[별표 1] 관리적 보호조치

구 분			세 부 조 치 사 항
1. 정보보호 정책 및 조직	1.1. 정보보호 정책	1.1.1. 정보보호 정책 수립	정보보호 정책을 문서화하고, 정보보호 최고책임자의 승인 후 정책에 영향을 받는 모든 임직원 및 외부 업무 관련자에게 제공하여야 한다.
		1.1.2. 정보보호 정책 검토 및 변경	정보보호 정책의 타당성 및 효과를 연 1회 이상 검토하고, 관련 법규 변경 및 내·외부 보안사고 발생 등의 중대한 사유가 발생할 경우에는 추가로 검토하고 변경하여야 한다.
		1.1.3. 정보보호 정책문서 관리	정보보호 정책 및 정책 시행문서의 이력관리 절차를 수립하고 시행하며, 최신본으로 유지하여야 한다.
	1.2. 정보보호 조직	1.2.1. 조직 구성	정보보호 활동을 계획, 실행, 검토하는 정보보호 전담조직을 구성하고 정보보호 최고책임자를 임명하여야 한다.
		1.2.2. 역할 및 책임 부여	정보자산과 보안에 관련된 모든 임직원 및 외부 업무 관련자의 정보보호 역할과 책임을 명확하게 정의하여야 한다. 또한 서비스 이용자의 정보보호 역할과 책임도 서비스 수준 협약 등을 통해 명확하게 정의하여야 한다.
2. 인적보안	2.1. 내부인력 보안	2.1.1. 고용계약	고용 계약서에 정보보호 정책 및 관련 법률을 준수하도록 하는 조항 또는 조건을 포함시키고, 새로 채용하거나 합류한 근무 인력이 클라우드컴퓨팅서비스의 설비, 자원, 자산에 접근이 허용되기 이전에 서명을 받아야 한다.
		2.1.2. 주요 직무자 지정 및 감독	클라우드컴퓨팅서비스의 시스템 운영 및 개발, 정보보호 등에 관련된 임직원의 경우 주요 직무자로 지정하여 관리하고, 직무 지정 범위는 최소화하여야 한다.
		2.1.3. 직무 분리	권한 오남용 등 내부 임직원의 고의적인 행위로 발생할 수 있는 잠재적인 위협을 줄이기 위하여 직무 분리 기준을 수립하고 적용하여야 한다.
		2.1.4. 비밀유지 서약서	정보보호와 개인정보보호 등을 위해 필요한 사항을 비밀유지서약서에 정의하고 주기적으로 갱신하여야 한다.

		2.1.5. 상벌규정	정보보호 정책을 위반한 임직원에 대한 징계 규정을 수립하고, 위반 사항이 발생 시 규정에 명시된 대로 징계 조치를 취하여야 한다. 또한 정보보호 정책을 충실히 이행한 임직원에 대한 보상 방안도 마련하여야 한다.
		2.1.6. 퇴직 및 직무변경	임직원의 퇴직 또는 직무 변경에 관한 책임을 명시적으로 정의하고 수행하여야 한다. 또한 이에 대한 접근권한도 제거하여야 한다.
	2.2. 외부인력 보안	2.2.1. 외부인력 계약	외부인력(외부유지보수직원, 외부용역자 포함)에 의한 정보자산 접근 등과 관련된 보안요구사항을 계약에 반영하여야 한다.
		2.2.2. 외부인력 보안 이행 관리	계약서에 명시한 보안요구사항 준수 여부를 주기적으로 점검하고 위반사항이나 침해사고 발생 시 적절한 조치를 수행하여야 한다.
		2.2.3. 계약 만료 시 보안	외부인력과의 계약 만료 시 자산 반납, 접근권한의 회수, 중요정보 파기, 업무 수행 시 알게 된 정보의 대한 비밀 유지서약 등을 확인하여야 한다.
	2.3. 정보보호 교육	2.3.1 교육 프로그램 수립	모든 임직원 및 외부 업무 관련자를 포함하여 연간 정보보호 교육 프로그램을 수립하여야 한다.
		2.3.2. 교육 시행	모든 임직원 및 외부 업무 관련자를 대상으로 연 1회 이상 정보보호 교육을 시행하고 정보보호 정책 및 절차의 중대한 변경, 내·외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생하면 추가 교육을 실시하여야 한다.
		2.3.3. 평가 및 개선	정보보호 교육 시행에 대한 기록을 남기고 결과를 평가하여 개선하여야 한다.
3. 자산관리	3.1. 자산 식별 및 분류	3.1.1. 자산 식별	클라우드컴퓨팅서비스에 사용된 정보자산(정보시스템, 정보보호시스템, 정보 등)에 대한 자산분류기준 수립하고 식별된 자산의 목록을 작성하여 관리하여야 한다.
		3.1.2. 자산별 책임할당	식별된 자산마다 책임자 및 관리자를 지정하여 책임소재를 명확히 하여야 한다.

		3.1.3. 보안등급 및 취급	기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 자산의 보안 등급을 부여하고, 보안 등급별 취급 절차에 따라 관리하여야 한다.
	3.2. 자산 변경 관리	3.2.1. 변경관리	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경이 필요한 경우 보안 영향 평가를 통해 변경 사항을 관리하여야 한다. 또한 이용자에게 큰 영향을 주는 변경에 대해서는 사전에 공지를 하여야 한다.
		3.2.2. 변경 탐지 및 모니터링	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경을 지속적으로 모니터링하여 허가 받지 않은 변경을 탐지하고 최신의 변경 이력을 유지하여야 한다.
		3.2.3. 변경 후 작업검증	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경 후에는 보안성 및 호환성 등에 대한 작업 검증을 수행하여야 한다.
	3.3. 위험관리	3.3.1. 위험관리 계획 수립	관리적, 기술적, 물리적, 법적 분야 등 정보보호 전 영역에 대한 위험식별 및 평가가 가능하도록 위험관리 방법과 계획을 사전에 수립하여야 한다.
		3.3.2. 취약점 점검	취약점 점검 정책에 따라 주기적으로 기술적 취약점(예 : 유·무선 네트워크, 운영체제 및 인프라, 응용 프로그램 취약점 등)을 점검하고 보완하여야 한다.
		3.3.3.위험분석 및 평가	위험관리 방법 및 계획에 따라 정보보호 전 영역에 대한 위험 식별 및 평가를 연 1회 이상 수행하고 그 결과에 따라 수용 가능한 위험수준을 설정하여 관리하여야 한다.
		3.3.4. 위험처리	법규 및 계약관련 요구사항과 위험수용 수준을 고려하여 위험평가 결과에 따라 통제할 수 있는 방법을 선택하여 처리하여야 한다.
4. 서비스 공급망 관리	4.1. 공급망관리 정책	4.1.1. 공급망 관리 정책 수립	클라우드컴퓨팅서비스에 대한 접근과 서비스 연속성을 저해하는 위험을 식별하고 최소화하기 위해 공급망과 관련한 보안 요구사항을 정의하는 관리 정책을 수립하여야 한다.

		4.1.2. 공급망 계약	클라우드컴퓨팅서비스 범위 및 보안 요구사항을 포함하는 공급망 계약을 체결하고 다자간 협약시 책임을 개별 계약서에 각각 명시해야하며, 해당 서비스에 관련된 모든 이해관계자에게 적용하여야 한다.
	4.2. 공급망 변경관리	4.2.1. 공급망 변경관리	정보보호 정책, 절차 및 통제에 대한 수정 및 개선이 필요하다고 판단될 경우 서비스 공급망 상에 발생할 수 있는 위험에 대한 검토를 통해 안전성을 확보 후 계약서 내용 변경 방안을 제시하여야 한다.
		4.2.2. 공급망 모니터링 및 검토	클라우드컴퓨팅서비스 공급망 상에서 발생하는 기록 및 보고서는 정기적으로 모니터링 및 검토하여야 한다.
5. 침해사고관리	5.1. 침해사고 대응 절차 및 체계	5.1.1. 침해사고 대응 절차 수립	침해사고에 대한 효율적이고 효과적인 대응을 위해 신고절차, 유출 금지 대상, 사고 처리 절차 등을 담은 침해사고 대응절차를 마련하여야 한다. 침해사고 대응절차는 이용자와 제공자의 책임과 절차가 포함되어야 한다.
		5.1.2. 침해사고 대응 체계 구축	침해사고 정보를 수집 · 분석 · 대응할 수 있는 보안관제 시스템 및 조직을 구성 · 운영하고, 침해사고 유형 및 중요도에 따라 보고 및 협력체계를 구축하여야 한다.
		5.1.3. 침해사고 대응 훈련 및 점검	침해사고 대응과 관련된 역할 및 책임이 있는 담당자를 훈련시켜야 하고, 주기적으로 침해사고 대응 능력을 점검하여야 한다.
	5.2. 침해사고 대응	5.2.1. 침해사고 보고	침해사고 발생 시 침해사고 대응절차에 따라 법적 통지 및 신고 의무를 준수하여야 한다. 또한 클라우드컴퓨팅서비스 이용자에게 발생 내용, 원인, 조치 현황 등을 신속하게 알려야 한다.
		5.2.2. 침해사고 처리 및 복구	침해사고 발생 시 침해사고 대응절차에 따라 처리와 복구를 신속하게 수행하여야 한다

	5.3. 사후관리	5.3.1. 침해사고 분석 및 공유	침해사고가 처리 및 종결된 후 발생 원인을 분석하고 그 결과를 이용자에게 알려야 한다. 또한 유사한 침해사고에 대한 신속한 처리를 위해 침해사고 관련 정보 및 발견된 취약점을 관련 조직 및 임직원과 공유하여야 한다.
		5.3.2. 재발방지	침해사고 관련 정보를 활용하여 유사한 침해사고가 반복되지 않도록 침해사고 재발방지 대책을 수립하고, 필요한 경우 침해사고 대응 체계도 변경하여야 한다.
6. 서비스 연속성관리	6.1. 장애대응	6.1.1. 장애 대응 절차 수립	관련 법률에서 규정한 클라우드컴퓨팅서비스의 중단으로부터 업무 연속성을 보장하기 위해 백업, 복구 등을 포함하는 장애 대응 절차를 마련하여야 한다.
		6.1.2. 장애 보고	클라우드컴퓨팅서비스 중단이나 피해가 발생 시 장애 대응 절차에 따라 법적 통지 및 신고 의무를 준수하여야 한다. 또한 클라우드컴퓨팅서비스 이용자에게도 발생 내용, 원인, 조치 현황 등을 신속하게 알려야 한다.
		6.1.3. 장애 처리 및 복구	클라우드컴퓨팅서비스 중단이나 피해가 발생할 경우, 서비스 수준 협약(SLA)에 명시된 시간 내에 장애 대응절차에 따라 해당 서비스의 장애를 처리하고 복구시켜야 한다.
		6.1.4. 재발방지	장애 관련 정보를 활용하여 유사한 서비스 중단이 반복되지 않도록 장애 재발방지 대책을 수립하고, 필요한 경우 장애 대응 절차도 변경하여야 한다.
	6.2. 서비스 가용성	6.2.1. 성능 및 용량 관리	클라우드컴퓨팅서비스의 가용성을 보장하기 위해 성능 및 용량에 대한 요구사항을 정의하고, 지속적으로 관리할 수 있는 모니터링 방법 또는 절차를 수립하여야 한다.
		6.2.2. 이중화 및 백업	정보처리설비(예 : 클라우드컴퓨팅서비스를 제공하는 물리적인 서버, 스토리지, 네트워크 장비, 통신 케이블, 접속회선 등)의 장애로 서비스가 중단되지 않도록 정보 처리설비를 이중화하고, 장애 발생 시 신속하게 복구를 수행하도록 백업 체계도 마련하여야 한다.
		6.2.3. 서비스	서비스 가용성에 대한 영향 평가를 주기적으로 점검하여야 한다.

		가용성 점검	
7. 준거성	7.1. 법 및 정책 준수	7.1.1. 법적요구사항 준수	정보보호 관련 법적 요구사항을 식별하고 준수하여야 한다.
		7.1.2. 정보보호 정책 준수	정보보호 정책 및 서비스 수준 협약에 포함된 보안 요구사항을 식별하고 준수하며 이용자가 요구하는 경우 관련 증거를 제공하여야 한다.
	7.2. 보안 감사	7.2.1. 독립적 보안감사	법적 요구사항 및 정보보호 정책 준수 여부를 보증하기 위해 독립적 보안감사 계획을 수립하여 시행하고 개선 조치를 취하여야 한다.
		7.2.2. 감사기록 및 모니터링	보안감사 증적(로그)은 식별할 수 있는 형태로 기록 및 모니터링 되어야 되고 비인가된 접근 및 변조로부터 보호되어야 한다.