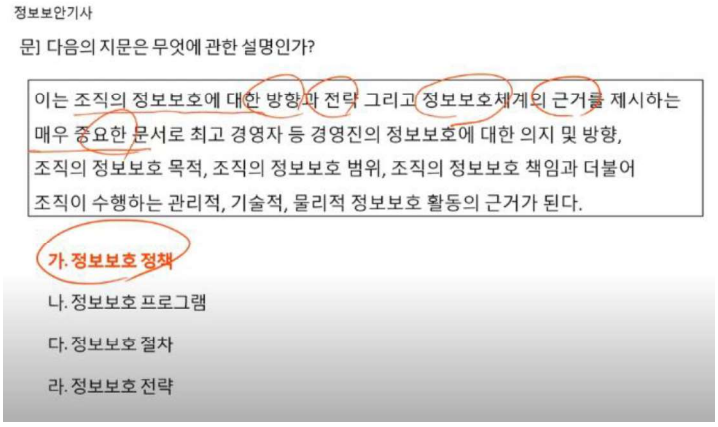
정보보호 정책

정보보호 정책이란 이는 조직의 정보보호에 대한 방향과 전략 그리고 정보보호체계의 근거를 제시하는 매우 중요한 문서로 최고 경영자 등 경영진의 정보보호에 대한 의지 및 방향, 조직의 정보보호 목적, 조직의 정보보호 범위, 조직의 정보보호 책임과 더불어 조직이 수행하는 관리적, 기술적, 물리적 정보보호의 활동의 근거가 된다.

조직의 내외부 환경과 업무성격에 맞는 효과적인 정보보호를 위하여 기본적으로 무엇이 수행되어야 하는가를 일목요연하게 기술한 지침과 규약으로서 정보자산을 어떻게 관리하고 보호할 것인가에 대하여 문서로 기술해 놓은것

관리적 ISMS-P 인증
물리적 CCTV, 자물쇠, 잠금, 출입통제(가장 적은 비용으로 확실한 효과)
기술적


정보보안기사

문] 다음의 지문은 무엇에 관한 설명인가?

이는 조직의 정보보호에 대한 방향과 전략 그리고 정보보호체계의 근거를 제시하는 매우 중요한 문서로 최고 경영자 등 경영진의 정보보호에 대한 의지 및 방향, 조직의 정보보호 목적, 조직의 정보보호 범위, 조직의 정보보호 책임과 더불어 조직이 수행하는 관리적, 기술적, 물리적 정보보호 활동의 근거가 된다.

가. 정보보호 정책
나. 정보보호 프로그램
다. 정보보호 절차
라. 정보보호 전략

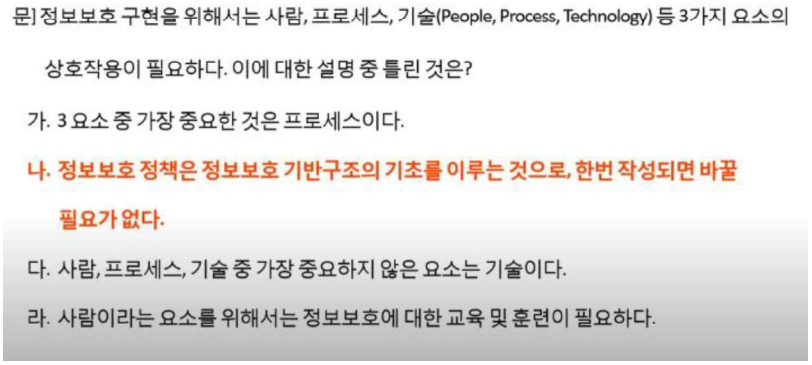
정보보호 정책

정보보호 정책이란 어떤 조직이 기술과 정보자산에 접근하려는 사람이 따라야 하는 규칙의 형식적인 진술(문서)
정보보호의정책의 목표를 결정하지 않고서는 보안에 관하여 적절한 결정을 할 수 없다.
정보보호관리자는 시스템의 안정성과 사용의 용이성을 동시에 고려하여 우선과제를 선정해야 한다.
정보보호 정책의 내용에는 필요한 보호의 수준에 따른 자산의 분류를 포함하여야 한다.
정보보호 정책은 정보보호 기반구조의 기초를 이루는 것으로 주기적으로 검토되고 변경되어야 한다.

정보보호 구현

정보보호 구현을 위해서는 사람, 프로세스, 기술(People, Process, Technology) 등 3가지 요소의 상호작용이 필요하다.

3요소 중 가장 중요한 것은 프로세스이다.
사람, 프로세스, 기술 중 가장 중요하지 않은 요소는 기술이다.
사람이라는 요소를 위해서는 정보보호에 대한 교육 및 훈련이 필요


문] 정보보호 구현을 위해서는 사람, 프로세스, 기술(People, Process, Technology) 등 3가지 요소의 상호작용이 필요하다. 이에 대한 설명 중 틀린 것은?

가. 3 요소 중 가장 중요한 것은 프로세스이다.
나. 정보보호 정책은 정보보호 기반구조의 기초를 이루는 것으로, 한번 작성되면 바꿀 필요가 없다.
다. 사람, 프로세스, 기술 중 가장 중요하지 않은 요소는 기술이다.
라. 사람이라는 요소를 위해서는 정보보호에 대한 교육 및 훈련이 필요하다.

정보보호의 보안 서비스

가용성 : 정보시스템은 적절한 방법으로 주어진 사용자에게 정보 서비스를 제공해야 한다.

기밀성(Confidentiality) : 허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것, 원치 않는 정보의 공개를 막는다는 의미에서 프라이버시 보호와 밀접한 관계가 있음

무결성(Integrity) : 허락되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는것, 다시 말하면 수신자가 정보를 수신했을 때 보관되어 있던 정보를 꺼내 보았을 때 그 정보가 중간에 수정, 첨삭되지 않았음을 확인할 수 있도록 하는 것

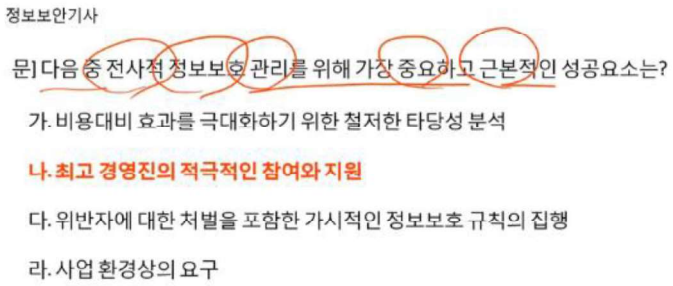
해시 함수를 이용하여 나의 내용이 바꾸지 않게 하는것

부인방지(Non-Repudiation): 부인 봉쇄라고도 하며, 정보를 보낸 사람이 나중에 정보를 보냈다는 것을 부인하지 못하도록 하는 것이다.

송신자의 개인키로 암호화하고 송신자의 공개키로 복호화 되면 그게 부인 방지

정보보호대책

전사적 정보보호 관리를 위해 가장 중요한 근본적인 성공요소는 최고 경영진의 적극적인 참여와 지원이다. (돈, CEO의 결정)



정보보호기술

관리적 보호기술

정보보호정책, 지침, 절차, 가이드라인, 문서처리 순서의 표준화 등의 대책을 수립

법,제도,규정,교육등을 확립하고, 보안계획을 수립하여 이를 운영(보안등급, Access 권한 등) 하고, 위험분석 및 보안감사를 시행하여 정보시스템의 안전성과 신뢰성을 확보하기 위한 대책

조직체의 정보보호를 효과적으로 보장하기 위해서는 다양한 기술적인 보호대책뿐만 아니라 이들을 계획하고 실계하면 관리하기 위한 제도, 정책 및 절차등의 관리적 보호 대책이 중요하다.

기술적 보호기술

안전한 패스워드 사용을 강제하고, 침입차단시스템(방화벽)을 이용하여 접속을 통제하며, 가상사설망(VPN)을 이용하여 안전한 통신환경 구현한다. 그리고 보안 솔루션, 보안 모니터링 및 감사 등의 대책을 수립한다.

정보 시스템, 통신망, 정보(데이터)를 보호하기 위한 가장 기본적인 대책

접근통제, 암호기술, 백업 체제, 정보시스템 자체에 보안성이 강화된 시스템 소프트웨어를 사용하는 등의 대책이 기술적 보호대책에 속한다.

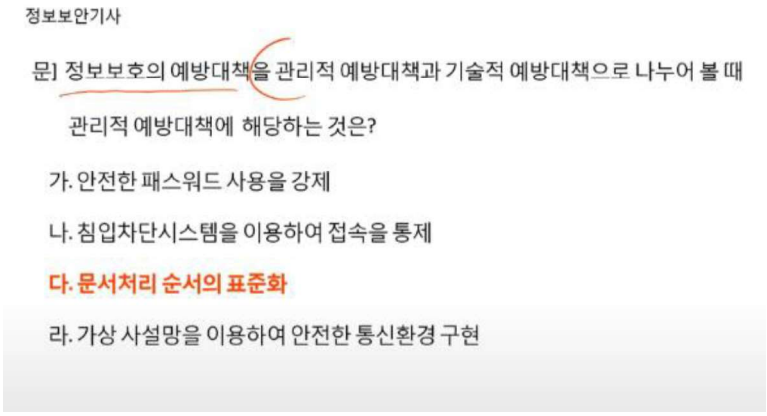
물리적 보호기술

물리적 접근 통제, 제한구역 설정, UPS 및 항온항습 장치 등의 대책을 수립

시건장치 등

화재, 수해, 지진, 태풍 등과 같은 자연재해로부터 정보시스템이 위치한 정보처리시설을 보호하기 위한 자연 재해대책이 있다.

또한 불순 세력이나 적의 파괴로부터 정보시스템을 보호하기 위한 출입통제, 장치 등의 물리적 보안대책으로 구분된다.



(사람, 프로세스, 기술) 보안 분야의 '정치적 올바름' 과 '실제적 올바름'

많은 전문가들은 IT 보안 세계에서 프로세스보다 사람이 중요하다고 말한다

그러나 이는 실제로 올바른 표현이라기보다는 정치적으로 옳은 표현

인식 전문가는 '프로세스' 라고 주장한다. 프로세스가 없다면 사람들은 무엇을 해야 할지 모른다

프로세스-기술-사람 삼각형 구조에서 사람이 최우선이라고 말하는 것은 정치적으로 옳은 표현일 수 있으나 현실적으로는 틀린 표현이다.

관 연 **제28조(개인정보취급자에 대한 감독)** ① 개인정보처리자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자(이하 "개인정보취급자"라 한다)의 범위를 최소한으로 제한하고, 개인정보취급자에 대하여 적절한 관리·감독을 하여야 한다. <개정 2023. 3. 14.>

② 개인정보처리자는 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다.

(개인정보보호위원회) 개인정보의 기술적·관리적 보호조치 기준

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보 보호책임자"란 이용자의 개인정보보호 업무를 총괄하거나 업무처리를 최종 결정하는 임직원을 말한다.
2. "개인정보취급자"란 이용자의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.
3. "내부관리계획"이라 함은 정보통신서비스 제공자등이 개인정보의 안전한 처리를 위하여 개인정보보호 조직의 구성, 개인정보취급자의 교육, 개인정보 보호조치 등을 규정한 계획을 말한다.
4. "개인정보처리시스템"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.
5. "망분리"라 함은 외부 인터넷망을 통한 불법적인 접근과 내부정보 유출을 차단하기 위해 업무망과 외부 인터넷망을 분리하는 망 차단조치를 말한다.
6. "비밀번호"라 함은 이용자 및 개인정보취급자 등이 시스템 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
7. "접속기록"이라 함은 이용자 또는 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
8. "바이오정보"라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
9. "P2P(Peer to Peer)"라 함은 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.
10. "공유설정"이라 함은 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것을 말한다.
11. "보안서버"라 함은 정보통신망에서 송·수신하는 정보를 암호화하여 전송하는 웹서버를 말한다.
12. "인증정보"라 함은 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등이 요구한 식별자의 신원을 검증하는데 사용되는 정보를 말한다.
13. "모바일 기기"란 스마트폰, 태블릿PC 등 무선망을 이용할 수 있는 휴대용 기기를 말한다.
14. "보조저장매체"란 이동형 하드디스크(HDD), USB메모리, CD(Compact Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 쉽게 분리·접속할 수 있는 저장매체를 말한다.

제3조(내부관리계획의 수립·시행) ① 정보통신서비스 제공자등은 다음 각 호의 사항을 정하여 개인정보보호 조직을 구성·운영하여야 한다.

1. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
2. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보 내부관리계획의 수립 및 승인에 관한 사항
4. 개인정보의 기술적·관리적 보호조치 이행 여부의 내부 점검에 관한 사항
5. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
6. 개인정보의 분실·도난·유출·위조·변조·훼손 등이 발생한 경우의 대응절차 및 방법에 관한 사항
7. 그 밖에 개인정보보호를 위해 필요한 사항

② 정보통신서비스 제공자등은 다음 각 호의 사항을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수 등을 고려하여 필요한 교육을 정기적으로 실시하여야 한다.

1. 교육목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

③ 정보통신서비스 제공자등은 제1항 및 제2항에 대한 세부 계획, 제4조부터 제8조까지의 보호조치 이행을 위한 세부적인 추진방안을 포함한 내부관리계획을 수립·시행하여야 한다.