[별표 3] 기술적 보호조치

구 분			세 부 조 치 사 항
9 가상화 보안	9.1. 가상화 인프라	9.1.1. 가상자원 관리	가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립하여야 한다.
		9.1.2. 가상자원 회수	이용자와의 계약 종료 시 가상자원 회수 절차에 따라 백업을 포함한 모든 클라우드 시스템에서 삭제하여야 한다.
		9.1.3. 가상자원 모니터링	가상자원에 대한 무결성 보장하기 위한 보호조치 및 가상자원의 변경(수정, 이동, 삭제, 복사)에 대해 모니터링 하여야 한다. 또한,가상자원에 손상이 발생한 경우 이를 이용자에게 알려주어야 한다.
		9.1.4. 하이퍼바이저 보안	가상자원을 관리하는 하이퍼바이저의 기능 및 인터페이스에 대한 접근 통제 방안을 마련하여야 한다. 또한 하이퍼바이저에 대한 소프트웨어 업데이트 및 보안패치를 최신으로 유지하여야 한다.
		9.1.5. 공개서버 보안	가상자원을 제공하기 위한 웹사이트와 가상소프트웨어(앱, 응용프로그램)를 배포하기 위한 공개서버에 대한 물리적, 기술적 보호대책을 수립하여야 한다.
		9.1.6. 상호 운용성 및 이식성	클라우드컴퓨팅서비스 제공자는 표준화된 가상화 포멧, 이식성이 높은 가상화 플랫폼, 공개 API 등을 이용하여 클라우드컴퓨팅서비스 간의 상호 운용성 및 이식성을 높여야 한다.
	9.2. 가상 환경	9.2.1. 악성코드 통제	바이러스, 웜, 트로이목마 등의 악성코드로부터 이용자의 가상 환경(가상PC, 가상 서버, 가상 소프트웨어 등)을 보호하기 위한 악성코드탐지, 차단 등의 보안기술을 지원하여야 한다. 또한 이상 징후 발견시 이용자 통지하고 사용 중지 및 격리 조치를 수행하여야 한다.
		9.2.2. 인터페이스 및 API 보안	가상 환경(가상PC, 가상 서버, 가상 소프트웨어 등) 접근을 위한 인터페이스 및 API에 대한 보안 취약점을 주기적으로 분석하고, 이에 대한 보호방안을 마련하여야 한다.

		9.2.3. 데이터 이전	이용자가 기존 정보시스템 환경에서 클라우드컴퓨팅서비스의 가상 환경으로 전환 시 안전하게 데이터를 이전하도록 암호화 등의 기술적인 조치방안을 제공하여야 한다.
		9.2.4. 가상 소프트웨어 보안	클라우드컴퓨팅서비스 제공자는 출처, 유통경로 및 제작자가 명확한 소프트웨어로 구성된 가상환경을 제공하여야 한다.
10. 접근통제	10.1. 접근통제 정책	10.1.1. 접근통제 정책 수립	비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다.
		10.1.2. 접근기록 관리	접근기록 대상을 정의하고 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 형태로 기록되고 유지하여야 한다.
	10.2. 접근 권한 관리	10.2.2. 사용자 등록 및 권한 부여	클라우드 시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다.
		10.2.3. 관리자 및 특수 권한 관리	클라우드 시스템 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.
		10.2.4. 접근권한 검토	클라우드 시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 점검하여야 한다.
	10.3. 사용자 식별 및 인증	10.3.1. 사용자 식별	클라우드 시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다. 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.
		10.3.2. 사용자 인증	클라우드 시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하여야 한다.
		10.3.3.	이용자가 클라우드컴퓨팅서비스에 대해 다중 요소 인증 등 강화된 인증 수단을 요청하는 경우 이를 제공하기 위한 방

		강화된 인증 수단 제공	안을 마련하여야 한다.
		10.3.4. 사용자 패스워드 관리	법적 요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경주기 등 사용자 패스워드 관리절차를 수립·이행하고 패스워드 관리 책임이 사용자에게 있음을 주지시켜야 한다. 특히 관리자 패스워드는 별도 보호대책을 수립하여 관리하여야 한다.
		10.3.5. 이용자 패스워드 관리	고객, 회원 등 외부 이용자가 접근하는 클라우드 시스템 또는 웹서비스의 안전한 이용을 위하여 계정 및 패스워드 등의 관리절차를 마련하고 관련 내용을 공지하여야 한다.
11. 네트워크 보안	11.1. 네트워크 보안	11.1.1. 네트워크 보안 정책 수립	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크에 대해 보안 정책과 절차를 수립하여야 한다.
		11.1.2. 네트워크 모니터링 및 통제	DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요 정보 유출 등을 막기 위해 네트워크를 모니터링하고 통제하여야 한다.
		11.1.3. 네트워크 정보보호시스템 운영	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보호시스템(방화벽, IPS, IDS, VPN 등)을 운영하여야 한다.
		11.1.4. 네트워크 암호화	클라우드 시스템에서 중요 정보가 이동하는 구간에 대해서는 암호화된 통신채널을 사용하여야 한다.
		11.1.5. 네트워크 분리	클라우드컴퓨팅서비스 제공자의 관리 영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리하여야 한다.
		11.1.6. 무선 접근 통제	클라우드 시스템은 무선망과 분리하고, 무선접속에 대한 접근을 통제하여야 한다. 무선접속을 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다

12. 데이터 보호 및 암호화	12.1. 데이터 보호	12.1.1. 데이터 분류	데이터 유형, 법적 요구사항, 민감도 및 중요도에 따라 데이터를 분류하고 관리하여야 한다.
		12.1.2. 데이터 소유권	이용자와 서비스 수준 협약 단계에서 데이터의 소유권을 명확하게 확립하여야 한다.
		12.1.3. 데이터 무결성	입·출력, 전송 또는 데이터 교환 및 저장소의 데이터에 대해 항상 데이터 무결성을 확인하여야 한다.
		12.1.4. 데이터 보호	데이터에 대한 접근제어, 위·변조 방지 등 데이터 처리에 대한 보호 기능을 이용자에게 제공하여야 한다.
		12.1.5. 데이터 추적성	이용자에게 데이터를 추적하기 위한 방안을 제공하고, 이용자가요구하는 경우 구체적인 제공정보(이용자의 정보가 저장되는 국가의 명칭 등)를 공개하여야 한다.
		12.1.6. 데이터 폐기	클라우드컴퓨팅서비스 종료, 이전 등에 따른 데이터 폐기 조치 시 이용자와 관련된 모든 데이터를 폐기하여야 하며, 폐기된 데이터를 복구할 수 없도록 삭제 방안을 마련하여야 한다.
	12.2 매체 보안	12.2.1. 저장매체 관리	중요정보를 담고 있는 하드디스크, 스토리지 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제하여야 한다.
		12.2.2. 이동매체 관리	중요정보 유출을 예방하기 위해 외장하드, USB, CD 등 이동매체 취급, 보관, 폐기, 재사용에 대한 절차를 수립하여야 한다. 또한 매체를 통한 악성코드 감염 방지 대책을 마련하여야 한다.
	12.3. 암호화	12.3.1. 암호 정책 수립	클라우드컴퓨팅서비스에 저장 또는 전송 중인 데이터를 보호하기 위해 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 마련하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.

		12.3.2. 암호키 관리	암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고, 암호키는 별도의 안전한 장소에 보관하여야 한다.
13. 시스템 개발 및 도입 보안	13.1. 시스템 분석 및 설계	13.1.1. 보안요구사항정의	신규 시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안취약점, 정보보호 기본요소(기밀성, 무결성, 가용성) 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용하여야 한다.
		13.1.2. 인증 및 암호화 기능	클라우드 시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입·출력 및 송수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다.
		13.1.3. 보안로그 기능	클라우드 시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 하여야 한다.
		13.1.4. 접근권한 기능	클라우드 시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다.
		13.1.5. 시각 동기화	로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 클라우드 시스템 시각을 공식 표준시각으로 정확하게 동기화 하여야 한다. 또한 서비스 이용자에게 시각 정보 동기화 기능을 제공하여 한다.
	13.2. 구현 및 시험	13.2.1. 구현 및 시험	안전한 코딩방법에 따라 클라우드 시스템을 구현 하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다
		13.2.2. 개발과 운영환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다. 단 분리하여 운영하기 어려운 경우그 사유와 타당성을 검토하고 안전성 확보 방안을 마련하여야 한다.
		13.2.3. 시험 데이터 보안	시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다.
		13.2.4. 소스프로그램	소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하

		보안	여 이행하여야 한다. 또한 소스 프로그램은 운영환경에 보관하지 않는 것을 원칙으로 한다.
	13.3. 외주 개발 보안	13.3.1. 외주 개발 보안	클라우드 시스템 개발을 외주 위탁하는 경우 분석 및 설계 단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독하여야 한다.
	13.4. 시스템 도입 보안	13.4.1. 시스템 도입 계획	클라우드 시스템의 처리 속도와 용량에 대하여 주기적인 모니터링을 수행하고 안정성의 확보에 필요한 시스템 도입 계획을 수립하여야 한다.
		13.4.2. 시스템 인수	새로 도입되는 시스템에 대한 인수 기준이 수립되어야 하며, 인수 전에 테스트가 수행되어야 한다.