정보보안 관리 및 법규 정리

정보보안 기사/산업기사

JMoon

1. **정보보호 관리**

1-1 정보보호 관리의 개념

정보보호 관리 이행을 위한 6단계 활동
정보보호 정책 및 조직수립
정보보호 범위 설정
정보자산의 식별
위험관리
구 현
사후관리활동

1-2 정보보호 정책 및 조직

정책(Policy)의 의미 : 정책이라 함은 기업(기관)이나 조직에 있어서 최상위 수준 경영진의 전략적인 사고의 문서화된 표현을 말함

1-3 정책의 유형

하향식 유형 : 상위 정책으로부터 하위수준의 정책을 도출
상향식 유형 : 기업의 정책을 기존 정책들을 종합하여 수립하는 방식

1-4 위험관리

위험관리의 정의 : 조직의 자산에 대한 위험을 수용할 수 있는 수준으로 유지하기 위해 자산에 대한 위험을 부석하고 이러한 위험으로부터 자산을 보호하기 위해 비용대비 효과적인 보호대책을 마련하는 일련의 과정을 말함
위험관리 전략 및 계획 수립 -> 위험분석 -> 위험평가 -> 정보보호 대책수립 -> 정보보호 계획수립

1-5 위험의 구성요소

위험 = 발생가능성 X 손실의 정도
자산 : 자산은 조직이 보호해야할 대상으로 정보,하드웨어 등 조직 운영과정에서 획득한 인적,물적 또는 유형, 무형의 재화나 서비스를 말함
위협 : 자산에 손실을 초래할 수 있는 원치 않는 사건의 잠재적 원인이나 행위자로 정의
취약성 : 자신의 잠재적 속성으로 위협의 이용 대상으로 정의되지만 정보보호 대책 미미로도 정의
정보보호대책 : 위협에 대응해 자산을 보호하기 위한 물리적, 기술적, 관리적 대응책을 말함

1-6 위험분석 접근법

베이스라인 접근법 : 위험분석을 수행하지 않고 모든 시스템에 대하여 표준화된 보호대책을 체크리스트형태로 제공한다. 소규모 조직이나 대규모조직에 중요하지 않은 일반 자산에 대해 사용하는 접근법이다.
비정형 접근법 : 구조적인 방법론에 기반하지 않고 경험자의 지식을 사용해 위험분석을 수행하는 것 보안전문성이 높은 인력이 참여해야하고 그렇지 않으면 실패할 확률이 높다
상세위험분석 : 자산분석, 위협분석, 취약성 분석의 각단계를 수행하여 위험을 분석하는 것을 말함. 조직의 자산 및 보안 요구사항을 구체적으로 분석해 가장 적절한 대책을 수립할 수 있는 방법이다. 고급인적 자원이 필요하다.
복합접근법 : 상세 위험분석을 수행하고 그 외의 다른 영역은 베이스라인 접근법을 사용하는 방식

1-7위험분석 방법론

정량적 분석방법 : 위험을 손실액과 같은 숫자값으로 표현을 한다. 주로 미국에서 사용하는 방식중 하나
(ex:회사에 대한 위협이 토네이도다 회사 시설에 50%손상을 입힌다 회사 시설가치는 200,000원이고 토네이도 발생 확률은 10년에 한번 200,000 x 0.5 x 0.1 = 10,000원)
과거자료 분석법 : 과거의 자료를 통해 위험 발생 가능성을 예측하는 방법이다.
수학공식 접근법 : 위협 발생빈도를 계산하는 식을 이용해 위험을 계량화 하는 것
확률 분포법 : 미지의 사건을 확률적으로 편차를 이용해 최저, 보통, 최고 위험평가를 예측함
정성적 분석방법 : 어떠한 위험 상황에대한 부분을 매우높음, 높음, 중간, 낮음으로 표현한다.
델파이법 : 전문가 집단의 의견과 판단을 추출하고 종합하기 위해 동일한 전문가 집단에게 설문조사를 실시해 의견을 정리하는 방법
시나리오법 : 어떤 사실도 기대대로 발생하지 않는다는 조건하에서 특정 시나리오를 ㅌㅇ해 발생 가능한 위협의 결과를 우선순위로 도출해 내는 방법
순위결정법 : 비교우위 순위 결정표에 위험 항목들의 서술적 순위를 결정하는 방식

1-8 정량적 분석과 정성적 분석의 장단점

구 분	정량적 분석	정성적 분석
장점	객곽저인 평가기준이 된다. 성능평가가 용이 납득이 잘됨 금전적 가치, 백분율등으로 표현되어 이해가 쉬움	계산에 대한 노력이 적게듬 비용/이익을 평가할 필요없음
단점	계산이 복잡해 분석하는데 비용이 많이듬 수작업의 어려움으로 자동화도구 사용시 신뢰도가 벤더에 의존	위험분석 과정이 지극히 주관적이라 사람에 따라 달라짐 화폐로 표현하기 어렵다 위험관리 성능을 추적할 수 없다
기법	과거자료 분석법,수학공식 접근법, 확률분포법, 점수법	델파이기법,시나리오법,순위결정법,질문서법,브레인스토밍,스토리보딩

1-9목표 위험 수준 및 우선순위 설정

위험평가가 이루어지면 수용 가능한 위험수준과 우선순위를 결정하는 것이 중요

1-10 위험처리방법

조직이 수용가능한 위험을 넘어선다면 그 위험을 어떤 식으로 처리할 것인지 결정해야 함

위험수용 : 위험의 잠재 손실 비용을 감수하는 것으로 어떠한 대책을 도입하더라도 완전히 제거 할 수 없으므로 일정 수준 이하의 수준을 감수하고 사업을 진행하는 방법

위험감소 : 위험을 감소시킬 수 있는 대책을 채택하여 구현하는 것 이는 많은 비용이 소요되기 때문에 실제 감소되는 위험의 크기와 비교하여 비용분석을 실시

위험회피 : 위험이 존재하는 프로세스나 사업을 수행하지 않고 포기

위험전가 : 보험이나 외주등으로 잠재적 비용을 제3자에게 이전하거나 할당하는 것을 말한다.

1-10 통제구분

예방통제 : 발생 가능한 잠재적인 문제들을 식별하여 사전에 대처하는 능동적인 개념의 통제

탐지통제 : 예방통제를 우회하는 문제점을 찾아내는 통제를 탐지통제

교정통제 : 문제발생 원인과 영향을 분석해 교정하기 위한 조치가 필요한 통제

잔류위험 : 관리를 통해 사건 발생 가능성과 손실관점에서 위험을 허용하는 부분에 남아 있는 위험을 잔류 위험이라 함

1-11 업무연속성 관리

재난,재해나 테러등의 예기치 못한 위기 상황에서도 회사의 핵심 서비스와 제품생산 활동을 적시에 복구해 업무를 계속 수행할 수 있는 위기관리 능력

1-12업무연속성 관리의 단계

시작단계 : 업무 연속성 관리에 관한 정책을 수립하는 단계

전략수립단계 : 점재적인 영향 및 위험을 평가하고 프로세스 복구를 위한 여러 옵션들을 파악 평가하여 전략을 수립함

구현단계 : 업무복구를 위한 계획 및 절차를 작성하고 초기 시험을 수행함

운영관리단계 : 테스트,검토,유주보수하여 적절한 교육 및 훈련 프로그램을 운영

1-13 업무연속성 계획

각종 재해, 재난으로 인한 비상사태 발생시 조직의 핵심 업무를 지속하고, 적정시간 안에 순차적으로 비즈니스 사이클을 회복하는데에 있다.

1-14업무연속성 5단계 방법론

프로젝트 범위 설정 및 기획 : 범위, 조직, 시간, 인원 등을 정의하고 개시를 나타냄

사업영향평가 : 사건이 사업에 어떠한 영향을 주는지 이해를 돕기 위해 사용되는 문서를 작성하는 것이 목적// 재적정적 손실영향도를 파악

복구전략개발 : 전단계에서 수집한 정보를 활용해 복구 자원을 추정함

복구계획수립 : 실제 복구계획 수립단계

프로젝트수행 및 테스트 : 유지보수 활동현황을 포함해 향후에 수행할 엄격한 테스트 및 유지보수 관리 절차를 수립

1-15 재난복구계획

재난으로 인해 손실이 발생 중이거나 발생 후 수반되는 절차나 계획을 말함

1-16 재난복구계획(DRP)목표와 목적
파괴적 사건이 발생할 경우 결정해야 할 사항으로 인한 혼란을 줄이고 위기상황에 대처하기 위한 조직의 능력을 확장

1-17 핫사이트(Hot Site)
전원이나 난방 공기 청정기, 기능성 파일/프린터 서버와 단말기까지 모든 컴퓨터 설비를 완전히 갖추고 있는 사이트. 실제로 운영되는 환경과 동일한 상태로 관리
장점 : 사고 발생후 즉시 사이트 정상 가동
단점 : 고가의 대체 사이트 방안

1-18 웜사이트(Warm site)
핫사이트처럼 웜사이트도 전원,컴퓨터 등은 갖추어진 설비지만 애플리케이션이 설치되거나 구성되어 있지는 않다.
장점 : 핫사이트보다 경제적이다.
단점 : 신규 사이트 운영시 핫사이트보다 시간과 노력이 많이 사용

1-19콜드사이트(cold site)
3가지중에 가장 미비한 사이트지만 가장 많이 사용된다. 비상시 장비를 가져올 준비만 할뿐 어떤 컴퓨터 하드웨어도 사이트에 존재하지 않는다.
장점 : 비용과 정소선정
단점 : 보안과 복구불능

1-20 상호지원계약
유사한 컴퓨터 요구를 가지는 다른 회사와 계약하는 방법을 말한다. 다른 회사와 비슷한 하드웨어, 소프트웨어를 가지고 네트워크나 데이터 통신이 가능할 수 잇도록 한다.

1-21 OECD 정보보호 가이드라인
인식 : 참여자들은 정보시스템과 네트워크 보호의 필요성과 그 안전성을 향상시키기 위해 취할 수 있는 사항을 알아야함
책임 : 정보시스템과 네트워크 보호에 책임이 있다.
대응 : 정보보호 사고를 예방,탐지,대응하기 위해 적기에 협력해서 행동해야한다.
윤리 : 타인의 적법한 이익을 존중해야 한다.
민주성 : 정보시스템과 네트워크 보호는 민주주의 사회의 근본적인 가치들에 부합해야한다.
위험평가 : 참여자들은 위험평가를 시행해야한다.
정보보호의 설계와 이행 : 정보보호를 정보시스템과 네트워크의 핵심 요소로 수용하여야 한다.
정보보호 관리 : 정보보호 관리에 대해 포괄적인 접근 방식을 채택해야 한다.
재평가 : 정보시스템과 네트워크 보호를 검토하고 재평가하여 정보보호 정책, 관행, 조치, 절차를 적절히 수정해야한다.

1-22 유럽평가기준 (ITSEC)
유럽 공통 평가기준으로 ITSEC을 공동으로 마련하여 1991년에 발표함.

1-23 미국평가기준 (TCSEC)
미국에서 1985년 최초로 만들어진 일명 오렌지북이라 불리는 TCSEC이 있음.

1-24 보안성평가(Common Criteria / CC)
위와 같이 나라별, 지역별로 서로 다른 평가기준을 가짐에 따라 동일 제품에 대한 중복 평가 문제가 발생하였다. 이를 해결 하기위해 범세계적인 표준화 작업이 ISO와 같은 국제 표준화기구에 의해 1990년 경부터 진행되어 왔다.

1-25 CC인증 국제적 효력
우리나라는 국제상호인정협정(CCRA)회원국에 2006년 5월 3일 정식가입하였다.
CCRA에는 인증서발행국(CAP)과 인증서 수용국(CCP)으로 나뉘게 된다.
CAP : 국내에서 발행한 정보보호시스템 평가 인증서를 해외에서도 인정받게 됨
CCP : 정보보호 펴아 인증서를 발행하지 않고 수용하는 국가

1-26 인증체계 (BS7799)

조직의 정보를 체계적으로 관리하고 정보보안 사고를 예방하기 위해 영국에서 제정된 규정을 말함.

1-27 정보보호 관리체계 구성요소

분야	
정보보호 관리 과정	정보보호 정책수립, 관리체계 범위 설정, 정보보호 정책수립 및 범위 설정 경영진 책임 및 조직구성, 위험관리, 구현, 정보보호대책 구현, 사후 관리
문서화	문서요건, 문서의 통제, 운영기록의 통제
정보보호 대책	정보보호정책, 정보보호 조직, 외부자 보안, 정보자산 분류, 정보보호교육 및 훈련 정보보호 교유, 인적 보안, 물리적보안, 시스템개발 보안, 암호 통제 접근통제, 운영관리, 운영보안, 전자거래보안, 보안사고관리, 침해사고관리 검토, 모니터링, 감사, 업무연속성 관리, IT재해복구

2. **정보보호관련 법규**

2-1정보통신망 이용촉진 및 정보보호 등에 관한 법류(정보통신망법)

정보통신망의 개발과 보급 등 이용촉진과 함께 통신망을 통해 활용되고 있는 정보보호에 관해 규정한 법률이다.

1-2 시책내용

정보통신망에 관련된 기술의 개발,보그
정보통신망 표준화
정보내용물 및 제11조에 따른 정보통신망 응용서비스의 개발 등 정보통신망의 이용 활성화
정보통신망을 통해 수집, 처리, 보관, 이용되는 개인정보의 보호 및 그와 관련된 기술의 개발 보급
인터넷 이용의 활성화
정보통신망에서의 청소년 보호
정보통신망의 안전성 및 신뢰성 제고
그 밖의 정보통신망 이용촉진 및 정보보호 등을 위하여 필요한 사항

1-3개인정보보호

망법과 개인정보보호법은 다르다. 정보통신망법에서 개인정보보호에 대한 조항은 제4장에서 제시하고 있음.

1-4 개인정보수집, 이용 및 제공

법률 조항	법률내용
제22조 개인정보의 수집,이용,동의 등	정보통신 서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음 각호의 모든 사항을 이용자에게 알리고 동의를 받아야한다. 1. 개인정보의 수집,이용목적 2.수집하는 개인정보의 항목 3. 개인정보의 보유, 이용기간
개인정보 수집시 고지 및 동의 사항	개인정보 수집 이용 목적, 수집하는 개인정보 항목, 개인정보 보유 이용 기간
동의 업싱 수집이용	계약을 이행하기 위해, 요금정산, 다른 법률에 규정

1-5 개인정보 수집 제한 등

법률 조항	법률내용
제23조 개인정보의 수집제한 등	정보통신서비스 제공자는 사상, 신념, 가족 및 친인척관계, 학력 병력, 기타 사회활동 경력등 개인의 권리,이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 안된다.
개인정보수집금지	사생활을 뚜렷하게 침해할 우려가 있는 경우
수집허용	이용자 동의, 다른 법률에 허용된 경우
서비스거부	이용자가 최소한 개인정보외에 제공하지 않는다는 이유로 서비스 거부 안됨.

1-6주민등록번호 사용제한

법률 조항	법률내용
제23조의2 주민등록번호의 사용제한	정보통신서비스제공자는 다음 각호 어느 하나에 해당하느 경우를 제외하고 이용자의 주민등록번호를 수집, 이용 할 수 없다 1. 제23조3에 다라 본인확인기관으로 지정받은 경우 2. 법령에서 이용자의 주민등록번호 수집,이용을 허용한 경우 3. 영업상 목적을 위해 이용자의 주민등록번호 수집, 이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는 경우
제23조의 2 주민등록번호의 사용제한	제1항 제2호 또는 제3호에 따라 주민등록번호를 수집, 이용할 수 있는 경우에도 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법

1-7 개인정보의 제공 동의

법률 조항	법률내용
제24조의 2 개인정보의 제공동의 등	정보통신서비스제공자는 이용자의 개인정보를 제 3자에게 제공하려면 제22조 제2항 제2호 및 제3호에 해당하는 경우 외에는 다음 각호의 모든 사항을 이용자에게 알리고 동의를 받아야한다. 1.개인정보를 제공받는자 2.개인정보를 제공받는 자의 개인정보 이용목적 3. 제공하는 개인정보의 항목 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용기간

1-8개인정보취급 위탁

법률 조항	법률내용
제 25조 개인정보 취급 위탁	업무를 위탁하는 경우 이용자에게 알리고 동의를 받아야 하고 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 같음 1. 개인정보 취급위탁을 받는자 2. 개인정보 취급위탁을 하는 업무의 내용

＊위탁과 제3자 제공 차이

	위탁	3자제공
업무처리	주는자	받는자
책임	위탁자책임	수탁자책임

1-9개인정보의 제공 동의

법률 조항	법률내용
제24조의2 개인정보의 제공동의	다음 각호의 모든 사항을 이용자에게 알리고 동의를 받아야한다. 1.개인정보를 제공받는 자 2.개인정보를 제공받는 자의 개인정보 이용목적 3. 제공하는 개인정보의 항목 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용기간

개인정보 제3자 제공에 대한 부분으로 이용자에 대한 개인정보를 제3작에게 제공할 경우가 있다. 이럴 경우에는 위 법률에 명시한 법률을 지켜야 한다. 제 3자에게 제공시에도 제공받는 자, 이용목적, 개인정봄항목, 보유 및 이용기간등을 이용자에게 알리고 동의 받아야한다.

1-10 개인정보 관리책임자 지정

1. 임원 2. 개인정보와 관련하여 이용자의 고충처리를 담당하는 부서의 장

＊개인정보책임자 지정예외 : 상시종업원 5명미만, 다만 인터넷 사업시 상시 종업원 5명미만이며, 전년도 말 기준 직전 3개월 일일평균 이용자 1천명 이하

1-11 개인정보 누출 등의 통지신고

법률 조항	법률내용
제27조 3 개인정보누출등의 통지, 신고	개인정보의 분실,도난,누출 사실을 안 때에는 지체 없이 다음 각호의 모든 사항을 해당 이용자에게 알리고 방통위 또는 한국인터넷진흥원에 신고하여야 한다. 1. 누출등이 된 개인정보 항목 2. 누출등이 발생한 시점 3. 이용자가 취할 수 있는 조치 4. 정보통신 서비스 제공자등의 대응조치 5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처

1-12 개인정보 이용내역의 통지

법률 조항	법률내용
제 30조의 2 개인정보의 이용내역 통지	수집한 이용자 개인정보의 이용내역을 주기적으로 이용자에게 통지하여야 한다. 다만 연락처 등 이용자에게 통지할 수 있는 개인정보를 수집ㅎ바지 아니한 경우에는 그러지하지 아니 하다.

연락처 등 이용자에게 통지할 수 있는 개인정보를 수집하지 아니한 경우에는 통지하지 않아도 된다.

1-13손해배상 및 법정 손해배상 청구

법률 조항	법률내용
제32조 손해배상	정보통신서비스 제공자 등에게 손해배상을 청구 할 수 있다.
제32조의 2 법정손해배상의 청구	300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 정보통신서비스 제공자등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다. 1.정보통신서비스 제공자등이 고의 또는 과실로 이 장의 규정을 위반한 경우 2. 개인정보가 분실,도난,누출된 경우

1-14정보보호관리체계(ISMS)

ISMS의무 인증대상	1.정보통신망서비스를 제공하는자(ISP) 2.집적정보통신시설사업자(IDC) 3.정보통신서비스 부문 전년도 매출액이 100억원 이상인자 4. 전년도 말 기준 직전 3개월간의 일일평균 이용자수가 100만명 이상인자

1-15접근통제

고시조항	고시내용
제4조 접근통제	정보통신서비스 제공자 등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위해 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여한다. 개인정보취급자가 변경 되었을 경우 개인정보처리시스템의 접근 권한을 변경 또는 말소 한다. 최소 5년간 보관한다. 개인정보처리시스템에 대한 접속 권한을 IP주소등으로 제한하여 인가 받지 않는 접근을 제한한다. 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출시도를 탐지한다. 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리하여야 한다. 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성 비밀번호 유효기간은 설정하여 반기별 1회 이상 변경

1-16접속기록의 위,변조방지

고시조항	고시내용
제5조 접속기록의 위,변조 방지	개인정보치급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인,감독하여야 하며 시스템의 이상유무의 확인등을위해 최소 6개월 이상 접속기록을 보존, 관리

1-17개인정보 암호화

고시조항	고시내용
제6조 개인정보 암호화	비밀번호 및 바이오정보는 복호화 되지 아니하도록 일방향 암호화 하여 저장 1. 주민등록번호 2. 여권번호 3. 운전면허번호 4. 외국인등록번호 5. 신용카드번호 6. 계좌번호 7. 바이오정보

1-18 악성프로그램 방지

고시조항	고시내용
제7조 악성프로그램 방지	보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지

1-19개인정보 표시제한 보호 조치

고시조항	고시내용
제10조 개인정보 표시제한 보호조치	개인정보 업무처리를 목적으로 개인정보의 조회,출력등의 업무를 수행하는 과정에서 개인정보보호를 위해 개인정보를 마스킹하여 표시제한 조치를 취할 수 있다(박XX)

2-20 용어의 정의

용어의 정의	설명
정보통신기반시설	국가안전보장, 행정, 국방, 치안, 금융, 통신, 운송, 에너지등의 업무와 관련된 전자적 제어,관리시스템
전자적침해행위	정보통신기반시설을 대상으로 해킹, 바이러스, 논리, 메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의해 공격하는 행위
침해사고	전자적 침해행위로 인하여 발생한 사태

2-21 정보통신기반보호위원회

법률조항	법률내용
제3조 정보통신기반 보호위원회	위원회의 위원은 위원장 1인을 포함한 2인 이내의 위원으로 구성한다.

2-22 주요 정보통신기반 시설의 보호자원

법률조항	법률내용
제7조 주요 정보통신 기반 시설의 보호자원	기술적 지원을 요청하는 경우 국가정보원장에게 우선적으로 그 자원을 요청하여야한다. 1.도로, 철도, 지하철, 공항, 항만 등 주요 교통시설 2.전력, 가스, 석유등 에너지, 수자원 시설 3. 방송중계, 국가지도통신망 시설 4. 원자력, 국방과학, 첨단방위산업관련(정부출연연구기관의 연구시설)

2-23 전자서명의 효력

법률조항	법률내용
제3조 전자서명의 효력	다른 법령에서 문서 또는 서면에 서명, 서명날인 또는 기명날인을 요하는 경우 전자문서에 공인전자서명이 있는 때에는 이를 충족한 것으로 본다. 공인전자서명이 있는 경우에는 당해 전자서명이 서명자의 서명, 서명날인 또는 기명날인이고, 당해 전자문서가 전자서명된 후 그 내용이 변경되지 아니하였다고 추정한다. 공인전자서명외의 전자서명은 당사자간의 약정에 따른 서명, 서명날인 또는 기명날인으로서의 효력을 가진다.

∗공인인증기관으로 지정 받을 수 있는 자는 국가기관, 지방자치단체, 법인에 한하여 인증기관으로 지정 받을 수 있다.

2-24공인인증업무준칙

인증업무종류, 인증업무의 수행방법 및 절차, 공인인증역무의 이용조건, 기타 인증업무 수행에 관하여 필요한 사항.

2-25공인인증서 발급

법률조항	법률내용
제15조 공인인증서 발급	공인인증기관이 발급하는 공인인증서에는 다음 각 호의 사항이 포함되어야 한다. 1. 가입자의 이름 2. 가입자의 전자서명검증정보 3.가입자와 공인인증기관이 이용하는 전자서명 방식 4.공인인증서의 일련번호 5. 공인인증서의 유효기간 6. 공인인증기관의 명칭 등 공인인증기관임을 확인 할 수 있는 정보 7. 공인인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항 8. 가입자가 제3자를 위한 대리권 등을 갖는 경우 또는 직업상 자격등의 표시를 요청한 경우 9.공인인증서를 나타내는 표시

2-26 공인인증서 효력 소멸

공인인증서 유효기간이 경과한 경우
공인인증기관의 지정이 취소된 경우
공인인증서의 효력이 정지된 경우
공인인증서가 폐지된 경우

2-27 개인정보보호 8원칙

수집제한의 원칙 : 목적에 필요한 최소한 범위 안에서 적법하고 정당하게 수집
정보정확성의 원칙 : 처리 목적 범위 안에서 정확성, 안정성, 최신성 보장
목적 명확성의 원칙 : 처리 목적의 명확화
이용제한의 원칙 : 필요 목적 범위 안에서 적합하게 처리, 목적 외 활용 금지
안전보호의 원칙 : 정보주체의 권리침해 위험성 등을 고려, 안전성 확보
공개의 원칙 : 개인정보 처리 사항 공개
개인참가의 원칙 : 열람청구권 등 정보주체의 권리 보장
책임의 원칙 : 개인정보처리자의 책임준수 실천 신뢰성 확보 노력

2-28 개인정보 보호위원회

법률조항	법률내용
제7조 개인정보 보호 위원회	개인정보보호에 관한 사항의 심의, 의결하기 위해 대통력 소속으로 개인정보보호 위원회를 둔다. 보호위원회는 위원장 1명, 상임위원 1명을 포함한 15명 이내의 위원으로 구성한다. 위원장과 위원의 임기는 3년으로 하되 1차에 한하여 연임 가능하다. 보호위원회의 회의는 위원장이 폴오하다고 인정하거나 재적위원 4분의 1 이상 요구가 있을 경우에 위원장이 소집한다. 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 의결한다.

2-29 개인정보 수집, 이용

법률조항	법률내용
제15조 개인정보의 수집,이용	개인정보처리자는 다음 각 호의 어느 하나에 해다하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다. 1. 정보주체의 동의를 받은 경우 2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위해 불가피한 경우 3.공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우 4. 정보주체와의 계약의 체결 및 이행을 위해 불가피하게 필요한 경우 5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로써 명백히 정보주체 또는 제 3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 6. 개인정보처리자의 정당한 이익을 달성하기 위해 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우, 이 경우 개인정보처리장의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니한 경우에 한한다. 개인정보처리자는 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야한다. 1. 개인정보의 수집, 이용 목적 2. 수집하려는 개인정보의 항목 3. 개인정보의 보유 및 이용 기간 4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용(개인정보법에 추가/ 망법엔 이항목이 없음)

2-30 개인정보 수집 제한

법률조항	법률내용
제16조 개인정보의 수집제한	개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야한다. 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부해서는 안된다.

＊개인정보를 수집할 때 최소한으로 수집을 해야 하고 그 최소한의 입증책임은 개인정보처리자가 입증해야한다.

＊개인정보 라이프 사이클 : 수집 -> 이용 -> 제공 -> 파기

2-31 민감정보처리제한

법률조항	법률내용
제23조 민감정보 처리제한	사상,신념,노동조합,정당의가입,탈퇴,정치적 견해, 건강, 성생활등에 관한 정보 그 밖에 정보 주체의 사생활을 현저히 침해할 우려가 있는 정보는 처리하여서는 안된다.

＊법령이나 정보주체의 동의시에는 별도의 동의를 받아야함(의료법)

2-32고유식별정보

주민등록번호, 여권번호, 운전자면허번호, 외국인등록번호는 원칙적으로 수집 불가능하다.

법률조항	법률내용
제24조의 2 주민등록번호의처리 제한	다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다. 1. 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우 2. 정보 주체 또는 제 3자의 급박한 생명, 신체, 자산의 이익을 위해 명백히 필요한 경우 제1호 및 제2호에 준해 주민등록번호 처리가 불가피한 경우로서 행정자치부령으로 정하는 경우 주민등록번호가 분실, 도난, 유출, 변조 또는 훼손되지 아니하도록 암호화조치를 통해 안전하게 보관해야한다.

2-33 영상처리정보기기의 설치 운영제한

법률조항	법률내용
제25조 영상정보처리기기의 설치, 운영제한	다음 각호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치,운영해선 안된다. 1. 법령에서 구체적으로 허용하고 있는 경우 2. 범죄의 예방 및 수사를 위해 필요한 경우 3. 시설 안전 및 화제 예방을 위해 필요한 경우 4. 교통단속을 위해 필요한 경우 5. 교통정보의 수집,분석 및 제공을 위해 필요한 경우 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며 녹음 기능은 사용할 수 없다.

＊

망법	개인법
이용자	정보주체
취급방침	처리방침
개인정보관리책임자	보호책임자