[별표 2] **침해사고 예방조치 시 고려사항(제24조 관련)**

가. 관리 · 운영 측면의 고려사항

구 분	주요 고려 사항
관리·운영절차	o 관리 · 운영절차의 수립 시 고려사항 - 시스템 문제발생시 재동작 및 복구 절차 - 시스템 모니터링 방안 - 중요 산출물에 대한 관리 방안 - 업무수행 시 발생될 예외사항 및 오류사항 처리 방안 - 정보처리 및 취급 절차
제한구역 설정 및 보호	o 제한구역 설정 시 고려 사항 - 보호대상 설정 - 특히 중요한 시설이나 장비는 제한구역으로 설정 - 출입 통제 방안 - 반출·입 물품에 대한 기록 유지 - 정전대비 별도의 전원 공급 시설
장비 · 시설의 도입 및 설치	o 시스템 구입 및 설치 시 일반적 고려 사항 - 현재 시스템의 성능과 가용능력의 한계에 대한 분석 - 시스템의 기능적, 운용적 요구사항 정의 및 시기의 예측 - 기존 시스템과의 적합성 확보 - 정보보호 시스템의 설치시는 보호지침과의 부합성 및 설치 필요성에 대하여 검증 - 정기적인 점검 및 안전성에 대한 재검토 o 정보보호시스템 도입 및 설치 · 운영 시 고려 사항 - 요구사항 파악 및 도입·설치의 목적 - 성능 및 도입·설치의 타당성에 대한 검토 - 관리의 편이성 및 로그관리의 편이성 - 정보보호시스템에 대한 로그 감시 기능
변경관리 절차	o 장비, 소프트웨어, 절차들의 변경사항에 대한 관리 책임 및 절차 수립 시 고려사항 - 주요 변경사항 및 변경대상에 관한 정의·기록 유지 - 변경 실패에 따른 복구나 폐기에 대한 책임 정의 절차 - 변경에 대한 잠정적인 영향 평가 - 요구된 변경사항에 대한 승인절차 - 모든 관련자에게 변경사항에 대한 공지 및 교육

구 분	주요 고려 사항
로그 관리	o 운영자 로그관리방안 수립 시 고려사항 - 시스템 시작, 종료시간, 사용자 인증실패, 접속 시도, 시스템 에러 및 수정 내용 등에 대한 로그 유지 - 로그 기록 방법, 대상, 보존 기간, 백업 등 - 주기적 로그 점검 및 방법 - 접근기록에 대한 정기적 분석 및 불법시도에 대한 조치 방법 - 보안 로그 기록 점검사항에 대한 주기적 보고 o 정보보호시스템의 로그 기록 시 필수 고려사항 - 성공적이거나 거부된 접속 - 정보보호시스템 구성요소로부터의 에러 메시지 - 다중 접근 시도 및 보안이 취약한 서비스 포트로의 접근 - 로그를 저장할 메모리 - 기록이 멈추게 되지 않도록 사전 대책 강구
장애 관리	o 장애관리 시 고려사항 - 장애의 감지 및 복구를 위해 운영상황 감시 기능 설정 - 장애관리 보고 절차 수립 - 전체시스템에 대한 피해 최소화를 위해 장애차단 및 장애복구 기능 설정 - 장애처리 후 로그에 대한 재점검으로 장애의 완전 복구상태 확인
저장매체 관리	o 테이프, 디스켓, 출력보고서 등의 저장매체 관리 시 고려 사항 - 저장매체에 대한 목록관리, 분류, 접근통제, 보관 장소, 보관기간, 보관절차 등 수립 - 저장매체에 대한 복사, 변경, 배포, 폐기 방안 - 저장매체 정보저장, 취급 및 전달 절차 수립 - 저장매체 사용에 대한 허가, 점검 수립 및 기록유지 - 저장매체 저장 내용 삭제·폐기 절차
악의적 소프트웨어 관리	o 컴퓨터바이러스 등 악의적 소프트웨어로부터의 보호를 위한 통제·탐지 조치 시 고려 사항 - 사용자에게 바이러스의 위험성에 대한 인식 필요 - 비인가 및 불법 소프트웨어 사용금지 - 알려진 바이러스 백신프로그램 사용 - 지속적인 바이러스 백신프로그램 업데이트 및 검사 - 검증되지 않은 저장매체는 사용 전에 검사 - 외부 네트워크나 매체로부터 파일 또는 소프트웨어 다운로드 시 대책 마련
백 업	o 시스템, 데이터, DB 등 정보자산에 대한 백업조치 시 고려 사항 - 정보자산에 대한 장애 대비 백업 및 복구 절차 규정 - 데이터 중요도에 따른 백업 대상, 백업 방식, 백업주기, 백업기준 등 설정 - 자연재해로부터 보호받을 수 있는 안전한 장소에 대한 지정 - 주기적으로 백업 받은 데이터에 대한 복구 테스트 실시 - 중요정보에 대하여는 제3의 장소 등 물리적으로 분리된 곳에 백업데이터 보관

나. 기술적 측면에서의 고려사항

구 분	주요 고려 사항
사용자 관리	o 사용자 계정 관리 시 고려 사항 - 시스템 접근에 대한 공식적인 사용자 등록 및 해지 절차 수립 - 주기적으로 인가된 사용자 여부 및 접근권한 점검 - 사용자의 공식적인 로그를 보관 - 동일사용자 계정의 다른 사용자 계정 재발급 방지 - 시스템 관리자가 일반 업무 시 일반 사용자 계정 사용
패스워드 관리	o 패스워드 관리 시 고려사항 - 책임 추적성을 위해 패스워드 할당 - 패스워드의 안전한 보관 - 패스워드의 노출가능성이 있으면 즉시 변경 - 패스워드 설정 시 기피해야 할 요건 . 특정 달, 요일, 머리글자, 주민등록번호, 자동차번호 . 회사이름, 전화번호 또는 비슷한 숫자 그룹 . 2개 이상의 연관된 신원확인 가능 문자, 숫자, 영문 알파벳 그룹 - 주기적으로 패스워드를 변경, 지난 패스워드 사용금지 - 특별권한이 부여된 ID의 패스워드는 정기적으로 점검 - 첫 로그온 시 임시 패스워드는 변경 - 비밀번호 오류 횟수의 제한
네트워크 접근 통제	o 네트워크 접근 통제 시 고려 사항 - 네트워크로 접근하는 사용자에 대한 인가 절차 - 원격접속 사용자 인가 절차 - 비인가된 접근을 막기 위해 서비스 경로의 제한 및 분리 - 관계회사 등과 네트워크 공유 시에는 물리적 또는 논리적으로 분리 - 원격 장비의 관리를 위한 책임 및 절차를 수립 - 개발업무 네트워크와 다른 업무용 네트워크와의 분리 운영 - 인증, 암호 활용을 통한 원격 접속 사용자에 대한 접근통제 - 네트워크를 통해 시스템 운영 시 시스템 관리는 원칙적으로 내부 특정 단말로 제한