정보보호 정책서는 클라우드컴퓨팅서비스를 제공하기 위한 운영문서로서 검토되고 승인됨	구분	직위	성명	일자	서명
	승인	정보보호 최고책임자	홍길동	2019.08.16	
	검토	정보보호 담당자	장길산	2019.08.12	

㈜클라우드
정보보호 정책서

2019. 08. 12

㈜클라우드

담당자문서 제·개정 이력				
번호	**날짜**	**쪽**	**내용**	**담당자**
1	2019-01-01	-	최초 작성	홍길동
2	2019-04-06	2	정보보호 최고책임자 변경	장길산
3	2019-07-01	10	망법 개정사항 반영 이용자 고지방법 변경	장길산
4	2019-08-12	2	정보보호 최고책임자 변경	장길산

[목 차]

제1장 총칙 ····· 1

제2장 정보보호 조직 ····· 1

제3장 인적 보안 ····· 1

제4장 정보자산 관리 ····· 2

제5장 서비스 공급망 관리 ····· 3

제6장 침해사고 관리 ····· 3

제7장 서비스연속성 관리 ····· 4

제8장 준거성 관리 ····· 4

제9장 가상화 보안 ····· 4

제10장 접근통제 ····· 5

제11장 네트워크 보안 ····· 5

제12장 데이터 보호 및 암호화 ····· 6

제13장 시스템 개발 보안 ····· 6

본 문서는 정보보호 정책서에 대한 예시이며, 클라우드컴퓨팅서비스 제공자는 자사의 서비스 형태, 운영환경 등을 고려하여 작성하여야 한다.

제1장 총칙

제1조(목적) 정보보호 정책서는 클라우드컴퓨팅서비스 제공을 위해 필요한 정보보호 정책을 수립하고 관리적, 물리적, 기술적인 정보보호 조치를 정의하기 위하여 작성되었다.

제2조(용어의 정의) 이 정책서에서 사용하는 용어의 뜻은 다음과 같다.

1. “클라우드컴퓨팅“(Cloud Computing)이란 집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원(이하 “정보통신자원“이라 한다)을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신축적으로 이용할 수 있도록 하는 정보처리체계를 말한다.
2. “클라우드컴퓨팅기술“이란 가상화 기술, 분산처리 기술 등 클라우드컴퓨팅의 구축 및 이용에 관한 정보통신기술을 말한다.
3. “클라우드컴퓨팅서비스“란 클라우드컴퓨팅을 활용하여 상용(商用)으로 타인에게 정보통신자원을 제공하는 서비스를 말한다.

제3조(적용범위) 이 정책서는 클라우드컴퓨팅서비스와 관련된 정보처리시스템, 전자적 파일과 인쇄물, 서면 등 모든 형태의 정보자산 및 정보자산을 관리 운영하는데 적용된다.

제2장 정보보호 정책 및 조직

제4조(정보보호 정책) ① 클라우드 정보보호정책을 수립하고, 정책 시행을 위한 관련 지침, 절차, 메뉴얼 등을 문서화하여야 한다.

② 클라우드 정보보호정책은 정보보호 최고책임자로부터 제·개정 시 승인을 받아야 한다.

③ 클라우드 정보보호정책에 영향을 받는 모든 임직원 및 외부 업무 관련자에게 정책의 내용을 이해하기 쉬운 형태로 전달하여야 한다.

④ 클라우드 정보보호정책 및 정책시행 문서에 대한 타당성 검토를 최소 연 1회 이상 수행하여야 한다. 또한, 관련 법규 변경 및 내·외부 보안사고 발생 등의 중대한 사유가 발생한 경우에는 추가로 검토하고 변경하여야 한다.

⑤ 정보보호 정책 및 정책 시행문서의 이력관리 절차를 수립하고 시행하며, 최신본으로 유지하여야 한다.

제5조(정보보호 조직) ① 조직 내에서 정보보호 관리 활동을 효과적으로 추진하기 위하여 이를 총괄 관리할 수 있는 정보보호 최고책임자(CISO)를 인사발령 등의 공식적인 지정절차를 거쳐 지정하여야 한다.

② 최고경영자는 조직의 규모 및 클라우드서비스의 중요도에 따라 필요인력, 예산 등을 분석하여 정보보호 실무조직을 구성하여야 한다.

③ 실무조직은 전담 또는 겸임조직으로 구성할 수 있으며 겸임조직으로 구성하더라도 정보보호 조직에 대한 공식적인 선언 또는 지정을 하여야 한다.

④ 정보보호 실무조직은 정보보호 관리자, 정보보호 담당자, 개인정보보호 책임자(CPO), 개인정보보호 관리자 및 개인정보보호 담당자로 구성할 수 있다.

⑤ 정보보호 조직 구성원의 주요 직무에 대하여 직무기술서 등을 통해 책임과 역할을 구체적으로 정의하여야 한다.

⑥ 회사가 제공하는 클라우드컴퓨팅서비스를 이용하는 이용자의 정보보호 관련 책임 및 역할은 이용자와의 계약서 또는 서비스 수준 협약(SLA)에 해당 내용을 반영하여야 한다.

제3장 인적 보안

제6조(내부인력 보안) ① 클라우드컴퓨팅서비스 업무에 종사하는 인력의 고용계약 시 정보보호 관련 법률 및 회사의 정보보호 정책을 준수하도록 비밀유지서약서를 부속 문서로 포함한다.

② 클라우드 운영, 보안, 개발 등 유관 업무에 새로 합류한 인원(신규입사 및 전입)은 정보보호 최고책임자의 승인을 득한 후 고용서약서에 서명하고 클라우드 컴퓨팅 서비스의 설비, 자원, 자산에 접근할 수 있다.

③ 중요 정보자산(정보, 시스템 등)을 취급하는 직무를 정의하고 해당 직무를 수행하는 주요 직무자를 지정하여야 하며, 주요 직무자는 최소의 인원으로 지정한다.

④ 주요 직무자의 현황을 주기적으로 관리하여 직무자별 부여된 권한의 적절성 여부를 검토하여야 한다.

⑤ 직무의 권한 오남용을 예방하기 위하여 주요 직무를 분리하고 직무별 역할 및 책임을 명확하게 기술하여야 한다.

⑥ 직무 분리가 어려운 경우 별도의 보완통제 방안을 수립하여 적용하여야 한다.

제7조(외부인력 보안) ① 클라우드컴퓨팅서비스 업무와 관련된 보안요구사항(정보자산 접근 등)을 외주 용역(업무 위탁, 유지보수 직원 등)과의 계약서에 반영하여야 한다.

② 명시된 보안요구사항의 준수 여부를 주기적으로 점검 또는 감사를 수행하여야 한다.

③ 외부인력이 업무를 수행하는 과정에서 퇴직, 인사이동 등 변경사항이 발생할 경우, 관련부서에 보고 및 공식적인 절차를 통해 자산 반납, 계정 삭제 등 보안절차를 수행하여야 한다.

④ 계약 만료 및 업무 종료 시 보안절차(자산 반납, 정보 파기, 계정 삭제 및 출입권한 삭제 등)를 수행하고 비밀유지서약서를 징구하여야 한다.

제8조(비밀유지서약서) ① 클라우드컴퓨팅서비스 업무를 수행하는 인력(외부인력 포함)은 정보보호

및 개인정보보호(해당되는 경우)에 대한 내용이 포함된 비밀유지서약서를 작성하여 회사에 제출하여야 한다.

② 비밀유지서약서는 주기적(연 1회)으로 작성하여 회사에 제출하여야 한다.

③ 직무변경, 휴직, 퇴직 등으로 인한 인사변경 발생하는 경우에 추가적으로 비밀유지서약서를 작성하여 회사에 제출하여야 한다.

④ 임시직원 혹은 외주 용역과 같은 외부자에게 정보자산에 대한 접근권한 부여, 변경 또는 해제 시 정보보호에 대한 책임, 조직 내 규정 준수, 정보보호 의무 미준수로 인한 사건사고 발생 시 책임 등이 명시된 정보보호서약서를 징구하여야 한다.

⑤ 정보보호서약서 및 비밀유지서약서는 법적 분쟁에 대한 증거자료로 사용할 수 있기 때문에 쉽게 찾아볼 수 있는 형태로 제3자에게 누출되지 않도록 안전한 장소에 보관 및 관리하여야 한다.

제9조(정보보호 교육) ① 내부의 관련된 모든 임직원과 외부 업무 관련자(외주 용역)를 위한 정보보호 교육, 훈련, 인식 프로그램을 수립하고 이에 따라 연 1회 이상 정기적으로 기본 정보보호 교육을 실시하여야 한다.

② 효과적인 교육 시행을 위해 다양한 교육방법(집합교육, 온라인교육 등)을 정할 수 있다.

③ 정보보호 인식제고를 위하여 정보보안의 날 지정, 뉴스레터 발송, 포스터 작성 등을 수행할 수 있다.

④ 개인정보관리책임자(CPO) 및 개인정보취급자는 정기적으로 개인정보보호 교육을 이수하여야 하며, 기본 정보보호 교육에 개인정보보호 내용을 포함하여 실시할 수 있다.

⑤ 클라우드 운영자 및 정보보호 직무자의 경우 기본 정보보호 교육 이외 클라우드 관련 보안교육을 별도로 연1회 이상 이수하여야 한다.

⑥ 정보보호 정책 및 절차의 중대한 변경, 조직 내·외부 보안사고 발생, 정보보호 관련 법률 변경 등 발생 시 정기 교육 외 추가 교육을 실시할 수 있다.

⑦ 정보보호 교육, 훈련, 인식 프로그램의 수행 결과를 평가하고 ~~평가~~ 결과를 분석하여 프로그램 개선에 반영하여야 한다.

제4장 정보자산 관리

제10조(자산 식별 및 분류) ① 정보자산(정보시스템, 정보보호시스템, 정보 또는 서비스)의 분류기준을 수립하고 클라우드컴퓨팅서비스를 제공하기 위한 모든 정보자산을 식별하여야 한다.

② 식별된 정보자산은 별도의 목록으로 문서화하여 관리하여야 한다.

③ 정보자산 목록은 정기적으로 정보자산 현황을 조사하여 최신으로 유지하여야 한다.

④ 식별된 정보자산에 대한 책임자 및 관리자(또는 담당자)를 지정하여 관리하여야 한다.

⑤ 정보자산의 중요도를 법적요구사항 및 기밀성, 무결성, 가용성 등을 고려하여 평가하기 위한

기준을 수립하고, 적절한 보안등급을 부여 및 관리하여야 한다.

⑥ 정보자산의 취급절차를 보안등급에 따라 정의 및 이행하여야 한다.

제11조(자산 변경 관리) ① 클라우드 시스템 관련 자산(시설, 장비, 소프트웨어 등)에 대한 변경을 위한 절차를 수립하고 이행하여야 한다.

② 클라우드 시스템 관련 자산에 대한 변경을 수행하기 전 성능 및 보안에 미치는 영향분석을 실시하고 이용자에게 큰 영향을 주는 경우 사전에 공지하여야 한다.

③ 클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경을 지속적으로 모니터링하여 허가 받지 않은 변경을 탐지하고 최신의 변경 이력을 유지하여야 한다.

④ 자산변경 후, 보안성 및 호환성에 대한 검증작업을 수행하여야 한다.

제12조(위험관리) ① 다양한 측면(관리적, 물리적, 기술적 등)에서 발생할 수 있는 위험을 식별하여 평가할 수 있는 방법을 정의하여 문서화 및 관리하여야 한다.

② 위험관리를 수행하기 위한 전문인력 구성, 기간 대상, 방법 등을 구체화하여 위험관리계획을 수립 및 이행하여야 한다.

③ 클라우드컴퓨팅서비스 취약점 점검 절차 및 기준을 수립하여 연 1회 이상 점검을 수행하여야 한다.

④ 발견된 취약점에 대한 대응방안 및 조치결과를 문서화하고 수행하고 그 결과를 책임자에게 보고하여야 한다.

제5장 서비스 공급망 관리

제13조(공급망 관리 정책) ① 클라우드컴퓨팅서비스에 대한 접근과 서비스 연속성을 저해하는 위험을 식별하고 최소화하기 위해 공급망과 관련한 보안 요구사항을 정의하는 관리정책을 수립하여야 한다.

② 클라우드컴퓨팅서비스 범위 및 보안 요구사항을 포함하는 공급망 계약을 체결하고 다자간 협약 시 책임을 개별 계약서에 각각 명시해야 하며, 해당 서비스에 관련된 모든 이해관계자에게 적용하여야 한다.

제14조(공급망 변경 관리) ① 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.

② 클라우드 공급망에 대한 보안위험을 재평가하여 안전성을 확보하여야 한다.

③ 서비스 수준 협약의 요구사항에 대한 준수 여부를 모니터링할 수 있는 체계를 수립하고 주기적인 검토를 수행하여야 한다.

제6장 침해사고 관리

제15조(침해사고 대응 절차 및 체계) ① 침해사고의 정의 및 범위, 긴급연락체계 구축, 침해사고 발생 시 보고 및 대응절차, 사고 복구조직의 구성 등을 포함한 침해사고 대응절차를 수립하여야 한다.

② 침해사고에 대한 효율적이고 효과적인 대응을 위해 신고절차, 유출 금지 대상, 사고 처리 절차 등을 담은 침해사고 대응절차를 마련하여야 한다.

③ 침해사고 대응절차는 이용자와 제공자의 책임과 절차가 포함되어야 한다.

④ 침해사고 정보를 수집·분석·대응할 수 있는 보안관제 시스템 및 조직을 구성·운영하고, 침해사고 유형 및 중요도에 따라 보고 및 협력체계를 구축하여야 한다.

⑤ 외부기관(외부 관제 업체 등)을 통해 침해사고 대응체계를 구축 및 운영할 경우 대응절차의 세부사항을 계약서에 반영하여야 한다.

⑥ 침해사고의 모니터링, 대응 및 처리와 관련되어 외부 전문가, 전문업체, 전문기관(KISA) 등과의 연락 및 협조체계를 수립하여야 한다.

⑦ 침해사고 대응과 관련된 역할 및 책임이 있는 담당자를 훈련시켜야 하고, 주기적으로 침해사고 대응 능력을 점검하여야 한다.

제16조(침해사고 대응) ① 침해사고 발생 시 침해사고 대응 절차에 따라 법적 통지 및 신고 의무를 준수하여야 한다.

② 클라우드컴퓨팅서비스 이용자에게 발생 내용, 원인, 조치 현황 등을 신속하게 알려야 한다.

③ 침해사고 발생 시 침해사고 대응 절차에 따라 처리와 복구를 신속하게 수행하여야 한다.

제17조(사후관리) ① 침해사고가 처리 및 종결된 후 발생 원인을 분석하고 그 결과를 이용자에게 알려야 한다.

② 침해사고 정보와 발견된 취약점을 관련 조직 및 인력과 공유하여야 한다.

③ 침해사고 분석을 통해 얻어진 정보를 활용하여 유사 사고가 재발하지 않도록 보안시스템 개선, 관련 보안교육 실시 등 대책을 수립하고 필요한 경우 침해사고 대응절차 등을 변경하여야 한다.

제7장 서비스연속성 관리

제18조(장애 대응) ① 관련 법률에서 규정한 클라우드컴퓨팅서비스의 중단으로부터 업무 연속성을 보장하기 위해 백업, 복구 등을 포함하는 장애 대응 절차를 마련하여야 한다.

② 클라우드컴퓨팅서비스 중단이나 피해가 발생 시 장애대응 절차에 따라 법적 통지 및 신고 의무를 준수하여야 한다. 또한, 클라우드컴퓨팅서비스 이용자에게도 발생 내용, 원인, 조치 현황 등을 신속하게 알려야 한다.

③ 클라우드컴퓨팅서비스 중단이나 피해가 발생할 경우, 서비스 수준 협약(SLA)에 명시된 시간 내에 장애 대응절차에 따라 해당 서비스의 장애를 처리하고 복구시켜야 한다.

④ 장애 관련 정보를 활용하여 유사한 서비스 중단이 반복되지 않도록 장애 재발방지 대책을 수립하고, 필요한 경우 장애대응 절차도 변경하여야 한다.

제19조(서비스 가용성) ① 클라우드컴퓨팅서비스의 가용성을 보장하기 위해 성능 및 용량에 대한 요구사항을 정의하고, 지속적으로 관리할 수 있는 모니터링 방법 또는 절차를 수립하여야 한다.

② 정보처리설비(예 : 클라우드컴퓨팅서비스를 제공하는 물리적인 서버, 스토리지, 네트워크 장비, 통신 케이블, 접속 회선 등)의 장애로 서비스가 중단되지 않도록 정보 처리설비를 이중화하고, 장애 발생 시 신속하게 복구를 수행하도록 백업 체계도 마련하여야 한다.

제8장 준거성 관리

제20조(법 및 정책 준수) ① 정보보호 관련 법적 요구사항을 식별하고 준수하여야 한다.

② 정보보호 정책 및 서비스 수준 협약에 포함된 보안 요구사항을 식별하고 준수하며 이용자가 요구하는 경우 관련 증거를 제공하여야 한다.

제21조(정보시스템 감사) ① 법적 요구사항 및 정보보호 정책 준수 여부를 보증하기 위해 독립적 보안감사 계획을 수립하여 시행하고 개선 조치를 취하여야 한다.

② 보안감사 증적(로그)은 식별할 수 있는 형태로 기록 및 모니터링 되어야 하고 비인가 된 접근 및 변조로부터 보호되어야 한다.

제9장 가상화 보안

제22조(가상화 인프라) ① 가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리방안을 수립하여야 한다.

② 가상자원 및 서비스를 제공하기 위한 웹사이트 또는 공개 서버를 제공하는 경우 기술적 보호대책을 수립 및 주기적 점검을 이행하여야 한다.

③ 이용자와의 계약 종료 시 자원 회수 절차에 따라 모든 가상 자원(백업 포함)을 모든 클라우드 시스템에서 삭제하여야 한다.

④ 무결성을 보장하기 위한 보호조치 및 변경내역(수정, 이동, 삭제, 복사 등)에 대해 모니터링하

고, 손상이 발생한 경우 이를 이용자에게 통지하기 위한 절차를 마련 및 운영하여야 한다.

⑤ 가상자원을 관리하는 하이퍼바이저의 기능 및 인터페이스에 대한 접근 통제 방안을 마련하고 하이퍼바이저에 대한 소프트웨어 업데이트 및 보안패치를 최신으로 유지하여야 한다.

⑥ 가상자원을 제공하기 위한 웹과 가상 소프트웨어(앱, 응용프로그램)를 배포하기 위한 공개서버에 대한 물리적, 기술적 보호대책을 수립 및 운영하여야 한다.

⑦ 표준화된 가상화 포멧, 이식성이 높은 가상화 플랫폼, 공개 API 등을 이용하여 클라우드컴퓨팅 서비스 간의 상호 운용성 및 이식성을 높여야 한다.

제23조(가상환경) ① 바이러스, 웜, 트로이목마 등의 악성코드로부터 이용자의 가상 환경(가상 PC, 가상서버, 가상 소프트웨어 등)을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술을 지원하고 이상징후 발견 시 이용자 통지하고 사용 중지 및 격리 조치를 수행하여야 한다.

② 가상 환경(가상 PC, 가상서버, 가상 소프트웨어 등) 접근을 위한 인터페이스 및 API에 대한 보안취약점을 주기적으로 분석하고, 이에 대한 보호 방안을 마련하여야 한다.

③ 이용자가 기존 정보시스템 환경에서 클라우드컴퓨팅서비스의 가상환경으로 전환 시 안전하게 데이터를 이전하도록 암호화 등의 기술적인 조치방안을 제공하여야 한다.

④ 클라우드컴퓨팅서비스 제공자는 출처, 유통경로 및 제작자가 명확한 소프트웨어로 구성된 가상환경을 제공하여야 한다.

제10장 접근통제

제24조(접근통제 정책) ① 비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다.

② 접근기록 대상을 정의하고 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 형태로 기록되고 유지하여야 한다.

제25조(접근 권한 관리) ① 클라우드 시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다.

② 클라우드 시스템 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제, 관리하여야 한다.

③ 클라우드 시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 점검하고 이상징후 발견 시 그에 따른 조치절차를 수립 및 이행하여야 한다.

제26조(사용자 식별 및 인증) ① 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.

② 클라우드 시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증절차에 의해 통제하여야 한다.

③ 이용자가 클라우드컴퓨팅서비스에 대해 다중 요소(인증서 기반, OTP, 지문 등)로 강화된 인증수단을 요청하는 경우 이를 제공하기 위한 방안을 마련하여야 한다.

④ 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.

⑤ 고객, 회원 등 외부 이용자가 접근하는 클라우드 시스템 또는 웹서비스의 안전한 이용을 위하여 계정 및 패스워드 등의 관리절차를 마련하고 관련 내용을 공지하여야 한다.

제11장 네트워크 보안

제27조(네트워크 보안) ① 클라우드컴퓨팅서비스와 관련된 내·외부 네트워크에 대해 보안정책과 절차를 수립하여야 한다.

② DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요정보 유출 등을 막기 위해 네트워크를 모니터링하고 통제하여야 한다.

③ 클라우드컴퓨팅서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보호시스템(방화벽, IPS, IDS, VPN 등)을 운영하여야 한다.

④ 클라우드 시스템에서 중요정보가 이동하는 구간에 대해서는 암호화된 통신 채널을 사용하여야 한다.

⑤ 클라우드컴퓨팅서비스 제공자의 관리 영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리하여야 한다.

⑥ 클라우드 시스템은 무선망과 분리하고 무선접속에 대한 접근을 통제하고, 무선접속 시 그 사유와 타당성을 검토하여 책임자의 승인을 받아야 한다.

⑦ 외부인에게 제공되는 무선네트워크는 내부네트워크(업무망)와 분리·운영하여야 한다.

제12장 데이터 보호 및 암호화

제28조(데이터 보호) ① 데이터 유형, 법적 요구사항, 민감도 및 중요도에 따라 데이터를 분류하고 관리하여야 한다.

② 이용자와 서비스 수준 협약 단계에서 데이터의 소유권을 명확하게 확립하여야 한다.

③ 입·출력, 전송 또는 데이터 교환 및 저장소의 데이터에 대해 항상 데이터 무결성을 확인하여

야 한다.

④ 데이터에 대한 접근제어, 위·변조 방지 등 데이터 처리에 대한 보호 기능을 이용자에게 제공하여야 한다.

⑤ 이용자에게 데이터를 추적하기 위한 방안을 제공하고, 이용자가 요구하는 경우 구체적인 제공 정보(이용자의 정보가 저장되는 국가의 명칭 등)를 공개하여야 한다.

⑥ 클라우드컴퓨팅서비스 종료, 이전 등에 따른 데이터 폐기 조치 시 이용자와 관련된 모든 데이터를 폐기하여야 하며, 폐기된 데이터를 복구할 수 없도록 삭제 방안을 마련하여야 한다.

제29조(매체 보호) ① 중요정보를 담고 있는 저장매체(하드디스크, 스토리지 등)의 폐기 및 재사용 절차를 수립하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제하여야 한다.

② 자체적으로 매체를 폐기할 경우 관리대장을 통해 이력관리를 수행하고, 폐기확인 증적을 함께 보관 및 관리하여야 한다.

③ 중요정보 유출을 예방하기 위해 이동매체(외장하드, USB, CD 등)의 취급, 보관, 폐기, 재사용에 대한 절차를 수립·운영하여야 하며 매체를 통한 악성코드 감염 방치 대책 및 중요정보 유출 방지 대책을 마련하여야 한다.

④ 중요 시스템이 위치한 통제구역, 주요 제한구역 등에서 이동매체의 사용을 제한하고, 사용 시 책임자의 허가절차를 거친 후 사용한다.

⑤ 이동매체의 보유현황을 최신화하여 유지하고, 관리실태를 주기적으로 점검하여야 한다.

제30조(암호화) ① 클라우드서비스에 저장 또는 전송 중인 데이터를 보호하기 위해 암호화 대상, 암호 강도(복잡도), 키 관리, 암호 사용에 대한 정책을 마련하고 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.

② 암호키 생성, 이용, 보관, 배포, 변경, 파기에 관한 안전한 절차를 수립하고, 암호키는 별도의 안전한 장소에 보관하여야 한다.

제13장 시스템 개발 보안

제31조(시스템 분석 및 설계) ① 신규 시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안취약점, 기밀성, 무결성, 가용성 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용하여야 한다.

② 클라우드 시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입·출력 및 송·수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다.

③ 클라우드 시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증

적을 확보할 수 있도록 하여야 한다.

④ 클라우드 시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다.

⑤ 로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 클라우드 시스템 시각을 공식 표준시각으로 정확하게 동기화하여야 한다. 또한 서비스 이용자에게 시각 정보 동기화 기능을 제공하여야 한다.

제32조(구현 및 시험) ① 안전한 코딩방법에 따라 클라우드컴퓨팅서비스를 구현하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다.

② 개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다. 단 분리하여 운영하기 어려운 경우 그 사유와 타당성을 검토하고 안전성 확보 방안을 마련하여야 한다.

③ 시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다.

④ 소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행하여야 한다. 또한 소스 프로그램은 운영환경에 보관하지 않는 것을 원칙으로 한다.

제33조(외주 개발 보안) ① 클라우드 시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독하여야 한다.

② 외주 위탁업체가 계약서에 명시된 보안요구사항 준수 여부를 관리·감독하여야 한다.

제34조(시스템 도입 보안) ① 신규 클라우드시스템 또는 보안시스템의 도입 시 안정성 확보를 고려한 도입계획을 수립하여야 한다.

② 클라우드시스템의 인수 여부를 판단하기 위한 인수 기준을 수립·운영하고 기준에 따른 적합성 테스트를 수행하여야 한다.

제14장 공공기관 보안요구사항

제35조(관리적 보호조치) ① 공공기관의 보안 요구사항이 반영된 보안서비스 수준 협약을 체결하고, 클라우드컴퓨팅서비스 관련 정보보호 정보를 공공기관에 제공하여야 한다.

② 클라우드컴퓨팅서비스 구축을 위해 도입되는 서버·PC 가상화 솔루션 및 정보보호 제품 중에

CC인증이 필수적인 제품군은 국내·외 CC인증을 받은 제품을 사용하여야 한다.

③ 클라우드컴퓨팅서비스 운영 장소 및 망은 공공기관 내부 정보 시스템 운영 보안 수준에 준하여 보안 관리하여야 한다.

④ 클라우드컴퓨팅서비스를 제공하는 민간 사업자는 사고 또는 장애 발생 시 공공기관의 사고·장애 대응 절차에 따라 해당 공공기관, 대내·외 관련 기관 및 전문가와 협조체계를 구성하여 대응하여야 하며, 공공기관의 사고·장애 대응에 적극 협조하여야 한다.

제36조(물리적 보호조치) ① 클라우드 시스템 및 데이터의 물리적 위치는 국내로 한정하고, 공공기관용 클라우드컴퓨팅서비스의 물리자원(서버, 네트워크, 보안장비 등), 출입통제, 운영인력 등은 일반 이용자용 클라우드컴퓨팅서비스 영역과 분리하여 운영하여야 한다.

② 클라우드컴퓨팅서비스를 제공하는 사업자는 네트워크 스위치, 스토리지 등 중요장비를 이중화하고 서비스의 가용성을 보장하기 위해 백업체계를 구축하여야 한다.

제37조(기술적 보호조치) ① 클라우드컴퓨팅서비스를 통해 생성된 중요자료를 암호화하는 수단을 제공하는 경우에는 검증필 암호모듈을 적용하여야 한다.

제15장 개인정보의 처리 및 안전한 관리

제38조(개인정보 수집·이용) ① 개인정보 수집□이용에 대하여 정보주체로부터 개인정보 수집에 대한 동의를 받아야 한다.

② 정보주체에게 개인정보 이용에 대한 사항을 고지하여야 한다.

③ 개인정보 처리방침을 수립하고 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.

제39조(개인정보 처리제한) ① 법령에서 정한 경우를 제외하고 민감정보를 처리하여서는 아니된다.

② 법령에서 정한 경우를 제외하고 고유식별정보를 처리하여서는 아니된다.

③ 법령에서 정한 경우를 제외하고 주민등록번호를 처리하여서는 아니된다.

제40조(개인정보의 안전한 관리) ① 개인정보는 처리목적 달성 및 관계기관의 요청이 있는 경우 즉시 파기하여야 한다.

② 법령에 의해 개인정보를 파기하지 않고 보존해야 하는 경우 다른 개인정보와 분리하여 저장하여야 한다.

③ 개인정보의 처리와 관련한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다.

부칙

제1조(시행일) 이 규정은 정보보호 최고책임자의 승인일로부터 시행한다.

제2조 (정책의 이행) ① 회사의 정보보호 업무는 이 규정에 근거하여 수행하며 이에 명시되지 않은 사항은 회사의 다른 규정 및 관련 법령이 정하는 바에 따른다.

② 회사는 정보보호 정책 제·개정, 위험관리 및 내부감사 등 회사 정보보호 활동에 대해 적정성 여부를 검토하여 승인하고, 정보보호 활동을 위한 예산과 인력을 확보하여야 한다.

제3조(정책의 검토) 본 정책의 적절성을 연 1회 이상 정기적으로 검토하고, 필요 시 개정안을 마련하며 제정, 개정 및 폐기에 대해 이력을 관리하여야 한다.

제4조(예외 적용) 다음 각 호에 해당하는 경우에는 이 규정에서 명시한 내용이라도 정보보호 최고책임자의 승인을 받아 예외 취급할 수 있다.

1. 기술 환경의 변화로 적용이 불가능할 경우
2. 기술적·관리적 필요에 따라 정책의 적용을 보류할 긴급한 사유가 있을 경우
3. 기타 재해 등 불가항력적인 상황인 경우