[별표 2] 물리적 보호조치

구 분			세 부 조 치 사 항
8. 물리적 보안	8.1. 물리적 보호구역	8.1.1. 물리적 보호구역 지정	중요 정보 및 정보처리시설을 보호하기 위한 물리적 보안 구역(예 : 주요 정보처리 설비 및 시스템 구역, 사무실, 외부인 접견실 등)을 지정하고, 각 보안 구역에 대한 보안 대책을 마련하여야 한다.
		8.1.2. 물리적 출입통제	물리적 보안 구역에 인가된 자만이 접근할 수 있도록 출입을 통제하는 시설(예 : 경비원, 출입 통제 시스템 등)을 갖추어야 하고, 출입 및 접근 이력을 주기적으로 검토하여야 한다.
		8.1.3. 물리적 보호구역 내 작업	유지보수 등 주요 정보처리 설비 및 시스템이 위치한 보호구역 내에서의 작업 절차를 수립하고 작업에 대한 기록을 주기적으로 검토하여야 한다.
		8.1.4. 사무실 및 설비 공간 보호	사무실 및 설비 공간에 대한 물리적인 보호방안을 수립하고 적용하여야 한다.
		8.1.5. 공공장소 및 운송·하역구역 보호	공공장소 및 운송.하역을 위한 구역은 내부 정보처리시설로부터 분리 및 통제하여야 한다.
		8.1.6. 모바일 기기 반출·입	노트북 등 모바일 기기 미승인 반출입을 통한 중요정보 유출, 내부망 악성코드 감염 등의 보안사고 예방을 위하여 보호구역 내 임직원 및 외부인력 모바일 기기 반출입 통제절차를 수립하고 기록·관리하여야 한다
	8.2. 정보처리시설 및 장비보호	8.2.1. 정보처리시설의 배치	물리적 및 환경적 위험으로부터 잠재적 손상을 최소화하고 비인가 된 접근 가능성을 최소화하기 위하여, 정보처리시설 내 장비의 위치를 파악하고 배치하여야 한다.
		8.2.2. 보호설비	각 보안 구역의 중요도 및 특성에 따라 화재, 누수, 전력 이상 등 자연재해나 인재에 대비하여 화재 감지기, 소화 설비,

			누수 감지기, 항온 항습기, 무정전 전원 장치(UPS), 이중 전원선 등의 설비를 갖추어야 한다.
		8.2.3. 케이블 보호	데이터를 송수신하는 통신케이블이나 전력을 공급하는 전력 케이블은 손상이나 도청으로부터 보호하여야 한다.
		8.2.4. 시설 및 장비 유지보수	정보처리시설은 가용성과 무결성을 지속적으로 보장할 수 있도록 유지보수 하여야 한다.
		8.2.5. 장비 반출·입	장비의 미승인 반출·입을 통한 중요 정보 유출, 악성코드 감염 등의 침해사고 예방을 위하여, 보안 구역 내 직원 및 외부 업무 관련자에 의한 장비 반출·입 절차를 수립하고, 기록 및 관리하여야 한다.
		8.2.6. 장비 폐기 및 재사용	정보처리시설 내의 저장 매체를 포함하여 모든 장비를 파악하고, 민감한 데이터가 저장된 장비를 폐기하는 경우 복구 불가능하도록 하여야 한다. 또한 재사용하는 경우에도 복구 불가능 상태에서 재사용하여야 한다.