



# ISMS정보보호 관리체계

**작성자 : Eric Yoon**

# 목 차

- 1. 개인정보 영향도 등급
- 2. PDCA 사이클
- 3. 거버넌스
- 4. 컴플라이언스
- 5. ISMS인증 이란 ??
- 6. ISMS인증심사 절차 1~4단계
- 7. 관리적, 물리적, 기술적 보호조치 보충설명
- 8. 인증 심사 항목 104 개

○ 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.

# 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. 계획 plan (①. 정책수립, 관리범위정함 ②. 관리범위내의 개인정보자산식별 ③. 개인정보흐름파악및 흐름도 작성 ④. 개인정보처리상에 문제점 파악.)
- 2. 실행 do (①. 식별된 정보자산을 바탕으로 위험평가 실시 ②. 정보보호대책의 수립과 이행)
- 3. 검증 check (①. 정보보호대책의 효과성확인 ②. 모니터링 정기적인점검, 감사실시등으로 체크)
- 4. 개선 act (잔여 위험에 대한 추가적인 조치사항 반영 ) **반영=순환 PDCA**

# 거버넌스 와 컴플라이언스 를 이해하고 나가자

## ○ 거버넌스 (governance) 란 무엇일까 ?

정부 와 비슷하지않은가 ???

## ○ 국가의 여러업무를 관리하기위해 정치,경제및 행정적권환을 행사하는방식으로써,

일종의 국정관리 체계라고 의미를 생각하자.

현재,우리는 정보보안을 말하고 있으므로 IT, Security 법,명령등을 준수 한다라고 해석 하면될것같다.

IT 거버넌스 와 컴플라이언스 ,

Security 거버넌스 와 컴플라이언스 에 대해 알아보도록 하자.

# 거버넌스

## 거버넌스(Governance)

IT Governance

정보기술(IT) 자원과 정보, 조직을 기업의 경영 전략 및 목표와 연계

경쟁 우위를 확보

의사결정 및 책임에 관한 프레임워크

이사회와 경영진의 책임 아래 수행되는 기업 지배 구조의 일부로 존재

리더십, 조직 구조, 프로세스 통제, 관리 체제로 구성

Security  
Governance

IT Governance

## 거버넌스(Governance)

Security  
Governance

최고 경영층의 정보보호에 대한 전략과 통제체계를 규정하는 보안정책 체계

정보보호는 기술적인 이슈가 아닌 전략적 이슈

법적인 문제임을 인식하는 것

정보보호에 대한 지시와 통제 수행



# 컴플라이언스 ?

## 컴플라이언스(Compliance)

IT Compliance

Security  
Compliance

각종 법, 제도적 규제 및 권고의 철저한 대응

각 나라별, 글로벌 감독당국이 제시한 각종 요건 만족

기업의 정보시스템과 업무프로세스 재정비

## 컴플라이언스(Compliance)

IT Compliance

Security  
Compliance

각종 법, 제도적 규제 및 권고의 철저한 대응

해당되는 법, 규제 요건 만족

기업의 정보보호 관리 프레임워크 구축, 운영



Governance 강화 측면

개인정보 법규제의  
강화에 맞춘  
보안관리 노력 필요

Compliance 강화 측면

ISMS 인증 의무화  
대상자에 대한  
강화된 정보보호 노력 요구

정보보호의 노력

법적으로 인정

정보보호 관리증적  
(Evidence)

정보보호 관리  
업무프로세스 정립

- 정보보호를 위해서는 거버넌스와 컴플라이언스의 강화가 필요하다.

# 정보보호관리체계 인증의 필요성

## 법률 등 컴플라이언스 측면

1

### 거버넌스(Governance) 강화 측면

- 영업비밀보호법으로부터 보호받기 위한 **회사의 보안관리 노력 강구**
- 법인 또는 개인이 위반 행위를 방지하기 위해 해당 업무에 관해 주의와 감독을 게을리하지 않은 경우 **양벌 규정에 대한 예외 적용**

2

### 개인정보 포함 인터넷 침해사고에 관련된 컴플라이언스(Compliance) 측면

- 정보통신서비스제공자는 **정보통신망법의 의무를 충실히 이행**
- 교육, 의료, 공공 부문 등 개인정보를 취급하는 모든 경우에는 **개인정보보호법을 지켜야 함**

# 정보보호관리체계 인증의 필요성

+ 법률 등 컴플라이언스 측면 +

3 2013년부터 정보통신망법 시행에 따른 정보보호 관리체계(ISMS) 인증제도 의무화

➤ 기존 안전진단 대상 사업자들은 강화된 정보보호 관리체계 인증을 의무적으로 받아야 함

4 개인정보보호법 및 정보통신망법 등 정보보호 관련 법률 강화

5 사회적으로 정보보호체계 수립 및 이행에 대한 요구 강화

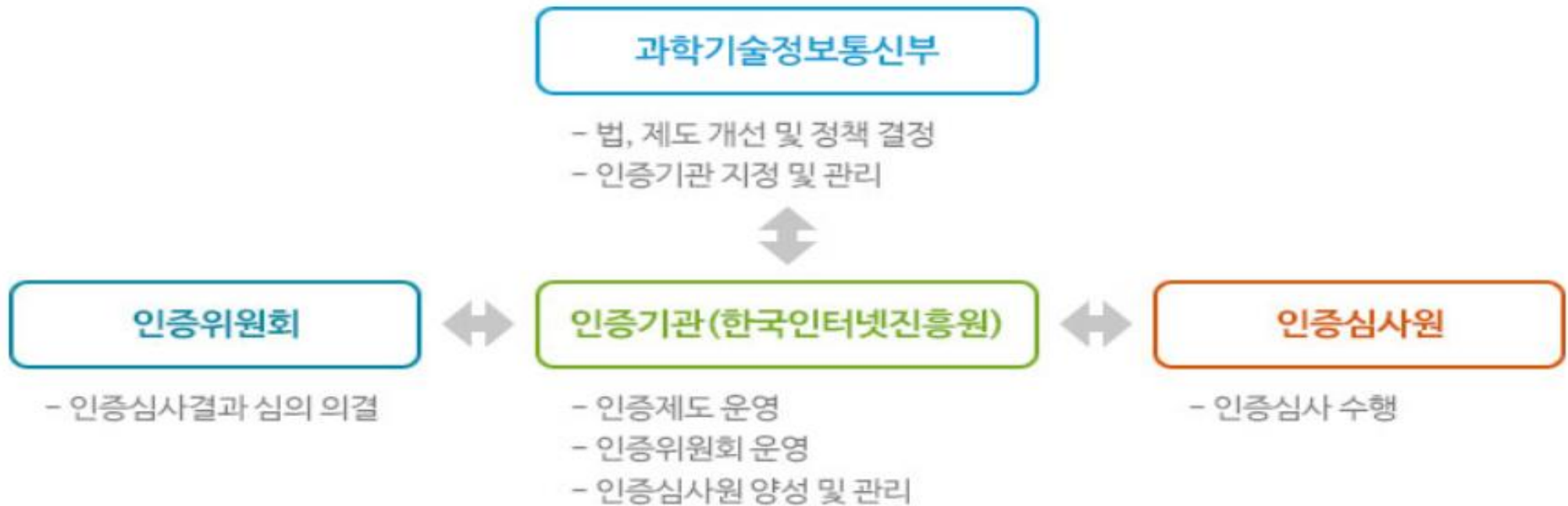
# ISMS 은 무엇인가요 ?

## 인증제도

- 기업이 주요 정보자산을 보호하기 위해 수립 · 관리 · 운영하는 정보보호 관리체계가 인증기준에 적합한지를 심사하여 인증을 부여하는 제도
- **ISMS 법적근거**
  - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 47조
  - 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제47조~54조
  - 정보보호 관리체계 인증 등에 관한 고시



## ■ 인증체계



- 인증제도의 객관성 및 신뢰성 확보를 위해 정책기관, 인증위원회를 분리하여 운영
- 과학기술정보통신부는 인증제도를 관리·감독하는 정책기관
- 한국인터넷진흥원은 인증기관으로서 인증제도 운영
- 산업계, 학계 등 관련 전문가 10명 이내로 인증위원회를 구성하여 인증결과 심의
- 인증심사팀은 인증심사원 양성교육을 수료하고 자격요건을 갖춘 자들로 구성

# ISMS 은 무엇인가요 ?

## ■ 인증대상자

### 자율신청

정보보호 관리체계를 구축, 운영하는 기업(기관)은 의무 대상이 아니더라도 인증 취득을 희망하는 경우 자발적 신청하여 인증취득 가능

### ISMS인증 의무대상자(정보통신망법 제47조 2항)

인증 의무대상자 확인 및 책임은 기업(기관)에 있으므로 스스로 의무대상 여부를 확인하여 인증 취득 필요

대상자 기준	세부분류 (정보통신서비스제공자)	비고
(ISP)전기통신사업법의 전기통신 사업자로 전국적으로 정보통신망 서비스를 제공하는 사업자	인터넷접속서비스, 인터넷전화서비스 등	서울 및 모든 광역시에서 정보통신망 서비스 제공(SKT,SK브로드 밴드,KT,LGU+등)
(IDC)타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자	서버호스팅, 코로케이션 서비스 등	정보통신서비스부문 전년도 매출액 100억 이하인 영세 VDC 제외
(매출액 및 이용자기준)연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신 서비스 매출액 100억 또는 이용자수 100만 명 이상인 사업자	인터넷쇼핑몰, 포털, 게임, 예약, Cable-SO 등	정보통신서비스 부문 전년도 매출액 100억 이상 또는 전년도말 기준 직전 3개월간 일일 평균 이용자수 100만명 이상
	상급종합병원 대학교	직전연도12월31일기준으로 재학생 수가 1만 명 이상인「고등교육법」제2조에 따른 학교

의무대상자 미인증시 3,000만원 이하의 과태료 (정보통신망법 제 76조 근거)



## ISMS 인증취득 시 혜택

구분	시행기관	혜택
평가항목	과학기술정보통신부	공공부문 정보시스템기획·구축·운영 사업자, SW개발사업자 선정 시 '소프트웨어 기술성 평가 기준'의 평가항목(기밀보안)에 ISMS 인증취득시 만점(최대5점)부여
		보안관제 전문업체 지정시 '보안관제수행능력평가기준'의 정보보호 인증기업(보안관리체계 보유기업)항목에 만점(최대5점)부여
		정보보호 전문 서비스 기업 지정시 '업무수행 능력심사 세부평가 기준'의 정보보호 인증기업(보안관리체계 보유기업)항목에 만점(최대5 점)부여
	KISA	정보보호대상 평가 시 가점 부여
	한국기업지배구조원	상장기업대상 ESG(환경, 사회, 지배구조)평가 일부항목 대체
요금할인	보험사	정보보호 관련 보험(배상책임보험 등)가입시 할인
권고	국토교통부	유비쿼터스 도시 기반 시설에 대해 정보보호 관리체계(ISMS)인증취득을 권고
	교육부	사이버 대학에 대하여 정보보호 관리체계 인증의 취득을 권고
ISMS인증 수수료 할인	KISA	중소기업 기업 할인(매출액 100억 미만, 30%)

# ISMS 인증심사 기준

## 정보보호관리체계 인증 구성 요소



# ISMS 인증심사 기준

## 정보보호 관리과정

정보보호 정책 수립 및 범위 설정

경영진 책임 및 조직 구성

위험 관리

정보보호 대책 구현

사후 관리

5단계 12개 인증기준

## 정보보호 대책

1. 정보보호정책

2. 정보보호 조직

3. 외부자 보안

4. 정보자산 분류

5. 정보보호 교육

6. 인적 보안

7. 물리적 보안

8. 시스템 개발보안

9. 암호 통제

10. 접근 통제

11. 운영 보안

12. 침해사고 관리

13. IT 재해 복구

13분야 92개 인증기준

## 그림 1.정보보호 관리과정에대해 알아보자

- 총5단계 12개의 인증 기준이 있는 정보보호 관리과정에 대해 각 단계별로 알아보도록하자.
- 3단계의 위험관리 부분에 대해서는 위험분석 부분에 따로 자세하게 만든 자료를 참고 하도록 하자.



# 1.정보보호 관리과정 세부사항

## 정보보호 관리과정

### 정책 수립 및 범위 설정

조직이 수행하는 모든 정보보호 활동 근거를 포함하는 정보보호 정책이 수립되었는지 확인

정보보호 관리체계 범위를 설정, 범위 내 모든 자산을 식별해 문서화 했는지 확인

### 경영진 책임 및 조직 구성

### 위험관리

### 정보보호 대책 구현

### 사후관리

## 정보보호 관리과정

### 정책 수립 및 범위 설정

### 경영진 책임 및 조직 구성

정보보호 활동 전반에 경영진의 참여가 있었는지 확인

정보보호 관리체계가 지속적으로 운영이 가능하도록 정보보호 조직을 구성하고 자원이 할당되었는지 확인

### 위험관리

### 정보보호 대책 구현

### 사후관리

# 1.정보보호 관리과정 세부사항

## 정보보호 관리과정

정책 수립 및 범위 설정

경영진 책임 및 조직 구성

위험관리

적절한 위험관리 방법 선정

전문인력 구성, 기간, 대상, 방법, 예산 등을 구체화한  
위험관리계획의 수립 여부 확인

정보보호 대책 구현

사후관리

## 정보보호 관리과정

정책 수립 및 범위 설정

경영진 책임 및 조직 구성

위험관리

전 영역에 대한 위험 식별 및 평가를 연 1회 이상 수행하고  
수용 가능한 위험수준(DoA)을 설정하여 관리

수용 가능한 수준으로 감소시키기 위한  
정보보호대책 선정 및 이행계획 수립 확인

정보보호 대책 구현

사후관리



# 1.정보보호 관리과정 세부사항

## 정보보호 관리과정

정책 수립 및 범위 설정

경영진 책임 및 조직 구성

위험관리

정보보호 대책 구현

정보보호 대책 이행계획에 따른 효과적인 구현 및 보고

운영 및 시행부서 담당자를 대상으로  
관련내용을 공유하고 교육 수행

사후관리

## 정보보호 관리과정

정책 수립 및 범위 설정

경영진 책임 및 조직 구성

위험관리

정보보호 대책 구현

사후관리

법적 요구사항 준수 검토 수행

정보보호 관리체계를 재검토하고 개선함

정기적인 내부감사를 통해 정책 준수 상황 확인

## 이번에는 2.정보보호 대책에 대해알아보자. 정보보호대책에는 크게 2가지로 나눌수 있다.

- 13개분야 92개 인증 기준이 있는 정보보호대책에 대해  
알아보자.
- 정보보호대책에는 크게 2가지로 나눌수 있다.
  1. 조직적/관리적 통제 –  
(정보보호정책,정보보호조직,외부자보안,정보자산 분류)
  2. 운영적/기술적 통제 –  
(정보보호교육,인적보안,물리적보안,시스템개발보안,암호  
통제,접근통제,운영보안,침해사고관리,IT재해복구)

## 2.정보보호 대책 세부사항

### 정보보호 대책

#### 조직적/관리적 통제

정보보호 정책

정보보호 조직

외부자 보안

정보자산 분류

### 정보보호 대책

#### 운영적/기술적 통제

정보보호 교육

암호 통제

인적 보안

접근 통제

물리적 보안

운영 보안

시스템 개발 보안

침해 사고 관리

IT 재해복구

# ISMS인증 절차

ISMS 인증 프로세스

인증  
준비 단계

ISMS  
구축단계

ISMS  
운영단계

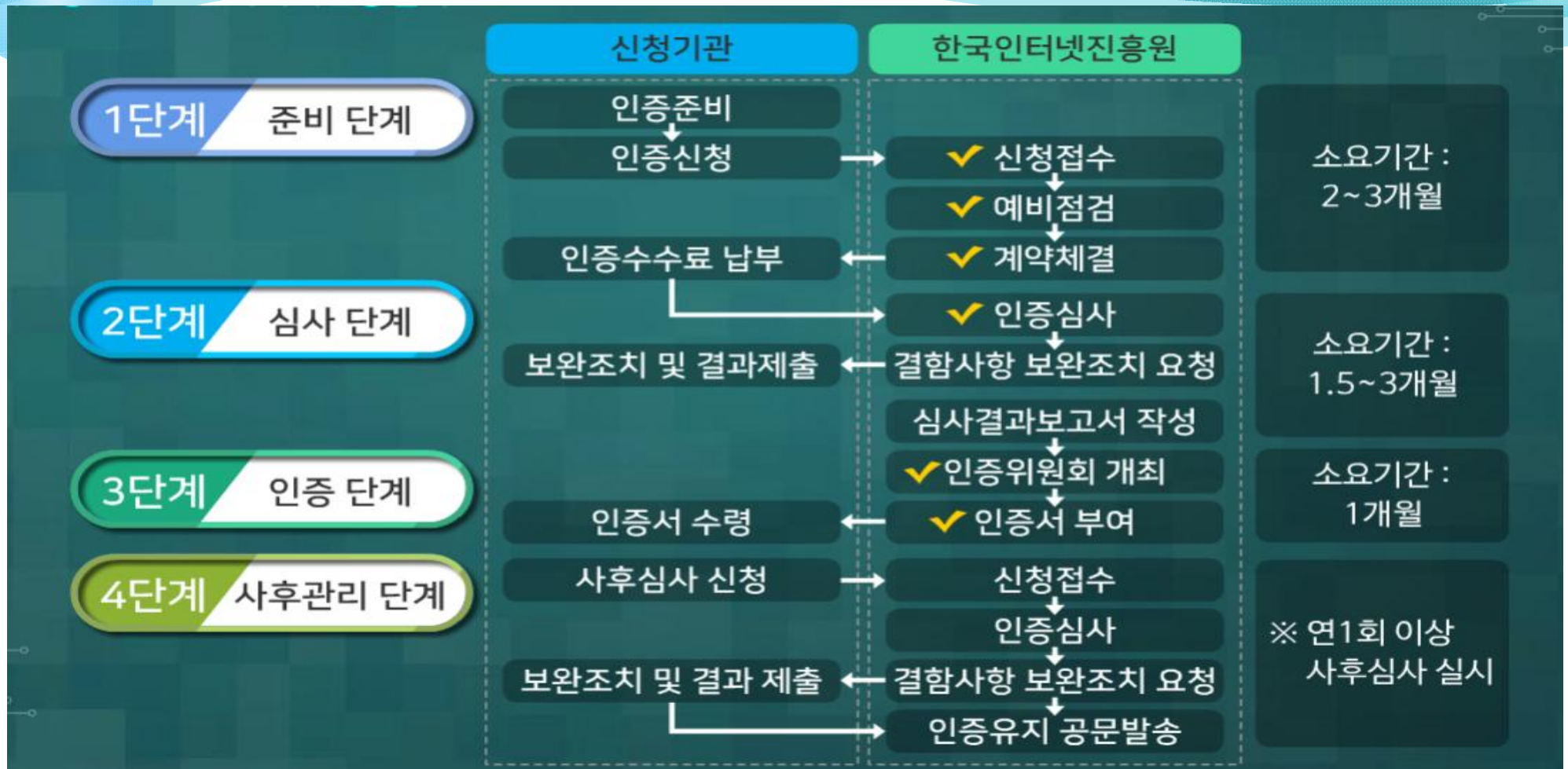
인증신청  
및  
심사단계

심사결과  
보완  
조치단계

사후관리  
단계

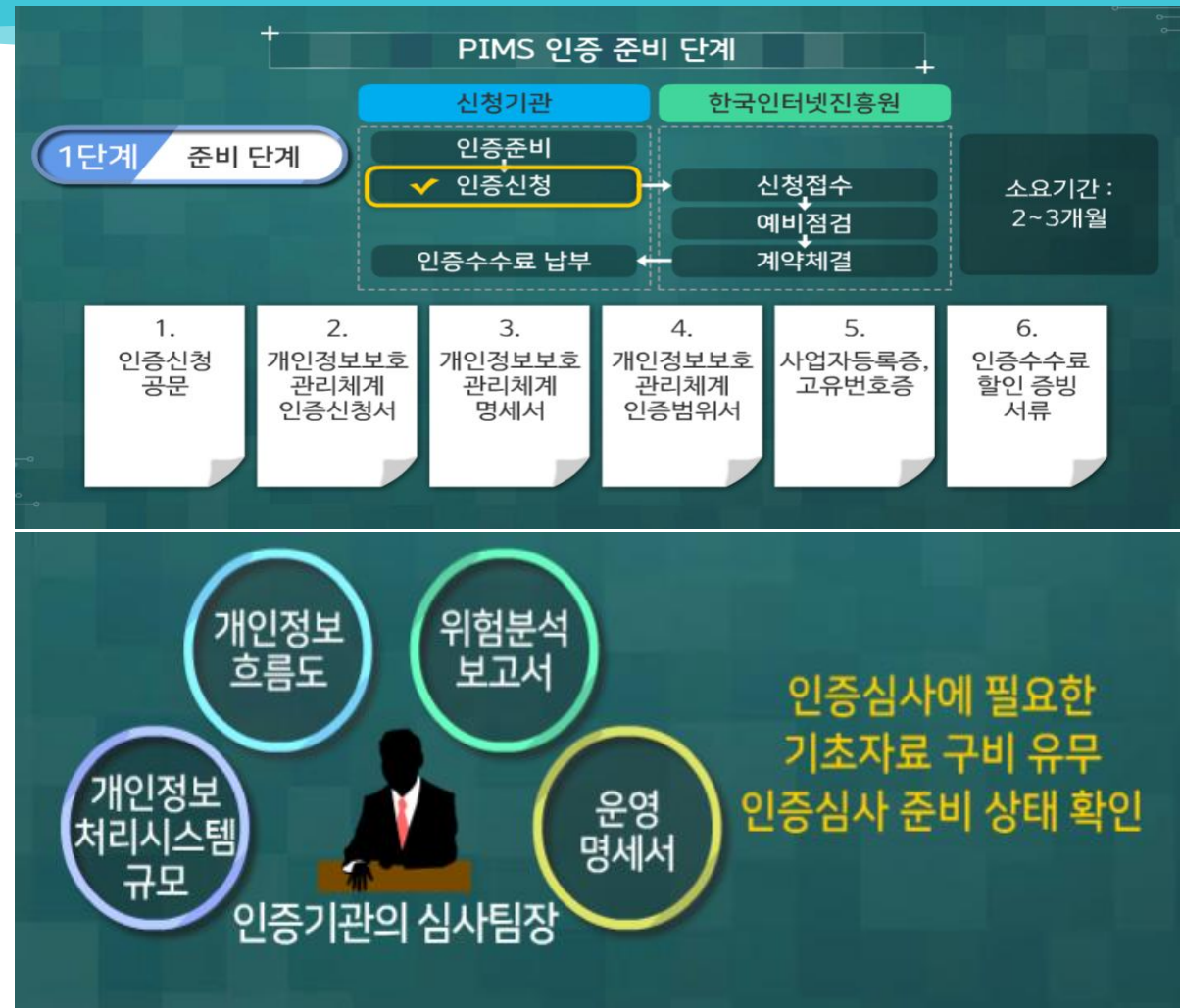


# ISMS 인증 절차를 한번 보자



# 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.





## 인증에 필요한 기본적인 문서목록

- 1 정보보호정책서
- 2 위험분석, 평가 보고서
- 3 정보보호계획서
- 4 정보보호대책명세서
- 5 ISMS 내부 감사 결과보고서
- 6 ISMS와 관련이 있는 주요 문서 목록

## 1-1. 인증 신청 제출 서류 꼭 암기하자

### 인증 신청 제출 서류

1.  
개인정보보호  
관리체계  
인증신청서

2.  
개인정보보호  
관리체계  
명세서

3.  
사업자등록증,  
고유번호증

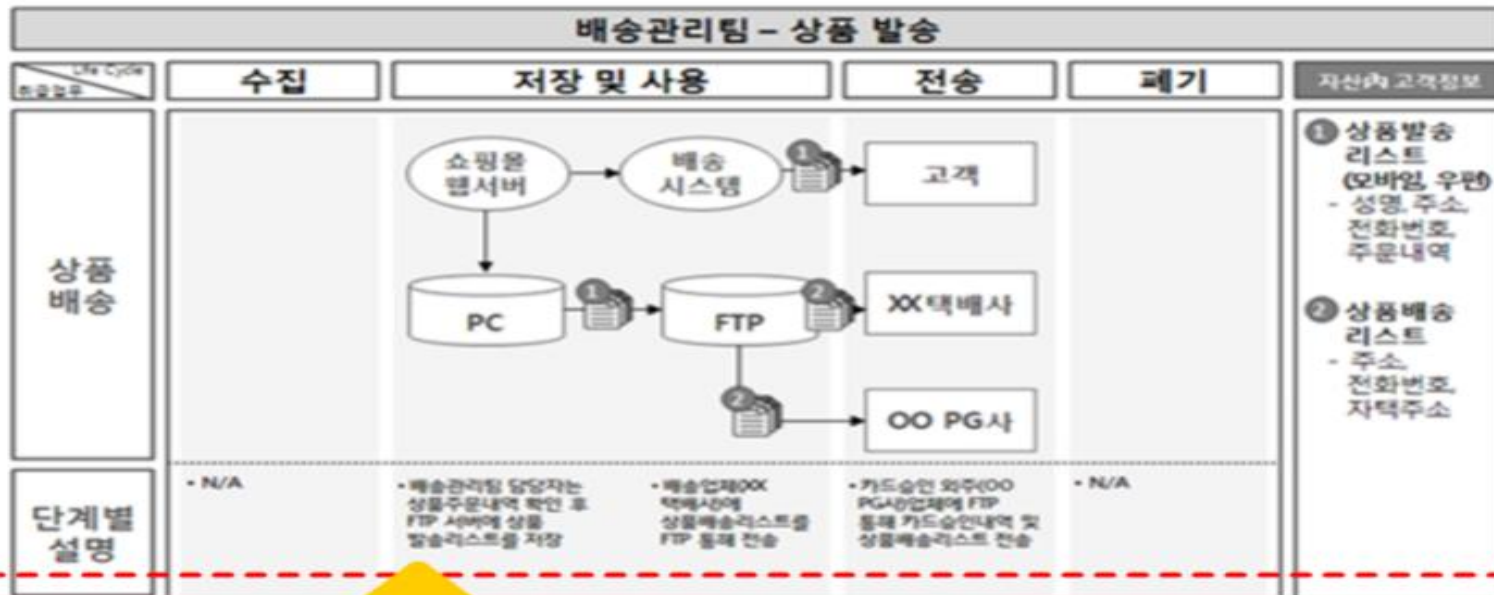
4.  
중소기업·  
소상공인  
증빙서류  
(해당 사업자)

- 인증신청 제출 필수 서류 3
- 1. ISMS인증신청서
- 2. 정보보호 관리체계 명세서
- 3. 사업자등록증

# 흐름도 예시

## 개인정보보호 관리체계 명세서

서비스 중 특정 업무의 개인정보 흐름도(업무별 흐름분석) 작성 예시



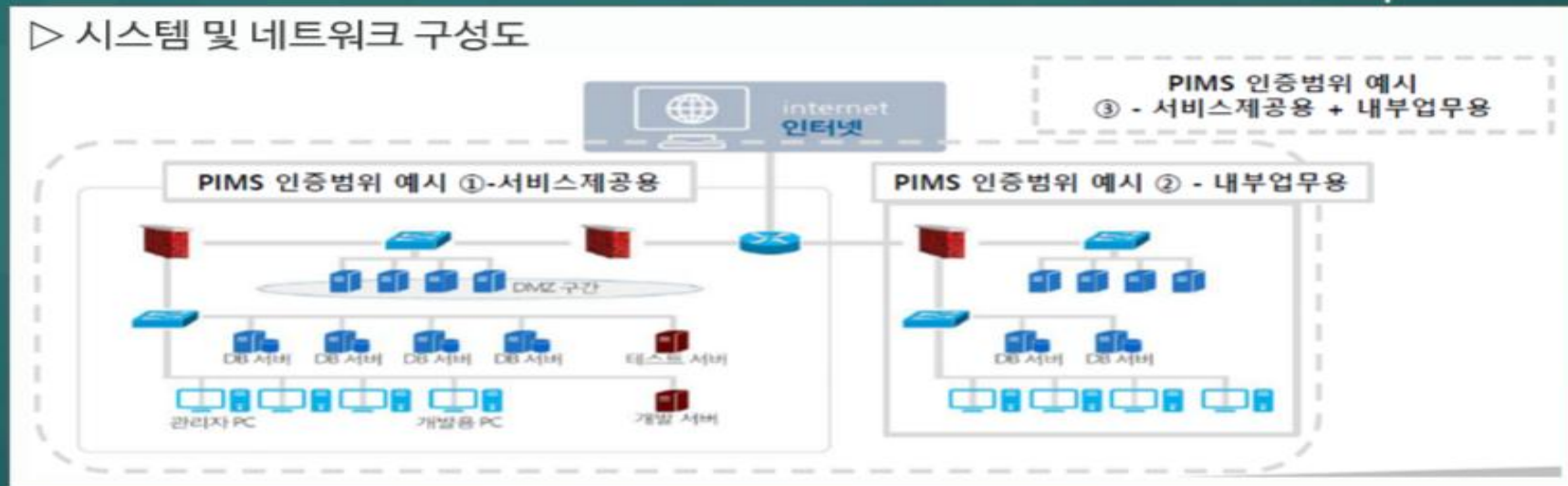
서비스 중 특정 업무의 개인정보 흐름을 파악할 수 있는 개인정보 취급업무별 개인정보 흐름도 작성



# 네트워크 구성도 예시

## 개인정보보호 관리체계 명세서

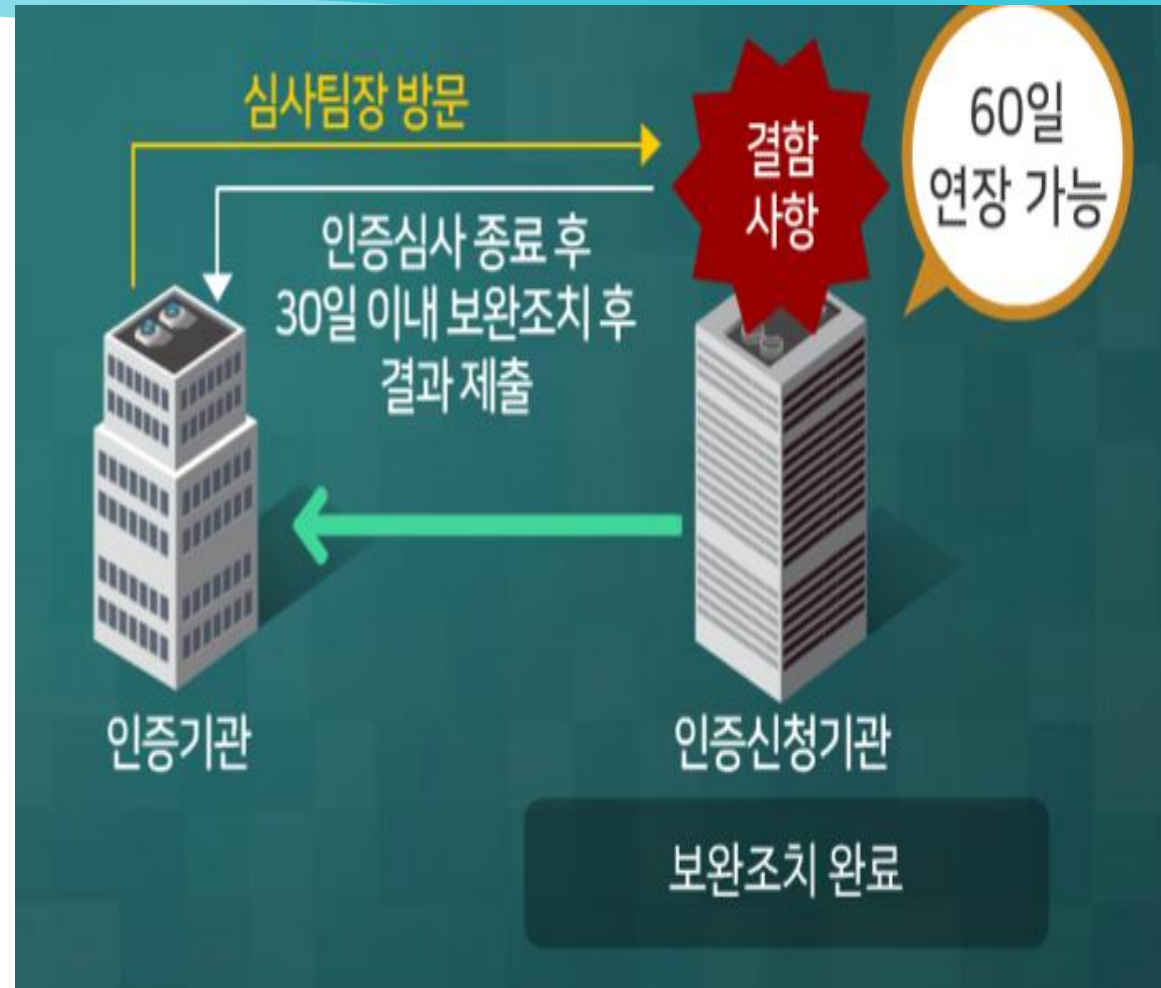
### ▷ 시스템 및 네트워크 구성도



- 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

- 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

# 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.

- ISMS 심사항목 총 104 개 이다
- 정보보호 관리과정 5단계 12 개 인증
- 정보보호대책 13 분야 92개 인증
- 이것만 기억하자.
- 수고 하셨습니다. ^^



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.