

과정명	
06차시	정보보호 정책

<1> 정보보호 정책의 개념

[1] 정보보호 정책 개념 및 유형

(1) 정보보호 정책의 개념

- 조직 내에서 정보보호 관리 활동의 매우 중요한 요소이며 정보보호 임무를 수행하기 위한 수단으로 정보보호 프로그램을 기획 및 수행하고 목표를 설정하며 책임을 부여하는 등 최고 경영진의 지시나 의지의 표현
- 임직원에게 책임의 할당과 책임 추적성을 제공하고 조직의 정보자산을 보호하기 위한 정보보호 목표를 수립한다. 임직원의 가치 판단이 기준을 제시하면 경영의 목표를 직원들이 공유할 수 있도록 함
- 정보보호 정책을 수립하기 위해서는 구체적인 정보보호 정책이 필요하고 어느 조직이든 정책이 없다면 일상적인 운영 활동을 개인의 판단 기준에 의존하여 수행하게 됨
- 정보보호 정책을 수립하기 위해서는 우선적으로 무엇을 해야 한다는 목적과 방향을 개념적으로 정의해야 하고 정책에서 정의한 내용을 준수하기 위해 필요한 점검 양식이나 전 조직 내에서 동일하게 사용할 필요가 있는 제품과 같은 사항은 표준으로 정의하여 사용해야 한다. 강제적인 준수보다는 권고되거나 효율적인 실행을 위한 사항을 지침이나 절차로 작성하여 배포함
- 정보보호 정책은 조직의 정보보호에 대한 방향과 전략 그리고 정보보호 프로그램의 근거를 제시하는 매우 중요한 문서이므로 정책의 의미, 유형, 수립 과정, 포함될 내용을 이해해야 한다. 또한, 정보보호에 대한 책임과 역할이 명확히 구현되어야 하고 이것이 조직체계로서 구현되어야 하므로 정보보호를 위한 조직의 유형과 역할, 구성 등에 대한 이해가 필요함

(2) 정보보호 정책의 유형

1) 상향식 정책

- 기업 차원의 정책은 차후에 기존의 운영 정책들을 종합하여 수립 정책 간의 불일치와 모순이 발생할 여지가 있음

2) 하향식 정책

- 기업 차원의 정책으로부터 하위 수준의 정책을 도출하는 방식

[2] 정보보호 정책의 요소

(1) 정보보호 정책 개발 전 고려할 지원적 요소

1) 경영진의 참여와 지원

- 성공적인 정보보호 실천을 위해서 정보보호 정책이 최고경영자 및 경영진에 대한 참여를 통하여 제정 승인되며, 직원들이 정보보호가 중요하다는 사실을 인식할 수 있음
- 모든 사람에게 경영진이 정보보호에 대한 확실한 실행 의지와 지원이 약속되었다는 것을 보여줄 수 있다. 즉, 경영진이 승한 정보보호 정책은 명확하고 분명한 방식으로 정보보호가 중요함을 보여줄 수 있고 직원들은 정보보호에 주의를 기울이게 됨
- 모든 조직에서 경영진은 컴퓨터와 네트워크의 운영과 보호에 대한 의도를 명확히 직원들에게 의사소통해야 한다. 따라서 정보 보호 정책을 작성할 때는 조직의 정보보호의 필요성을 논의하는데 최고 경영진이 반드시 참여한다. 경영진은 이러한 대화를 통해 정보보호의 중요성과 필요성에 대하여 인식하게 될 수 있음

2) 관계 법령의 고려

- 정보보호 정책은 조직 내에서 정보보호 실천을 위한 최상위의 규정이지만 조직의 사업 목적과

관계 법령에 종속

- 정보보호는 한 조직만의 문제는 아니며 국가의 안전과 시민의 권리와 관련되어 있으므로 정보로 정책은 제반 법적 요구사항을 만족하여야 할 뿐만 아니라 적극적으로 정보보호에 관련된 법적 요구사항을 달성하도록 명시

3) 상위 정책과의 일관성 유지

- 정보보호 정책의 체계를 수립하는 것은 경영전략, 정보기술전략(ISP)등의 상위 정책과의 일관성을 유지하는 것과 정책, 표준, 지침, 절차 등의 정보보호 관련 문서의 유형을 조직에 맞도록 정형화하는 것을 의미
- 상위 정책과의 일관성을 유지하기 위해서 정보보호 정책을 새롭게 개발하거나 개정하는 경우에는 경영전략, 사업 목표 등의 상위 문서를 개발의 초기단계에서 우선적으로 검토하여 필요한 사항을 적절하게 반영해야 함

4) 정보보호 정책 구성 체계

- 정보보호에 관련된 문서 체계는 상위의 정보보호 정책과 중간의 절차, 표준 지침, 그리고 하위의 정보보호 관리 체계를 운영하면서 발생하는 기록 등으로 분류하여 관리하여야 하며, 하위의 문서는 상위의 문서를 구체화하며 상위 문서에 종속
- 목적, 적용 대상과 범위에 따라 계층화 될 수 있으며, 전체 조직에 적용되는 최상위의 정보보호 정책이 존재하고 이를 달성하기 위해 부서별로 업무에 관련된 정보보호 정책이 존재할 수 있음

(2) 정책, 표준, 지침, 절차의 정의 및 특성

- 정보보호 활동에 대한 목표와 방향을 제시하는 상위의 규정이라면, 구체적으로 정보보호를 위하여 무엇을 어떻게 해야 하는가에 대한 구체적인 사항은 관련된 표준, 지침, 절차로 구성됨

구분	정의 및 특성
정책 (Policy)	<ul style="list-style-type: none">· 정보보호에 대한 상위 수준의 목표 및 방향을 제시· 조직의 경영목표를 반영하고 정보보호 관련 상위 정책과 일관성을 유지· 정보보호를 위해 관련된 모든 사람이 반드시 지켜야 할 요구사항을 전반적이며 개략적으로 규정
표준 (Standard)	<ul style="list-style-type: none">· 정보보호 정책과 마찬가지로 반드시 지켜야 하는 요구사항에 대한 규정이지만, 정책의 만족을 위해 반드시 준수해야 할 구체적인 사항이나 양식을 규정· 조직의 환경 또는 요구사항에 따라 관련된 모든 사용자들이 준수하도록 요구 되는 규정
지침 (Guideline)	<ul style="list-style-type: none">· 반드시 지켜야 하는 것이 아니라 선택 가능하거나 권고적인 내용이며 융통성 있게 적용할 수 있는 사항을 설명· 정보보호 정책에 따라 특정 시스템 또는 특정 분야별로 정보보호 활동에 필요 하거나 도움이 되는 세부 정보를 설명
절차 (Procedure)	<ul style="list-style-type: none">· 정책을 만족하기 위하여 수행하여야 하는 사항을 순서에 따라 단계적으로 설명· 정보보호 활동의 구체적 적용을 위해 필요한 적용 절차 들의 구체적이고 세부 적인 방법을 기술

<2> 정보보호 정책 수립

[1] 정보보호 정책 수립 내용

(1) 정보보호 정책의 정의

- 정보보호 정책은 어떤 조직의 기술과 정보 자산에 접근하려는 사람이 지켜야 하는 규칙의 형식적인 진술임
- 반드시 충족해야 할 특정 요구사항 또는 규칙에 대한 윤곽을 명시하며, 고위 경영진에 의해 생성된 고위급 성명서(High Level Statement)로서 사내의 중요한 정보를 보호 관리 배포하기 위한 방법을 규정함

(2) 정보보호 정책의 필요성

- 정보보호와 관련된 결정은 대부분 정보보호 관리자가 네트워크의 안전 영부, 제공 기능, 편의성에 대해 결정했을 때에 만들어짐
- 정보보호 정책의 목표를 결정하지 않고서는 보안에 관하여 적절한 결정을 할 수 없다. 정보보호 목표를 결정할 때까지는 무엇을 점검하고 무엇을 제한할 것인지를 전혀 알지 못하기 때문에 어떤 보안 도구도 효과적으로 사용할 수 없음
- 현재의 업무 체계와 미래의 업무 체계에 대한 요건을 고려하여, 장기적 관점에서 기업의 비전과 방향을 제시하는 경영 전략의 이해 및 분석을 선행하여야 함

(3) 정보보호 정책 수립을 위한 외부 환경 분석

- 기업이 준수하여야 법규에 대한 충분한 분석을 통하여 이에 합당한 정보보호 정책을 기획해야 함
- 이 분야에 대하여 우수한 상대를 찾아 우수한 성공 사례를 도출하고 성공차이를 확인하여 그 차이를 극복하기 위하여 상대의 뛰어난 경영 방식을 배우면서 자기 혁신을 추구하는 방식의 벤치마킹을 수행
- 참조 자료의 분석 방향은 일반적으로 전략, 업무 프로세스, 조직, 정보 기술 등에 대한 정보 수집 및 사례 분석으로 실시되고, 선정 대상의 우수성과 자사와의 성과 차이에 대한 원인을 분석하고 이를 극복하기 위한 방안을 자사의 혁신 활동에 반영하는 방식으로 진행됨

(4) 선진 사례 벤치마킹 자료의 수집 및 분석

1) 벤치마킹 조사 방식

1. 직접 조사 방식

- 직접 조사 방식은 선진 사례 업체 또는 기관을 방문하여 성공 전략 및 차별화 요소 등을 조사하는 방식
- 정확하고 핵심적인 자료를 획득할 수 있으나 시간 및 비용이 많이 소요

2. 간접 조사 방식

- 벤치마킹을 수행할 대상 업체 및 기관의 수에 제한 없이 다양한 인터넷, 문헌 등 개방된 정보망을 통하여 분석함으로써 폭 넓은 조사가 가능함
- 업체가 입수하고자 하는 핵심적인 자료 확보에 어려움이 있다는 단점이 존재

2) 직접적 벤치마킹 과정

1. 벤치마킹 목적 수립

- 벤치마킹 하고자 하는 대상에 대하여 선진 사례 도출에 대한 목표를 정확히 수립해야 함

2. 벤치마킹 요소 도출

- 벤치마킹의 목적과 도출할 내용에 대하여 정확한 기준을 수립하여야 벤치마킹의 정확한 내용에 대한 벤치마킹 작업 소요 시간을 줄일 수 있음
- 벤치마킹 수행 시 목적을 정확히 수립하여야 벤치마킹 요소에 대한 정확한 도출이 가능

3. 벤치마킹 대상 선정 및 기준 설정

- 벤치마킹 대상에 대한 사전 정확한 도출이 선행되어야 함
- 기준 설정은 목표에 따른 벤치마킹 요소 도출 기반으로 대상을 설정

4. 벤치마킹 분석 및 선정

- 벤치마킹 수행을 수행하기 위한 사전 기준에 기반하여 벤치마킹을 수행해야 함
- 수행 결과는 철저한 분석으로 도출하고자 하는 목표에 합당한 요소를 선정

5. 벤치마킹 적용

- 선정된 벤치마킹에 대하여 그 내용을 실제 적용하는 단계
- 이 시점에 유의할 사항은 벤치마킹 요소가 초기 목표 사항에 합당한 것인지 재검토하여야 하며 적용 시에는 법적 요소 등에 위배 사항이 없는지를 면밀히 검토 후 적용함

3) 정보보호 목표 선정 시 고려사항

1. 서비스 제공

- 사용자에게 제공하는 서비스의 이점이 잠재적 위험보다 크다면 정보보호 관리자는 사용자들이 위험으로부터 서비스를 안전하게 사용할 수 있도록 보호대책을 수립해야 함

2. 용이성

- 누구나 쉽게 시스템에 접근하여 사용할 수 있다면 사용하기에 편리한 반면 각종 위험에 노출될 가능성이 높음
- 관리자는 시스템 사용의 용이성이 다소 떨어지더라도 시스템의 안전을 최우선 과제로 선정

3. 정보보호 비용과 손실 위험

- 정보보호를 하기 위해서는 비용이 많이 소요되므로 각 비용의 형태는 발생 가능한 손실의 형태에 따라서 신중하게 결정
- 정보보호 정책의 영역은 정보기술, 저장된 정보, 기술에 의해 조직된 정보의 모든 형태를 포함 함

(5) 정보보호 정책의 특징

1) 정보보호 정책 유형

1. 전사 정책

- 일반적으로 조직의 최고 관리자가 수립
- 상위 수준의 정책으로 프로그램 목적, 적용범위, 관리 및 책임 등을 부여

2. 프로그램 문제 지향 정책

- 특정한 관심 분야에 초점을 맞추어 개발되는 정책
- 새로운 문제 발생 시 개정이 쉽고 자주 변경 가능

3. 시스템 지향 정책

- 세부사항에 맞추어 특정한 시스템에 대한 보안 정책을 기술

2) 정보보호 정책의 일반 원칙

1. 개인적 측면

- 개인의 프라이버시가 침해되지 말아야 하며, 정보보호의 목적을 달성하기 위하여 IT분석 또는 정보보호 담당자의 편의 중심으로 개발되어서는 안됨

2. 사회적 측면

- 도덕적 판단 기준, 사회적 측면에서 일반적이고 보편타당함

3. 법률적 측면

- 다른 사람의 법적인 권리를 보장할 수 있는 바탕에서 개발되어야 하며, 정보보호 법률 및 규제 들의 요구사항이 반영되어야 함

[2] 정보보호 정책 수립 절차

(1) 요구사항에 대한 개념

1) 요구사항 개념

- 문제의 해결 또는 목적을 달성하기 위하여 사용자에게 의하여 요구되거나, 표준이나 명세 등을 만족하기 위하여 시스템이 가져야 하는 서비스 또는 어떤 제약 사항이 구현되어야 하는지에 대한 명세로, 시스템의 동작 방법과 속성들에 대한 설명이며, 시스템 개발 프로세스상의 제약(Constraint) 사항임

2) 요구사항의 유형 및 특징

구분	내용
기능적 요구	<ul style="list-style-type: none"> - 시스템과 외부 요소 간의 상호 연관성으로서 외부 사용자에게 직접 적으로 혜택을 줄 수 있는 시스템 서비스의 기능 - 사용자 요구 사항 명세서(User Requirement Specification)로부터 요구 사항을 도출 - 기능적 요구 사항 명세서는 완전성과 일관성 확보 필요 - 기능적 요구 항목의 문제들은 구현 기술과는 독립적

비기능적 요구	<ul style="list-style-type: none"> - 시스템의 전체적 품질이나 특성 및 기능적 요구 사항을 구현할 때 고려하여야 하는 제약 사항 - 요구 분석 이후의 설계 단계에서 이루어질 언어나 플랫폼, 구현 선택 등의 기술에 영향을 줌
---------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------

(2) 요구사항 수집 방법

구분	내용	고려 사항
인터뷰	일반적이고 기본적인 요구 사항 도출 방식, 분석가와 고객 간의 인터뷰를 기반으로 요구 사항을 도출	인터뷰 참여율이 저조하거나 인터뷰 내용에 과장, 누락, 애매 모호성 등의 위험 요소 존재 가능
시나리오	고객의 요구 사항에 대하여 Story를 작성함. 일반적으로 USE CASE가 대표적인 사례	고객은 분석가가 제시하는 스토리에 대한 이해도가 있어야 하며 시나리오를 작성하여야 함
프로토타입	구체적이지 못한 요구 사항에 대한 UI 또는 프로토타입 등을 통하여 고객과의 피드백으로 요구 추출	제작 비용 및 기간 소요, 화려한 UI로 핵심 기능 간과될 우려가 있음
회의 진행	이해 관계자들의 모임을 구성하여 브레인스토밍(brainstorming)을 통하여 요구 추출	모임의 주선이 어려울 수 있고 이해 관계자들 간 상충되는 사항에 대한 합의가 없을 때 서로의 주장으로 와해가 될 수 있음
관찰	WBS(Work Breakdown Structure)를 통하여 각 분석가별 분석 대상 업무의 할당, 사용자의 비즈니스 수행, 현행 시스템의 이용을 관찰	장기간 시간 소요 및 분석가의 상주 비용

(3) 정보보호 정책 수립

1) 정책 수립 시 고려사항

- 시스템의 안전을 우선적으로 고려
- 손실 비용에 대하여 신중히 결정
- 조직의 규모, 역할, 정보 시스템 활용 특성을 고려
- 기존의 상위 정책이나 규칙, 법령 등과 부합되도록 함
- 계층 구조를 가지는 경우 상부 조직의 정책을 준수하면서 자신의 환경에 맞도록 세분화
- 정책 개발에서는 수용 가능한 지침과 적절한 방법들을 수립
- 시스템 관리 절차를 통하여 구현 가능해야 함
- 예방이 불가능한 경우에는 인가된 보안 도구 실행이 가능해야 함
- 시스템 관리자, 보안 전문가, 일반 사용자, 감사인, 물리적 보안 요원들과의 협의 절차를 거침
- 주기적인 위험 분석 결과로 나타난 보안 우선순위를 반영해야 함

2) 정보보호 정책 작성 방안

1. 목적

- 중요한 정보자산을 식별하여 선언하고 정보의 어떤 특성이 만족되어야 하는지 선언하는 것

2. 적용 범위

- 정책의 적용 범위를 명시하며, 전 조직을 대상으로 하여 정보 자산에 접근하는 외부인을 포함하는 것이 가장 일반적이고 바람직함

3. 정책 내용

- 관리 체계 범위 내의 전 직원에게 적용되는 것이 원칙이므로 모두가 숙지할 수 있도록 가장 중요한 사항만으로 간단하고 명료하게 만들어야 함

4. 책임

- 정책을 수행하기 위해 기본적으로 정의해야 하며, 경영진의 책임, 정보관리 또는 정보보호 조직의 책임, 일반 직원의 책임 등이 언급됨

5. 문서 승인

- 조직의 최고 책임자가 정책을 승인하고 지원 의지를 알리기 위한 것

[3] 조직 체계와 역할 및 책임

- 적합한 정보보호 정책을 계획, 구현, 승인, 감독할 수 있는 조직 체계를 수립하여야 하며 모든 조직은 독자적인 체계를 가지고 이에 적합한 방식으로 정보보호와 관련된 직무를 할당해야 함

(1) 역할

1) 사고 대응 팀/정보보호 위원회

- 전략적 보안 계획과 관련하여 IT운영위원회에 조언
- IT 보안의 전략적 지원에 관련하여 조직 IT 정보보호 정책을 수립하고 IT운영위원회로부터 승인 획득
- 조직 IT 정보보호 정책을 IT 보안 프로그램으로 전환
- IT보안 프로그램 실행을 모니터링
- 조직 IT 보안 정책의 유효성 검토
- IT보안 문제 인식 촉진
- 계획 프로세스를 지원 및 IT 보안 프로그램 실행을 지원하는 데 필요한 자원(인력, 예산 등)에 입각하여 조언

2) 정보 시스템 관리 책임자

- IT 보안 프로그램 실행을 감독
- 정보보호 관리팀 및 조직 정보보호 임원에 대한 연락 및 보고
- 조직 IT 보안 정책과 지침을 유지
- 사고 조사 조정
- 조직의 전반적인 보안 인식 프로그램 관리
- IT 프로젝트 및 시스템 보안 담당의 권한 결정

3) 프로젝트 보안 담당자/시스템 보안 담당자

- 정보보호 관리팀 및 조직 IT 보안 담당에 대한 연락 및 보고
- IT 프로젝트 및 시스템 보안 정책을 수립, 유지
- 정보보호 계획을 개발, 구현
- IT 프로젝트 및 시스템 보안 대책의 구현 및 사용을 모니터링
- 사고 조사의 착수, 지원

(2) 책임

1) 최고 경영자

- 정보보호를 위한 총괄 책임

2) 정보보호 관리자

- 조직의 정보보호 정책, 표준, 대책, 실무 절차를 설계, 구현, 관리, 조사할 책임

3) 데이터 관리자

- 정보시스템에 저장된 데이터의 정확성과 무결성을 유지하고 데이터의 중요성 및 분류를 결정할 책임

4) 프로세스 관리자

- 해당 정보시스템에 대한 조직의 정보보호 정책에 따라 적절한 보안을 보증할 책임

5) 기술지원 인력

- 보안 대책의 구현에 대하여 조언할 책임

6) 사용자

- 조직의 정보보호 정책에 따라 수립된 절차를 준수할 책임

7) 정보 시스템 감사자

- 보안 목적이 절절하고 정보보호 정책, 표준, 대책, 실무 및 절차가 조직의 보안 목적에 따라 적절하게 이루어지고 있음을 독립적인 입장에서 관리자에게 보증할 책임

<3> 예산 수립 및 정당화 방법

[1] 정보 자산

- 조직의 정보자산으로 보호할 가치가 있는 정보 자산을 식별하고 이를 정보 자산의 형태, 소유자, 관리자, 특성 등을 포함한 목록으로 만들어야 함

(1) 정보자산의 식별

- 조직의 자산을 파악하고, 자산의 가치 및 중요도를 산출하며, 정보 자산과 업무처리와의 관계도 알아낼 수 있음
- 위험 분석을 위한 자산 목록에는 자산 유형, 자산 또는 자산 그룹을 식별하기 위한 식별 번호, 자산명, 자산의 설명, 소유자, 관리자, 기밀성 요구사항, 무결성 요구사항, 가용성 요구사항이 명시되어야 하며, 이 외에도 분석이나 진단 시 활용하기 위한 추가 정보가 포함될 수 있음
- 문서, 시설, 지원 서비스, 인력, 매체의 경우, 조직의 업무상 이들이 중요하지 않거나 보안상의 큰 영향을 미치지 않는 경우, 분석에 필요한 인력과 시간이 부족한 경우, 위험 분석을 IT 시스템 중심으로 수행하는 경우에는 세부 목록을 작성하지 않을 수 있음

(2) 자산 가치 선정

- 자산의 중요도를 파악하고, 위험이 발생할 경우 있을 수 있는 피해량 측정에 필요한 정보를 얻기 위해 위험분석 대상 자산의 가치를 정량 또는 정상적인 방법으로 평가하는 과정

1) 정량적 기준

- 자산 도입 비용
- 자산 복구 비용
- 자산 교체 비용

2) 정성적 기준

- 업무 처리에 대한 자산의 기여도
- 자산이 영향을 미치는 조직과 작업의 수
- 시간
- 조직의 특성에 맞는 기타 요소

(3) 자산 평가

- 위험 분석 결과의 정확도를 결정하는 중요한 과정

1) 자산 조사

- 조사할 자산의 범위를 설정하고 자산 목록을 작성

2) 자산 가치 산정

- 자산을 정량적 또는 정성적으로 산출하는 기준과 절차를 정의

3) 자산 가치 평가 기준

- 식별된 자산에 대한 침해 사고가 발생한 경우에는 기밀성, 무결성, 가용성으로 평가할 수 있으며, 비즈니스와 서비스에 영향을 주는 정도를 고려하면 장애 복구를 위한 목표 시간, 침해 사고 발생 시 피해 규모, 위험 발생 가능성으로 평가할 수 있음

[2] 사후관리, 모니터링, 내부감사, 변경관리

(1) 정보보호 관리체계의 재검토

- 정보보호 관리체계의 효율성, 범위의 적절성, 잔류 위험의 수준이나 절차 등의 문서를 조직의 목표, 기술 등 내외부의 변화와 내부 감사 결과, 보안사고 등을 고려하여, 공식적이고 정기적으로 재검토해야 함
- 적절한 단계에서 다음 목적을 위하여 정책의 계획 및 구현에 대한 체계적인 검토를 수행하고

검토에 참여하는 인원은 검토가 진행되고 있는 대상의 계획 및 구현 단계에 관련된 인원이 포함되어야 하며, 검토 및 검토로 야기된 조치의 결과를 기록함

(2) 정보보호 관리체계의 모니터링 및 측정

- 개선사항을 식별하고 적절한 수정이나 예방 조치를 통해 효과적으로 개선사항을 구현해야 함
- 정보보호 관리체계의 성과 측정방법으로 정보보호 정책이 조직의 요구사항을 충족시키는지 여부에 대해 모니터링하여야 하며, 정보의 획득 및 활용에 대한 방법을 결정해야 함

(3) 내부 감사

- 정보보호 관리체계가 계획된 절차에 따라 효과적으로 실행되는지를 점검하기 위하여 감사의 기준, 범위, 주기 및 방법을 규정하고 계획된 주기로 내부감사는 수행해야 함
- 감사의 기획 및 수행, 결과보고, 기록 유지 및 이행 모니터링에 대한 책임과 요구사항을 문서화된 절차에 의해 규정하고 감사 분야의 관리자는 발견된 부적합 사항 및 그들의 원인을 제거하기 위한 조치가 취해졌으며, 취해진 조치가 검증되고 검증 결과가 보고됨을 보장해야 함

(4) 변경 관리

- 정기적으로 정보보호 정책 및 정책 시행 문서의 타당성을 검토
- 중대한 보안 사고 발생, 새로운 위협 또는 취약성의 발견, 정보보호 환경에 중대한 변화 등이 정보보호 정책에 미치는 영향을 분석하여 필요한 경우 제·개정하여야 한다. 즉, 정보시스템에 관련된 변경은 지속적으로 관리
- 변경 관리를 위해서는 장비, 소프트웨어, 절차 등에 대한 모든 변경사항을 반영할 수 있는 공식적인 관리책임 및 절차를 수립