제3장 정보보호 정책

정보보호 정책의 필요성

- 정보보호의 목적과 목표를 명확히 함
- 조직에서 필요한 적절한 수준의 정보보호를 규정하고 직원들에게 알려야 함
- 정보보호의 장기적인 방향 설정
- 정보보호에 대한 최고경영자의 추진의지 및 지원에 대한 공약
- 정보보호에 관련된 최상위 문서이며 장기적으로 유지할 내용 포함

정보보호 정책의 효과

- 효율성 제고
  - 비효율적인 의사결정과 불필요한 시행착오를 줄임
- 경영층의 지원 확인
  - 경영층과 정보보호 추진 부서와의 의사소통 경로가 확보되며 정보보호 사업에 대한 가시성 구축
- 마찰 최소화
  - 정보보호 관련 내부 정책들과의 마찰을 줄임으로써 타그룹과의 연대 강화
- 책임회피 방지
  - 정보보호 의무를 위반하거나 소홀히 하는 것을 사전에 방지
- 규정 준수 효과
  - 감사나 징계의 참고자료

정보보호 정책의 내용

- 정보보호의 정의, 목표, 범위 및 중요성
- 경영층 의지의 표명
- 설명 자료
- 정보보호 관리에 대한 일반적인 또는 구체적인 책임들에 대한 정의
- 참고 문헌 목록

정보보호의 정의, 목표, 범위 및 중요성

- 정의
  - 조직이 지향하는 정보보호의 방향에 대해 포괄적으로 언급
- 목표
  - 대규모 데이터 처리->입력에러나 데이터 오류 방지 강조
  - 민감한 개인정보 처리->불법침입 방지 강조
- 범위
  - 정보보호의 대상이 되는 시설, HW, SW, 정보, 인력 등을 명시
  - 내부망을 사용하는 외부조직이나 연결된 조직을 대상으로 할지 여부 결정

경영층 의지의 표명

- 조직의 여러 부서가 정보보호를 적절히 추진하기 위해서는 정보보호의 목표와 원칙을 지원하기 위한 경영층의 의지의 표명이 필수적
- 문서, 비디오 등을 통해 전 직원들에게 전달되어야

설명 자료

- 정보보호의 필요성을 직원들에게 알리는 설득력 있는 설명이 필요
- 정책이 명확하고 간략하고 통일성과 일관성이 있어야 함
- 정보보호 정책, 원칙, 표준 및 각종 규정들에 대한 설명자료 예시
  - 법적 준수 사항이나 계약에 따른 준수 사항
  - 정보보호 교육의 필요사항
  - 바이러스나 다른 악의적인 소프트웨어의 예방 및 탐지
  - 업무지속성관리
  - 정보보호 정책 위반 사항이 미치는 영향
- 정보보호를 위해 어떤 대응수단을 사용할지를 결정하는 근거를 제공

정보보호 관리에 대한 일반적인 또는 구체적인 책임들에 대한 정의

- 정보보호에 관련된 책임 부여에 대한 기본적인 방향 제시
- 예시
  - 직원, 물리적 자산, 정보 자산의 보호에 대한 기본적인 책임은 관리자에게 있다
  - 관리자들은 자신의 통제 영역 안의 정보자산을 식별하고 보호할 책임이 있다
  - 관리자들은 자신들의 감독 하에 있는 특정인들에게 정보자산의 소유와 책임을 할당할 수 있다
  - 관리자들은 정보자산을 보호할 책임을 모든 직원들이 이해하는가를 확인해야 한다
  - 관리자들은 조직의 관리기준과 정보자산의 가치를 고려하여, 정보보호에 관한 시행세칙과 절차를 만들 의무가 있다

참고 문헌 목록

- 정보보호 정책을 지원할 수 있는 정보보호 절차나 규칙 등에 관한 참고문헌의 목록 제공
- 경영층의 승인을 얻어 모든 사람들이 읽기에 적절하고 이해할 수 있는 형태로 문서화되어 조직 안의 모든 사용자들에게 전달
- 표준 (standards)
  - 시스템의 보안을 위해 사용할 기술이나 방법을 구체적으로 명시한 것
  - ID 신분증의 표준: 구체적인 기술과 파라메터의 설정 등
- 지침 (guidelines)
  - 사용자들이나 관리자들이 자신의 시스템을 적절히 보호하는 것을 도와주기 위한 것
  - 시스템 자체 또는 외부 환경이 변화함에 따라 표준의 마련이 어려운 경우에 사용자들에게 정보보호에 대한 중요한 내용을 전달함
- 절차 (procedures)
  - 특정한 정보보호 임무를 달성하기 위하여 밟아 나가야 하는 세부단계를 담고 있음
  - 신규 사용자 계정을 여는 세부 절차와 같이 정보보호 정책, 표준 및 지침 등을 따르기 위한 상세한 업무 수행 절차

정보보호 정책의 재검토와 평가

- 누가?
  - 정보보호 정책 문서에 대한 정해진 재검토 과정에 따라 이를 유지하고 재검토하는 책임자가 있어야 함
    - 내부감사기능
    - 독립적인 관리자
    - 전문성을 가지고 적절한 기술과 경험을 가진 제3의 기관
- 언제?
  - 기존에 수행된 위험평가의 기존적 사항에 영향을 미칠만한 상황의 변화가 있을 때
    - 심각한 정보보호사고 발생
    - 조직구조나 기술의 기반구조에 새로운 취약점이나 변동사항이 있는 경우
- 무엇을 더?
  - 과거에 일어난 정보보호 사건들의 성격, 횟수 및 이들이 끼친 영향으로부터 평가된 정보보호 정책의 효과성
  - 정보보호 통제의 비용과 이러한 통제가 조직 본연의 사업 효율성에 미치는 영향
  - 기술의 변화가 가져오는 영향

정책에 대한 교육 및 홍보

- 직원들 대상의 교육 및 홍보를 통해 정보보호인식 제고
- 부서간 협조를 통한 적극적인 정보보호 활동