㈜클라우드 정보자산관리지침은 클라우드컴퓨팅서비스를 제공하기 위한 운영문서로서 검토되고 승인됨	구분	직위	성명	일자	서명
	승인	정보보호 최고책임자	홍길동	2019.01.01	
	검토	정보보호 담당자	장길산	2019.01.01	

㈜클라우드
정보자산 관리지침

2019. 01. 01

㈜클라우드

문서 제·개정 이력				
번호	**날짜**	**쪽**	**내용**	**담당자**
1	2019-01-01	-	최초 작성	홍길동

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

제1장 총칙

제1조(목적) 이 지침은 ㈜클라우드의 「정보보호정책서」에 의거 정보자산에 대한 관리에 필요한 사항을 규정함을 목적으로 한다.

제2조(적용범위) 이 지침은 ㈜클라우드의 클라우드컴퓨팅서비스 업무에 종사하는 임직원 및 ㈜클라우드와 계약을 맺어 클라우드컴퓨팅서비스 업무 외부업체 직원 모두에게 적용된다.

제3조(용어정의) 이 지침에서 사용되는 용어 정의는 다음 각 호와 같다.

1. “서버”라 함은 서버용 운영체제(윈도우, 리눅스 등)가 탑재되어 운영되는 하드웨어, 소프트웨어를 총칭한다.
2. “서버관리자”라 함은 정보시스템에서 서비스되고 있는 서버 장비의 보안 및 운영 업무를 담당하는 자를 말한다.
3. “정보자산”이라 함은 클라우드서비스를 제공하는데 포함되는 정보시스템, 정보보호시스템, 정보 또는 서비스를 말한다.

제4조(서버관리자) ① 서버관리자는 서버의 운용 유지보수 관리 및 보안 운용을 위한 업무는 다음 각 호와 같다.

1. 서버 운영 관리(계정, 서비스, 도입/변경/폐기, 백업/복구, 관리)
2. 서버의 로깅 설정, 로그 점검
3. 보안문제에 대한 신속한 해결 및 패치
4. 보안사고 대응 및 지원
5. 서버 보안패치 적용 및 취약점 제거
6. 보안관련 문제 발견, 장비의 상태 및 로그관리, 장애발생 시 정보보호최고책임자에게 통보

제5조(사용자) ① 사용자는 서버에 접속할 수 있는 자와 서버 응용프로그램에 접속하여 업무를 수행하는 자로서 다음 각 호의 업무를 수행한다.

1. 서버에 접속하거나 서버의 응용프로그램에 접속하여 업무 수행 시 접근이 불가능하거나 이상이 발견되면 즉시 서버관리자에게 통보하여야 한다.
2. 모든 사용자는 서버 접근 시 인가된 경로를 통해 허용된 용도로만 사용하여야 한다.

제2장 정보자산의 식별 및 분류

제6조(정보자산 식별) ① 클라우드컴퓨팅서비스에 사용된 정보자산(정보시스템, 정보보호시스템, 정보 등)에 대한 자산분류기준 수립하고 식별된 자산의 목록을 작성하여 관리하여야 한

다.

② 주기적으로 정보자산 현황을 조사하여 정보자산목록을 최신으로 유지하여야 한다.

제7조(정보자산 분류) ① 서비스의 특성에 적합하도록 별지 제2호 서식 '정보자산분류표'를 참고하여 정보자산 분류기준을 수립하여야 한다.

제8조(정보자산 식별자 부착) ① 식별된 정보자산 중 서버나 관리용 단말과 같은 HW장비, SW의 CD케이스, USB 등의 경우에는 해당 정보자산을 쉽게 확인할 수 있도록 식별자를 부착하여야 한다.

장비관리번호	
장비명	
구입날짜	사용용도
팀명	관리자명

제3장 정보자산 변경관리

제9조(변경관리) ① 운영체제 업그레이드, 상용 소프트웨어 설치, 운영 중인 응용프로그램 기능 개선, 네트워크 구성 변경, CPU/메모리/저장장치 증설 등 정보시스템 관련 자산 변경이 필요한 경우 변경요청, 책임자 검토·승인, 변경확인, 변경이력관리 등의 공식적인 절차를 수립하고 이행하여야 한다.

② 클라우드컴퓨팅서비스에 사용된 자산의 변경이 발생할 경우 다음 사항을 고려하여 보안영향평가를 수행하여야 한다.

- 변경이 클라우드서비스의 보안에 미치는 영향
- 변경이 클라우드서비스의 성능에 미치는 영향
- 변경이 클라우드서비스의 일반적인 업무에 미치는 영향

③ 클라우드서비스 관련 정보자산 변경 시 사용자에게 큰 영향을 주는 변경에 대해서는 사전에 다음의 내용을 사용자에게 공지하여야 한다.

- 변경 내용(자산변경, 작업 등) 및 일시
- 영향 범위
- 긴급연락처 등

④ 자산의 변경 시 문제가 발생할 것을 대비하여 변경을 수행하기 전에 정보자산의 백업을 수행하여야 한다.

⑤ 변경을 수행하기 전에 변경에 대한 계획을 수립하고 변경계획에 대하여 정보보호 최고책임자로부터 승인을 받아야 한다.

⑥ 서버 등 전산장비 및 전산시설을 변경하는 경우 운영 전에 정상적으로 동작하는지 확인

하여야 한다.

⑦ 소프트웨어 등 어플리케이션에 대한 변경(업데이트 포함)을 수행하는 경우 운영 전에 타 운영자산과의 호환성 등을 확인하여 운영에 지장을 초래하지 않도록 하여야 한다.

제4장 위험관리

제10조(취약점 점검계획) ① 정보보호 최고책임자는 클라우드컴퓨팅서비스 전체를 대상으로 주기적(년 1회 이상)으로 취약점 점검을 수행하여야 한다.

② 정보보호 담당자는 취약점 점검 계획을 수립하고 정보보호 최고책임자의 승인을 받은 후에 수행하여야 한다. 취약점 점검 계획에는 다음의 사항이 포함되어야 한다.

- 취약점 점검대상
- 취약점 점검일정
- 취약점 점검 담당자 및 책임자 지정
- 취약점 점검 절차 및 방법 등

③ 외부의 전문업체를 통하여 취약성 점검을 수행하는 경우 관련 계약서 제2항의 내용이 상세하게 포함되도록 하여야 한다.

④ 정보보호 담당자는 취약점 점검으로 인하여 클라우드서비스 운영에 영향을 미치지 않도록 사전 확인을 수행하여야 한다.

제11조(취약성 점검) ① 정보보호 담당자는 취약성점 점검을 수행하는 경우 다음의 항목을 포함하여 취약성 점검을 수행하여야 한다.

- 서버 OS, 보안 설정 취약점
- 애플리케이션 취약점
- 웹 서비스 취약점
- 스마트기기 및 모바일 서비스(모바일 앱 등) 취약점
- 가상인프라 및 가상자원 취약점 등

② 취약점 점검 시 이력이 관리될 수 있도록 점검일시, 점검대상, 점검방법, 점검내용 및 결과, 발견사항, 조치사항 등이 포함된 보고서를 작성하여야 한다.

③ 취약점 점검결과 발견된 취약점별로 대응방안 및 조치결과를 문서화하여야 하며 조치결과서를 작성하여 정보보호 최고책임자에게 보고하여야 한다.

[별지 제1호 서식]정보자산 목록

별첨 “03. 정보자산관리지침 별첨 클라우드 보안인증(SaaS) 정보자산목록.xlsx” 참조

[별지 제2호 서식]정보자산 분류

정보자산 분류표

분류	설명
정보시스템	운영체제, 소프트웨어를 동작시키기 위해 필요한 WEB/WAS/DBMS 등이 설치된 시스템(가상서버 포함) 예) 클라우드 상의 가상 서버(VM), 방화벽, IPS, WAF 등
소프트웨어	CSP 등에 의해 개발되거나(예 : 그룹웨어, 보안서비스 등) 도입된(예 : WAS, DBMS 등) 애플리케이션(SaaS 서비스를 개발 및 운영하는데 사용된 오픈소스 포함)
정보	문서적 정보(라이센스 등)와 전자적 정보(SW이미지 등 모두를 포함)

[별지 제3호]정보자산 중요도 평가 기준

보안 요구사항	내 용	평가 수준
기밀성	■ 자산이 유출되는 경우 회사에 중대한 금전적 손실이 발생할 수 있는 경우 ■ 자산 소유자인 담당부서 또는 담당자만이 접근 및 관리가 가능한 자산	상
	■ 자산이 유출되는 경우 회사에 약간의 금전적 손실이 발생할 수 있는 경우 ■ 자산 소유 담당부서/담당자 이외 관련 담당부서 등 회사 조직 내부에 국한하여 접근 및 열람이 가능한 정보를 가지고 있는 자산	중
	■ 자산이 유출되어 공개되어도 관계 없거나 손실을 발생시키지 않는 경우 ■ 조직 외부인이 접근 및 열람이 가능한 정보를 담고 있는 자산 ■ 해당 자산에 별도 정보가 기록되어 있지 않거나, 공개되어도 무방한 경우	하
무결성	■ 자산 변조 시 업무수행 또는 서비스에 중대한 장애를 유발하거나, 회사에 중대한 금전적 손실이 발생하는 경우 ■ 자산 변조 가능성이 높고, 변조 시 데이터의 무결성을 검증하기 힘든 경우 ■ 해당 자산정보에 대한 실시간 백업이 이루어지고 있지 않아 원래의 정보를 복구하기 힘든 경우	상
	■ 자산 변조 시 업무수행 또는 서비스에 중대한 장애를 유발하거나, 회사에 중대한 금전적 손실이 발생하는 경우 ■ 자산 변조 가능성이 높고, 변조 시 데이터의 무결성을 검증하기 힘든 경우 ■ 해당 자산정보에 대한 실시간 백업이 이루어지고 있지 않아 원래의 정보를 복구하기 힘든 경우	중
	■ 자산이 변조되어도 업무수행에 미치는 영향이 미흡한 경우 ■ 자산에 포함된 정보의 변조 가능성이 희박하고, 정보 변조 시 무결성 검증이 용이한 경우	하
가용성	■ 자산의 가용성 훼손 시, 업무수행 또는 서비스에 중대한 장애를 유발하거나, 회사에 중대한 금전적 손실이 발생하는 경우 ■ 해당 자산이 사용 불가능할 때, 대체(백업) 자산이 없어 장기적인 업무 중단이 발생하는 경우 ■ 연중 24시간 무중단 운영되는 자산(장비)으로서, 장애 발생 시 즉시 복구되어야 하는 경우 ■ 해당 자산에 대한 장애 또는 침해사고 발생 시 직접적인 서비스 중단을 야기하는 경우	상
	■ 해당 자산이 사용 불가능할 때, 대체 자산을 투입하기까지 단기적인 업무장애가 발생하는 경우 ■ 연중 24시간 무중단 운영되는 자산(장비)으로서, 장애 발생 시 1시간 이내에 복구되어야 하는 경우 ■ 장비 장애로 인하여 서비스 중단은 발생하지 않으나 성능에 영향을 미치는 경우	중
	■ 해당 자산이 사용 불가능할 때, 대체 자산을 즉시 투입하여 업무 장애 발생 가능성이 낮은 경우 ■ 연중 24시간 무중단 운영되는 자산(장비)으로서, 장애 발생 시 수 시간 이내에 복구되어야 하는 경우 ■ 장비 장애 시 서비스 중단 또는 성능 저하에 직접적인 영향을 미치지 않는 경우 ■ 백업 장비의 경우	하