 뷰 또는 컬럼 등)수준에서 사용자 접근을 통제</li> <li>- 조회 권한의 계정과 DBA권한 계정의 구분</li> <li>- APP계정과 사용자 계정의 공용 사용 제한</li> <li>- 계정별 명령어 제한</li> <li>- 사용 가능한 응용프로그램 제한</li> </ul> <p>DB접근제어 등</p> <p>개인정보를 저장하고 있는 데이터베이스는 별도의 네트워크 영역으로 구분하고 있는가?</p> <p>데이터베이스 접근을 허용하는 IP, 포트, 응용프로그램을 제한하고 있는가?</p>
8.3.5	원격 운영접근	내부 네트워크를 통하여 개인정보처리시스템을 관리하는 경우 특정 단말에서만 접근을 할 수 있도록 제한하고, 외부 네트워크를 통하여 개인정보처리시스템을 관리하는 것은 원칙적으로 금지한다. 부득이한 사유로 인해 허용하는 경우에는 관련 법률에 따른 보호대책을 수립하여야 한다.	○	○	○		<p>내부 네트워크를 통해서 원격으로 개인정보처리시스템 및 개인정보 처리와 연관된 주요 자산(서버, 네트워크 장비, 보안장비 등)을 운영하는 경우 특정 단말에 한해서만 접근을 허용하고 있는가?</p> <p>인터넷과 같은 외부 네트워크를 통한 개인정보처리시스템 및 개인정보 처리와 연관된 주요 자산(서버, 네트워크 장비, 보안장비 등)의 원격운영은 원칙적으로 금지하고 있으며 부득이하게 허용하는 경우 다음과 같은 대책을 마련하고 있는가?</p> <ul style="list-style-type: none"> <li>- 책임자 승인</li> <li>- 접속 단말 및 사용자 인증</li> <li>- 한시적 접근권한 부여</li> <li>- VPN 등의 전송구간 암호화</li> <li>- 접속 단말 보안</li> <li>- 원격운영 현황 지속적인 모니터링 등</li> </ul> <p>정보통신망을 통해 외부에서 개인정보처리시스템에 접속하여 개인정보 파일을 다운로드하거나 출력 시 통제 기준을 수립하여 이행하고 있는가 ?</p>

8. 기술적 보호조치			8.3.6	인터넷 접속 통제	개인정보처리시스템에 접근 가능한 개인정보취급자의 PC는 인터넷 접속 또는 서비스 제한 및 통제하고, 필요시 인터넷 접속내역을 모니터링 하여야 한다.	○	○	○	<p>개인정보처리시스템에 접근 가능한 개인정보취급자의 PC 등 인터넷 접속에 대한 정책을 수립·이행하고 있는가?</p> <ul style="list-style-type: none"> <li>- 인터넷 연결시 네트워크 구성 정책</li> <li>- 이메일, 인터넷 사이트의 접속, 소프트웨어 다운로드 및 전송 등의 사용자 접속정책</li> <li>- 유해사이트(성인, 오락 등) 접속 차단 정책</li> <li>- 정보 유출 가능 사이트(웹하드, P2P 등) 접속 차단 정책</li> <li>- 인터넷 접속내역 검토(모니터링) 정책 등</li> </ul> <p>주요 개인정보취급자(권한부여자, 개인정보 삭제 및 다운로드 가능자)를 식별하여 인터넷 접속을 제한하고 있는가?</p> <p>아래의 내용을 포함하는 개인정보처리시스템 운영절차를 마련하였는가?</p> <ul style="list-style-type: none"> <li>- 문제 발생 시 재동작, 복구 절차</li> <li>- 오류 및 예외사항 처리 방안</li> <li>- 악성코드 통제</li> <li>- 보안시스템 운용</li> <li>- 모바일 기기 관리</li> <li>- 패치관리 등</li> </ul>
			8.4.1	운영절차 수립	개인정보처리시스템 동작에 문제 발생 시 재 동작 및 복구, 오류 및 예외사항 처리 등 시스템 운영을 위한 절차를 수립하여야 한다.	○	○		<p>개인정보처리시스템 운영절차(또는 매뉴얼)를 주기적으로 검토하고 있는가?</p> <p>개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응매뉴얼 등 대응절차를 마련하고 정기적으로 점검하고 있는가?</p>
			8.4.2	직무분리	개인정보처리시스템의 오남용 예방을 위해 직무 분리 기준을 수립·적용하고, 직무 분리가 어려운 특수한 경우 별도의 보호 대책을 마련하여야 한다.	○	○		<p>직무의 권한 오남용을 예방하기 위하여 개인정보보호 관련 주요 직무 분리 기준을 수립하고 직무별 역할과 책임을 명확하게 기술하고 있는가?</p> <ul style="list-style-type: none"> <li>- 개발과 운영 직무 분리 등</li> </ul> <p>불가피하게 직무 분리가 어려운 경우 직무자간 상호검토, 상위관리자 정기모니터링 및 변경사항 승인, 책임추적성 확보방안 등의 보완통제를 마련하고 있는가?</p>

8.4.3	악성코드 통제	바이러스, 웜, 트로이목마 등의 악성코드로부터 정보시스템과 개인정보취급자 단말기(PC, 노트북 등)를 보호하기 위해 보호대책을 수립하여야 한다.	○	○	○	○	바이러스, 웜, 트로이목마 등의 악성코드로부터 개인정보처리시스템을 보호하기 위하여 보호대책을 수립·이행하고 있는가?
							백신프로그램 등을 통한 최신 악성코드 예방, 탐지 활동을 지속적으로 수행하고 있는가?
							악성코드 감염 발견 시 악성코드 확산 및 피해 최소화 등의 대응절차를 수립·이행하고 있는가?
							백신 소프트웨어 등 보안프로그램은 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하도록 설정하고 있는가?
							개인정보처리시스템, 개인정보취급자의 PC에 P2P, 웹 하드 등과 같은 비인가 프로그램 설치를 금지하고 있는가?
							악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용프로그램이나 운영체제 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시하는가?
8.4.4	취약점 점검	개인정보처리시스템에 대한 비인가 접근 시도 등을 예방하기 위하여 정기적으로 기술적 취약점 점검을 수행하고 발견된 취약점들은 조치하여야 한다.	○	○	○		개인정보처리시스템 및 개인정보 처리와 연관된 주요 자산(서버, 네트워크 장비, 보안장비 등)의 취약점 점검 기준을 아래 내용을 포함하여 수립하고 정기적으로 점검을 수행하고 있는가? - 취약점 점검 대상 - 취약점 점검 주기 및 방법 - 중요도에 따른 조치 기준 - 보고 절차 - 미 조치 취약점에 대한 보안성 검토 등
							발견된 취약점에 대한 조치를 수행하고 그 결과를 책임자에게 보고하고 있는가?
8.4.5	개인정보 표시제한	개인정보 조회, 출력 등을 수행할 경우, 마스킹 기술 등을 통해 개인정보 표시를 제한하여야 한다.	○	○	○		개인정보 표시제한 조치의 일관성을 확보하기 위하여 관련 표준을 수립하고 개인정보처리시스템에서 개인정보의 인쇄물 출력시 용도에 따른 출력 항목을 최소화하고 있는가?
							개인정보처리시스템 등에서 화면이나 출력물을 통해 개인정보를 조회·출력 시 업무내용 및 취급자의 권한에 따라 필요한 최소한의 정보만을 표시하도록 운영하고 있는가?
							개인정보가 포함된 인쇄물, 외부 저장매체 등 개인정보의 출력, 복사물을 안전하게 관리하기 위해 잠금장치가 있는 안전한 장소에 보관하는 등의 통제 방안을 갖추고 있는가?
							표시제한된 개인정보를 해제하여 볼 수 있는 경우 해당 행위에 대한 승인, 로그생성 및 검토가 이루어지고 있는가?

8.4	운영보안	8.4.6	보안 시스템 설치· 운용	불법적인 접근 및 침해사고 방지를 위해 침입차단 및 탐지 기능을 포함한 시스템을 설치·운용하여야 한다. 또한, 보안시스템 운영절차를 수립하고 보안시스템별 정책적용 현황을 관리하여야 한다.	○	○	○	·	<p>불법적인 접근 및 침해사고 방지를 위하여 보안시스템을 설치·운영하고 있는가?</p> <p>외부침입 탐지 및 차단, 내외부자에 의한 정보유출 방지 등을 위하여 도입·운영하고 있는 보안시스템에 대한 운영절차를 수립하여 운영하고 있는가?</p> <ul style="list-style-type: none"> <li>- 보안시스템 유형별 책임자 및 관리자 지정</li> <li>- 보안시스템 정책(룰셋 등) 적용(등록, 변경, 삭제 등) 절차</li> <li>- 보안시스템 이벤트 모니터링 절차</li> <li>- 보안시스템 접근통제 정책</li> <li>- 보안시스템 운영현황 주기적 점검 등</li> </ul> <p>사용자 인증, 관리자 단말 IP 또는 MAC 접근통제 등의 보호대책을 적용하여 보안시스템 관리자 등 접근이 허용된 인원 이외의 비인가자 접근을 엄격히 통제하고, 주기적인 보안시스템 접속로그 분석을 통해 비인가자에 의한 접근시도를 확인하고 적절한 조치를 취하고 있는가?</p> <p>보안시스템 특성에 따른 정책(룰셋 등)의 신규 등록, 변경, 삭제, 백업 등 절차를 수립하고 정책의 타당성 검토를 주기적으로 수행하고 있는가?</p> <p>보안시스템의 예외 정책 등록에 대하여 절차에 따라 관리하고 있으며, 예외 정책 사용자에게 대하여 최소한의 권한으로 관리하고 있는가?</p>
		8.4.7	공개 서버 보안	웹사이트 등에 정보를 공개하는 경우 정보 수집, 저장, 공개에 따른 허가 및 게시 절차를 수립하고 공개서버에 대한 물리적, 기술적 보호대책을 수립하여야 한다.	○	○	○	○	<p>웹서버 등 공개 서버(WAS 포함)를 운영하는 경우 이에 대한 보호대책을 마련하고 있는가?</p> <p>공개서버는 내부 네트워크와 분리된 DMZ(Demilitarized Zone)영역에 설치하고 침입차단시스템 등 보안시스템을 통해 보호하고 있는가?</p> <p>웹사이트에 개인정보를 게시하거나 웹서버에 개인정보를 저장하여야 할 경우 내부 통제 절차를 수립·이행하고 중요정보 노출 여부를 주기적으로 점검하고 있는가?</p>

			8.4.8	모바일 기기 관리	업무 목적으로 모바일기기를 내·외부 네트워크에 연결하여 사용할 경우 모바일 기기 접근통제 대책을 수립하여야 한다.	○	○	○	<p>업무 목적으로 모바일기기를 사용할 경우, 접근 통제 정책을 마련하고 이에 따라 이행하고 있는가?</p> <ul style="list-style-type: none"> <li>- 모바일기기 허용기준</li> <li>- 모바일기기를 통한 업무 사용범위</li> <li>- 모바일기기 사용시 승인 절차 및 방법</li> <li>- 모바일기기 인증(MAC 인증 등)</li> <li>- 모바일기기 이용에 따른 보안 정책, 정책 및 오남용 모니터링 대책 등</li> </ul> <p>업무용 모바일 기기의 분실, 도난 등으로 인한 개인정보의 유·노출을 방지하기 위하여 비밀번호 설정 등의 보안대책을 적용하고 있는가?</p>
			8.4.9	백업 관리	데이터의 무결성 및 개인정보처리시스템의 가용성을 유지하기 위해 백업 절차를 수립하여 주기적으로 백업 및 관리를 하여야 한다.	○	○		<p>다음의 사항을 포함한 백업 및 복구절차를 수립·이행하고 있는가?</p> <ul style="list-style-type: none"> <li>- 백업담당자 및 책임자 지정</li> <li>- 백업대상별 백업 주기 및 보존기한 정의</li> <li>- 백업방법 및 절차</li> <li>- 백업매체 관리</li> <li>- 백업 복구 절차</li> <li>- 복구 테스트 계획</li> <li>- 백업관리대장 관리 등</li> </ul> <p>개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하고 있는가?</p> <p>개인정보의 무결성 및 개인정보처리시스템의 안전한 관리를 위해 주기적으로 백업하고 있으며, 재난에 대처할 수 있도록 백업매체를 물리적으로 떨어진 장소에 소산하고 있는가?</p>
			8.4.10	패치 관리	소프트웨어, 운영체제, 보안시스템 등에 대하여 시스템에 미치는 영향을 분석하여 주기적으로 최신 패치를 적용하여야 한다.	○	○	○	<p>개인정보처리시스템 및 개인정보 처리와 연관된 주요 자산(서버, 네트워크 장비, 보안장비 등)의 자산 중요도 또는 특성에 따라 OS, 소프트웨어 패치관리 정책 및 절차를 수립·이행하고 있는가?</p> <ul style="list-style-type: none"> <li>- 패치 적용 대상 및 주기</li> <li>- 패치 배포 전 사전 검토 절차</li> <li>- 긴급 패치 적용 절차 등</li> <li>- 패치 미 적용 시 보안성 검토 수행</li> </ul> <p>개인정보처리시스템 및 개인정보 처리와 연관된 주요 자산(서버, 네트워크 장비, 보안장비 등)의 경우 설치된 OS, 소프트웨어 패치적용 현황을 관리하고 있는가?</p> <p>개인정보처리시스템 및 개인정보 처리와 연관된 주요 자산(서버, 네트워크 장비, 보안장비 등)의 경우 공개 인터넷 접속을 통한 패치를 제한하고 있는가?</p> <p>패치관리시스템(PMS)를 활용하는 경우 접근통제 등 충분한 보호대책을 마련하고 있는가?</p>





			8.6.1	개인정보 영향평가	개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 수행하여야 한다.	○			공공기관은 개인정보처리시스템 신규 개발 또는 변경을 위한 계획 수립 시 개인정보 영향평가의 무대상 여부를 검토하고, 의무 대상인 경우에 영향평가 계획을 수립하고 관련 예산을 확보하는가?
									공공기관은 개인정보처리시스템 신규 개발 또는 변경 시 분석·설계 단계에서 영향평가기관을 통해 영향평가를 수행하고 그 결과를 개발에 반영하고 있는가?
									공공기관은 개인정보 영향평가서를 개인정보처리시스템 오픈 전 또는 영향평가 종료 후 2개월 이내에 행정자치부장관에게 제출하고 있는가?
									개인정보 영향평가 결과에 따른 개선요구사항에 대한 이행여부를 관리하고 있는가?
			8.6.2	개발 시 보안조치	개인정보처리시스템을 개발·변경 시 개인정보 영향평가 수행 결과를 보안 요구사항에 포함하여 개발하고, 안전한 코딩방법에 따라 구현 및 시험을 수행하며, 취약성에 대한 노출여부를 점검하여 이에 대한 보호대책을 수립하여야 한다.	○	○		신규 개인정보처리시스템 개발 및 기존 시스템 변경 시 개인정보 영향평가 결과 등을 고려하여 보안 요구사항을 정의하는가?
									사전 정의된 보안요구사항을 설계 및 구현에 반영하고 있는가?
									개인정보처리시스템의 안전한 구현을 위한 코딩 표준이 마련되어야 하며 이에 따라 구현하고 있는가?
									구현된 기능이 사전 정의된 보안 요구사항을 충족하는 지 시험을 수행하고 있는가?
8.6	개발보안	8.6.3	개발과 운영환경 분리	개발 및 시험 시스템은 운영시스템과 원칙적으로 분리하고, 운영환경으로의 이관은 통제된 절차에 따라 이루어져야 하며, 실행코드는 시험과 인수 절차에 따라 실행되어야 한다.	○	○			개인정보처리시스템의 개발 및 시험 시스템을 운영시스템과 분리하고 있는가?
									운영환경으로의 이관 절차를 수립·이행하고 있는가?
									운영환경에는 서비스 실행에 불필요한 파일을 제거하고 있는가?


8.6.4	시험 데이터 및 소스 프로그램 보안	운영데이터를 테스트 데이터로 사용할 시 보호조치에 관한 절차를 수립.이행하여야 한다. 또한, 소스 프로그램은 인가된 사용자만이 접근하도록 통제하고 운영환경에 보관하지 않아야 한다.	○	○		개인정보를 포함한 회사의 중요한 정보가 시스템 시험과정에서 유출되는 것을 방지하기 위하여 시험데이터는 임의의 데이터를 생성하거나 운영데이터를 가공하여 사용하고 있는가?
						불가피하게 운영데이터를 시험 환경에서 사용할 경우 책임자 승인 등의 절차 및 보호대책을 수립.이행하고 있는가?
						소스 프로그램의 변경 절차를 수립.이행하고 변경 이력을 관리하고 있는가?
						시스템 운영 장애 등 비상시를 대비하여 이전 시스템의 소스 프로그램 및 관련 정보를 보관하고 있는가?
						비인가자의 소스프로그램의 접근을 통제하기 위하여 절차를 수립.이행하고 있는가?
8.6.5	외주개발 보안	개인정보처리시스템의 개발을 외주 위탁하는 경우 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리.감독하여야 한다.	○	○		개인정보처리시스템 개발을 외주 위탁하는 경우 개발 시 준수해야할 보안 요구사항을 제안요청서에 기재하고 계약시에 반영하고 있는가?
						외주 위탁업체가 계약서에 명시된 보안요구사항을 준수하는 지 여부를 관리.감독하고 있는가?
						개인정보처리시스템 개발 완료 후 SW 보안취약점 제거여부 진단, SW 보안취약점 발견사항 조치 여부 등을 확인 후 검수.인수하고 있는가?

9.1	영상정보처리 기기 관리	9.1.1	영상정보처리기기 의 설치·운영 제한	영상정보처리기기 설치·운영 시, 설치 목 적에 따라 법적 요구사항(안내판 설치 등) 을 준수하고, 적절한 보호조치를 마련하 여야 한다.	○	○	○	공개된 장소에 영상정보처리기기를 설치·운영할 경우 법적으로 허용한 장소인지 검토하고 있는 가?
								영상정보처리기기를 설치·운영하는 자(영상정보처리기기운영자)는 정보주체(이용자)가 쉽게 인식 할 수 있도록 안내판 설치 등 필요한 조치를 하고 있는가?
								영상정보처리기기 운영자는 아래 사항이 포함된 영상정보처리기기 운영·관리 방침을 마련하여 운 영하고 있는가 ? - 영상정보처리기기의 설치 근거 및 설치 목적 - 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위 - 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법 - 정보주체(이용자)의 영상정보 열람 등 요구에 대한 조치 - 영상정보 보호를 위한 기술적·관리적 및 물리적 조치 - 그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항 등
		9.1.2	영상정보처리기기 설치·운영 사무의 위탁 관리	영상정보처리기기 설치·운영에 관한 사무 를 위탁하는 경우, 적절한 위탁절차를 마 련하여야 한다.	○			공공기관이 공개된 장소에 영상정보처리기기를 설치·운영하려는 경우 공청회·설명회의 개최 등의 법령에 따른 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하고 있는가?
								영상정보의 보관 기간을 정하고 있으며, 보관 기간 만료 시 지체없이 삭제하고 있는가?
								영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 관련 절차 및 요건에 따라 계약서에 반영하고 있는가?
		9.2.1	보호구역의 지정 및 관리	주요 설비 및 시스템을 보호하기 위하여 보호구역을 지정하고 보호구역 내의 작 업 절차를 포함하여 보호대책을 수립·이 행하여야 한다. 보호구역의 특성에 따라 보호설비를 갖추고 운영하여야 한다. 또 한 외부 집적정보통신시설에 위탁·운영하 는 경우 관련 요구사항을 계약서에 반영 하고 주기적으로 검토하여야 한다.	○	○	○	영상정보처리기기의 설치 및 관리에 관한 사무를 위탁한 경우, 안내판에 수탁기관의 명칭 등을 포 함하고 있는가?
								주요 설비, 시스템 및 문서를 보호하기 위하여 물리적 보호구역을 다음과 같이 정의하고 구역별 보호대책을 수립·이행하고 있는가? - 통제구역 : 주요 정보처리 설비 및 시스템 구역 등 - 제한구역 : 사무실 지역 등 - 접근구역 : 외부인 접근 구역
								화재, 전력 이상 등 재해에 대비하여 필요한 설비를 갖추고 운영절차를 수립·운영하고 있는가?
								주요 정보시스템을 외부 집적정보통신시설(IDC)에 위탁운영하는 경우, 물리적보호 및 개인정보보 호에 필요한 요구사항을 계약서에 반영하고 운영상태를 주기적으로 검토하고 있는가?
								정보시스템 도입, 유지보수 등으로 보호구역 내 작업이 필요한 경우 작업신청 및 수행 관련 절차 를 수립하고 작업기록을 주기적으로 검토하고 있는가?



9.3	매체 관리	9.3.2	휴대용 저장매체 관리	휴대용 저장매체를 통해 개인정보 유출이 발생하거나 악성코드가 감염되지 않도록 관리하고, 개인정보가 포함된 휴대용 저장매체는 안전한 장소에 보관하여야 한다.	○	○	○	외장하드, USB, CD 등 보조저장매체 사용, 보관, 폐기, 재사용에 대한 정책 및 절차를 수립·이행하고 있는가?
								개인정보처리시스템 및 개인정보 처리와 연관된 주요 자산(서버, 네트워크 장비, 보안장비 등)이 위치한 통제구역, 중요 제한구역 등에서 보조저장매체 사용을 제한하고 있는가?
								보조저장매체를 통한 악성코드 감염 및 개인정보 유출 방지를 위한 대책을 마련하고 있는가?
								보조저장매체 보유현황 및 관리실태를 주기적으로 점검하고 있는가?
								개인정보가 포함된 보조저장매체를 잠금장치가 있는 안전한 장소에 보관하고 있는가?
		9.3.3	이동컴퓨팅관리	보호구역 내 임직원 및 외부자의 이동컴퓨팅에 대하여 반·출입을 통제하고 기록·관리하여야 한다.	○	○	○	이동컴퓨팅기기(노트북, 태블릿, 스마트폰 등)를 보호구역에 반출입하는 경우 반출입 통제 및 보안 사고 예방절차를 수립·운영하고 있는가?
								주요 시설 및 개인정보자산이 위치한 통제구역 내 이동컴퓨팅기기의 반입을 제한하고 불가피하게 이동컴퓨팅기기를 사용하여야 하는 경우 사전 승인을 받고 상기 이동컴퓨팅기기 보안사고 예방절차를 이행한 후에 사용하고 있는가?
								이동컴퓨팅기기에 대한 반출입 통제 절차에 따라 반출입대장을 작성하는 등 이력 관리 및 주기적인 점검을 수행하고 있는가?





많이 부족한 자료 이지만, 나름대로 열심히 공부 하였고, 지금 이시간에도  
열심히 공부할 누군가와 공유 하고 싶어 작성 하게 되었습니다.

감사합니다 ^^

- 무료, 공개 스터디 카페 입니다.
- 배포 자유!! 하지만 수정은 금지 합니다. !! (힘들게 제작한 제작자 입니다)
- 비영리 목적으로 순수 하게 학습이 목표 입니다.
- 순수한 학습 목적 이기에 검색 엔진에서 검색이 되던 안되던, 신경 쓰고 있지 않습니다.
- 그렇기 때문에, 학습 하며 작성한 자료를 이미지 그대로 첨부 하였습니다.
- 순수한 학습 목적 이기에 검색 엔진에서 검색이 되던 안되던, 신경 쓰고 있지 않습니다.
- 잘못된 부분이나, 수정될 부분이 있으면 피드백 주시는되로 즉시 수정 하도록 노력하겠습니다.
- KISA, google, Naver 사의 위키피디아, 이미지 를 사용 하였습니다. 문제시, 즉시 삭제 하도록 하겠습니다.