㈜클라우드 데이터보호 및 암호화 지침은 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
데이터보호 및 암호화 지침

2019. 01. 01

㈜클라우드

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

본 문서는 데이터보호 및 암호화 지침에 대한 예시이며, 클라우드컴퓨팅서비스 제공자는 자사의 서비스 형태, 운영환경 등을 고려하여 작성하여야 한다.

제1장 총칙

제1조(목적) 이 지침은 ㈜클라우드의 「정보보호정책서」에 의거 구성원의 데이터보호 및 암호화 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 사용하는 용어의 정의는 다음과 같다.

1. “암호화(Encryption)”라 함은 암호화 기법 및 프로그램을 사용하여 평문 정보를 알아볼 수 없는 정보로 변환하는 과정을 말한다.
2. “복호화(Decryption)”라 함은 암호화 기법 및 프로그램을 사용하여 암호화된 정보를 다시 평문 정보로 변환하는 과정을 말한다.
3. “암호 키(Encryption Key)” 라 함은암호화 및 복호화를 수행하기 위해 암호화 기법 및 프로그램에서 사용하는 키를 말한다.

제2장 데이터 보호

제4조(데이터 생명주기) ① 클라우드컴퓨팅서비스 이용자의 데이터 생성, 전송, 저장, 사용, 이전, 폐기, 백업 및 복구 등의 내용이 포함된 데이터 생명주기를 수립하여야 한다.

제5조(데이터 분류) ① 이용자 데이터, 사용자 데이터, 개인정보 데이터를 분류하고 각 데이터의 특성에 맞는 보안대책을 적용하여야 한다.

- 이용자 데이터 : 데이터의 소유권이 이용자에게 있고 이용자의 업무를 위해 이용자가 생성한 데이터
- 사용자 데이터 : 데이터의 소유권이 클라우드서비스 제공자에게 있고 클라우드컴퓨팅서비스 운영을 위해 필요한 데이터
- 개인정보 : 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보

제6조(데이터 소유권 고지) ① 클라우드 사업자는 서비스 제공 시 발생되는 데이터의 명확한 소유권을 확립하여야 하며, 데이터 소유권은 사업자와 이용자 사이의 계약서에 의해 정의되어야 한다.

② 이용자 데이터는 이용자에게 소유권이 있음을 SLA에 명확하게 명시하여야 한다.

③ 이용자 데이터에 대한 저장 위치(IDC 센터명)를 명확하게 고지하여야 한다.

제7조(데이터 무결성) ① 데이터 생명주기 전반에 걸쳐 이용자 데이터를 보호하기 위한 다음의 사항을 고려하여 안전한 관리 방안(접근통제, 무결성 점검 등)이 수립하여 적용하여야 한다.

- 접근통제 방안
  - 관리자/이용자 등록 및 권한 부여
  - 접근권한 관리 및 검토
  - 접근기록 관리
  - 사용자에 대한 식별 및 인증
  - 비밀번호 관리
- 무결성 점검 방안
  - 이용자 데이터 입출력, 전송, 저장 시 암호화
  - 접근기록 검토(응용프로그램, 데이터베이스 등)

② 사용자는 법적으로 허용된 범위 외에는 이용자 소유의 파일에 접근하거나 파일 내용을 볼 수 없도록 하여야 한다.

③ 클라우드시스템 내 이용자 데이터의 무결성을 보장하기 위한 다음과 같은 무결성 보장절차를 적용하여야 한다.

- 데이터 입력, 출력 시
  - 서비스 이용자 또는 서비스 관리자 App에서 데이터 입력, 출력 시 무결성 보장
- 데이터 전송 시
  - 데이터 전송 시 암호화
- 데이터 저장 시
  - 중요 데이터 저장 시 암호화
  - 다수 이용자에게 서비스를 제공할 경우 데이터 개별 분리 (텐넌트 분리, 테이블 분리, 물리적 분리 등)
- Application 및 툴을 통한 데이터베이스 접근 시
  - 이용자, 관리자 인증 및 단말기 인증 등 접근통제
  - 접근가능 권한 보유자 및 권한 최소화 관리 등
- 기타
  - 접근 기록 생성 및 보관
  - 접근 기록 주기적인 검토

제8조(개인정보 보호) ① 이용자의 개인정보는 관련 법률에 따라 안전하게 보호하여야 한다.

② 관련 법률이라 함은 개인정보보호법, 동법 시행령, 동법 시행규칙, 개인정보의 안전성 확보조치 기준, 정보통신망법, 동법 시행령, 동법 시행규칙, 개인정보의 기술적 관리적 보호조치 기준 등을 말한다.

제9조(데이터 보호) ① 클라우드컴퓨팅서비스 제공자는 중요 데이터(로그정보, 이용자 데이터 등)에 대한 접근을 엄격히 통제하고 안전히 처리・보관하여야 한다.

② 모든 매체(스토리지, 백업 드라이브 등), 가상화된 이미지, 스냅샷에 대해 엄격한 접근 통제가 이루어져야 된다.

- 데이터에 대한 논리적 접근제어(가상화 이지미 및 스냅샷 등)

③ 다음과 같은 데이터의 분실 방지 대책이 마련, 운영하여야 한다.

- 저장 데이터 : 클라우드시스템 내 스토리지에 저장된 데이터
- 이동 중인 데이터 : 클라우드 서비스 중 내외부 네트워크에서 이동 중인 이용자 데이터

④ 이용자 데이터는 가상화 기술을 통한 테넌트 분리, DB 테이블 분리 등을 통해 논리적으로 분리되어 운영되거나, 물리적 분리가 필요한 경우 별도의 저장장치(스토리지 등)를 통해 저장되어 관리되어야 한다.

제10조(데이터 폐기) ① 클라우드시스템 폐기 또는 재사용 발생 시 중요정보를 담고 있는 저장매체 처리(폐기, 재사용) 절차를 수립•이행하여야 한다.

② 이용자와의 서비스 종료 또는 이전 시, 이용자의 데이터를 재사용 할 수 없도록 정보를 삭제하여야 한다.

③ 이용자의 데이터를 백업해 놓은 경우, 저장된 백업 데이터도 일정 기간 이내(이용자와 협의하여 기한을 정함)에 삭제되어야 한다.

④ 재해복구(DR)를 위해 이용자의 데이터를 백업해 놓은 경우, 저장된 백업 데이터도 일정 기간 이내에 삭제되어야 한다.

⑤ 데이터 폐기 이후 폐기 사실에 대하여 이용자에게 통보한다.

제3장 암호화

제11조(암호정책) ① 클라우드시스템에서 중요정보의 전송 및 저장 시 안전한 보호를 위한 암호 정책을 수립•이행하여야 한다.

② 다음과 같은 중요정보 및 법적 요구사항에 따라 암호화가 필요한 데이터는 암호화하여 저장하여야 한다.

- 중요정보

  • 클라우드 시스템 운영과 관련된 정보 (정보자산목록, 네트워크 구성도, 취약점점검결과, 위험분석평가결과보고 등)

- 클라우드서비스와 관련하여 이용자와 협의된 정보
- 기타 SaaS 사업자가 중요도를 판단한 정보

- 법적 요구사항
  - 고유식별정보 (여권번호, 외국인등록번호, 운전면허번호, 주민등록번호)
  - 금융정보 (계좌번호, 신용카드번호)
  - 개인정보
  - 인증정보 (비밀번호, 바이오정보 등)

② 데이터 암호화 시에는 안전한 암호알고리즘을 사용하여야 하며, 보안강도가 2112 이상의 암호 키를 사용하여야 한다.

③ 관리자/사용자/이용자의 비밀번호를 저장하는 경우 복호화가 불가능한 일방향 해시알고리즘을 적용하여 저장하여야 한다.

④ 주요정보의 전송 시에는 기밀성 및 무결성이 지원되는 안전한 채널을 적용하여야 한다.

제12조(암호 키 관리) ① 암호키 생성, 이용, 보관, 배포, 파기에 대해 다음과 같은 항목이 포함된 정책 및 절차를 수립하고 이행하여야 한다.

- 암호키 관리 담당자 지정
- 암호키 생성, 보관(소산 백업 등) 방법
- 암호키 배포 대상자 정의 및 배포방법 (복호화 권한 부여 포함)
- 암호키 사용 유효기간 (변경주기)
- 복구 및 폐기 절차 및 방법 등

② 암호키는 별도의 안전한 장소에 소산 보관하고, 암호키 사용에 관한 접근권한 부여를 최소화하여야 한다.

③ 생성된 암호키는 손상 시 시스템 또는 암호화된 정보의 복구를 위하여 별도의 매체에 저장 후 안전한 장소에 보관(소산 백업 포함)하여야 하며, 물리적으로 분리된 서버에 저장관리하여야 한다.

④ 암호키 변경에 관한 정책을 수립•이행하여야 하며, 유출 또는 해킹이 의심될 경우 즉시 암호키를 변경하여야 한다.