㈜클라우드 접근통제 관리지침은 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
접근통제 관리지침

2019. 01. 01

㈜클라우드

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

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

제1장 총칙

제1조(목적) 이 지침은 ㈜클라우드의 「정보보호정책서」에 의거 구성원의 접근통제 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. “접근통제”이라 함은 보안정책에 따라 접근객체에 대한 접근주체의 접근권한 확인 및 접근제러를 통해 자원에 대한 비인가 사용을 방지하는 기술을 말한다.

제2장 접근통제

제4조(접근통제 정책) ① 접근통제 정책은 네트워크, 서버, 응용프로그램, DB, 모바일기기 등 영역별 접근통제 규칙, 방법, 절차 등을 포함하여야 하며, 관리서버의 경우 강력한 인증을 고려하여야 한다.

② 업무상 불가피하게 접근통제 정책 예외사항이 발생할 경우 이를 보완할 수 있는 통제방안(허용 기간, 허용 단말기, 접근 위치 등)을 마련한 후 한시적으로 허용하여야 한다.

③ 클라우드시스템의 사용자/관리자 접속 내역을 기록하고, 접근의 타당성을 정기적으로 검토하여야 한다.

④ 클라우드시스템 관리자는 운영·관리 중인 시스템의 중요도에 따라 접근통제가 이루어지도록 한다.

⑤ 클라우드시스템 관리자는 접근통제시스템을 우회하여 접근하지 않도록 하여야 한다.

⑥ 클라우드시스템 관리자는 서버가 정상적으로 동작하지 않는 경우 정상 동작 시까지 사용자의 접근을 제한할 수 있다.

⑦ 5회에 걸쳐 사용자 인증 실패 시 서버 접속을 중지시키고 비인가자의 침입 여부를 점검하여야 한다.

제5조(원격접속 관리) ① 클라우드시스템는 원칙적으로 원격접속을 허용하지 않으며 다만 부득이한 경우 다음 각 호의 사항을 확인하고 정보보호 관리자의 승인을 득한 경우는 허용할 수 있다.

1. 별지 제2호 서식 ‘원격접속 보안서약서’
2. 원격접속 시간의 최소화
3. 원격접속에 대한 인증기능 사용

② 원격접속 관리를 위하여 통제할 사항은 다음 각 호와 같다.

1. 원격접속이 필요한 경우 접근통제 기능을 적용하여 제한된 서비스만을 사용하도록 통제하여야 한다.
2. 원격접속 시는 사용자 인증, 비밀번호 사용기준(자릿수, 변경주기, 사용기간 등) 및 사용기록 로깅 등의 보안기능을 적용하여야 한다.
3. 원격접속에 대한 무결성 및 비밀성 확보를 위해 암호화된 프로그램 또는 가상사설망(VPN)을 적용하여야 한다.
4. 인가하지 않은 사용자의 접근이 시도되고 있는지 주기적으로 점검(원격접속 주소, 시간 등)하여야 한다.

제6조(사용자 계정관리) ① 클라우드시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다.

② 사용자 계정 등록(신규, 변경, 삭제)이 필요한 경우 정보보호 관리자에게 제출하여야 하는 서류는 다음 각 호와 같다.

1. 원격작업 : 별지 제1호 서식 ‘사용자 계정(신규, 변경, 삭제, 공용) 신청서’ 및 별지 제2호 서식 ‘원격접속 보안서약서’
2. 사용자 계정 : 별지 제1호 서식 ‘사용자 계정(신규, 변경, 삭제, 공용) 신청서’

③ 클라우드시스템의 사용자 계정 등록•삭제(비활성화) 및 접근권한 등록•변경•삭제를 담당자가 임의대로 수행하여서는 안되며 수립된 절차에 따라 책임자의 승인이 완료된 후 이루어져야 한다.

④ 사용자 계정 발급 및 접근권한 부여의 적정성 검토를 위하여 클라우드시스템에 등록된 사용자 계정 및 접근권한 부여 현황을 문서 또는 시스템으로 기록•관리하여야 한다.

⑤ 특수권한을 갖는 관리자는 별도로 별지 제4호 서식 ‘특수권한 관리자 계정 관리대장’에 기록하고 관리하여야 한다.

제7조(사용자 인증) ① 클라우드시스템(네트워크 장비, 가상화 서버, 응용프로그램, DB 등) 및 정보보호시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하여야 한다.

② 공개 인터넷망을 통하여 접속을 허용하는 포털시스템의 경우 아이디, 비밀번호 기반의 사용자 인증 이외의 강화된 인증수단(OTP, 공인인증서 등) 적용을 고려하여야 한다.

③ 법적 요구사항에 따른 강화된 인증방식 사용이 필요한 경우 해당 정보시스템 접근 시 강화된 인증방식을 적용하여야 한다.

④ SSO 등 다양한 정보시스템에 대한 사용자 인증을 용이하게 하는 시스템을 운영하는 경우 병목 및 침투(인증 도용 등) 시 피해 확대 가능성이 있으므로 별도의 보안대책(주요 정보시스템 재인증 등)을 마련하여야 한다.

제8조(비밀번호 관리) ① 클라우드시스템 및 정보보호시스템에 대한 사용자의 안전한 비밀번호 사용 및 관리절차(작성규칙 등)를 다음과 같이 수립하고 이행하여야 한다.

- 사전공격(Dictionary attack)에 취약하지 않도록 문자(영문 대소문자), 숫자, 특수문자 등을 일정 자리수 이상으로 조합하도록 비밀번호 작성규칙을 수립하고 주기적으로 변경(분기 1회 이상 권고)
- 연속 숫자, 생일, 전화번호, 아이디 등 추측하기 쉬운 개인 신상정보를 활용한 취약 비밀번호사용 제한
- 정보시스템 도입 시 초기/임시 비밀번호 로그인 시 지체 없이 변경
- 비밀번호 처리(입력, 변경) 시 마스킹 처리
- 종이, 파일, 포켓용 소형기기 등에 비밀번호 기록•저장을 제한하고 부득이하게 기록 • 저장해야 하는 경우 암호화 등의 보호대책 적용
- 주기적인 비밀번호 변경
- 정보시스템 침해사고가 발생 또는 비밀번호의 노출 징후가 의심될 경우 지체없이 비밀번호 변경
- 비밀번호 자동 저장 금지
- 개인정보취급자의 경우, 비밀번호 작성 규칙에 대해 법적 요구사항 반영 등

② 클라우드시스템의 관리자 비밀번호는 일반 사용자 비밀번호와 별도로 관리하여야 하며, 관리자 비밀번호를 기록한 문서 또는 저장장치(보안USB 등)는 비밀등급에 준하여 취급하고, 내화 금고 등 잠금장치로 비인가자의 접근을 통제할 수 있는 안전한 곳에 보관하여야 한다.

③ 교육, 홍보, 안내 등을 통해 사용자 계정 및 비밀번호의 안전한 관리 절차에 대해 충분하게 공지하고 그에 따른 책임이 사용자에게 있음을 주지시켜야 한다.

④ 이용자가 접근하는 클라우드시스템 또는 웹서비스의 안전한 이용을 위하여 계정 및 비밀

번호의 관리절차를 마련하고, 관련 내용을 홈페이지 또는 메일 등을 통하여 이용자가 쉽게 확인하고 이해할 수 있도록 공지하여야 한다

⑤ 클라우드시스템 관리자는 관리자 계정에 대해서 별지 제3호 서식 ‘서버 관리자계정 관리대장’에 기록하여 대외비 문서로 취급하고, 별지 제4호 서식 ‘특수권한 관리자계정 관리대장’ 역시 대외비 문서로 등록하여 별도의 잠금장치가 있는 문서함에 보관하며 인가된 자 외에는 열람을 금지하여야 한다.

⑥ 클라우드시스템 관리자는 관리자 계정을 전자파일로 관리하는 경우 해당 파일은 암호화 등 안전한 조치를 취하여야 한다.

제9조(사용자 권한 관리) ① 클라우드시스템 관리자는 서버 접근 및 사용 권한 부여 시 고려하여야 하는 사항은 다음 각 호와 같다.

- 유지보수, 장애처리 등의 업무적인 필요성에 의하여 제3자에게 접근권한을 부여하여야 하는 경우, 정보보호 관리자의 승인을 득한 후 부여
- 서버의 정상적인 운용을 방해하거나, 다른 사용자의 사용을 저해하는 등의 행위가 발견되거나 의심이 될 때, 사용자의 권한을 제한 또는 취소 가능
- 공식적인 절차에 따른 접근권한 부여 여부
- 접근권한 분류체계의 업무목적(직무) 및 보안정책 부합 여부
- 접근권한 부여 승인자에 대한 적절성
- 직무변경 시 기존 권한 회수 후 신규업무에 적합한 권한부여 여부
- 업무 목적 이외의 과도한 권한 부여

② 클라우드시스템 관리자는 장기 미사용, 직무변경, 휴직, 퇴직, 업무시간 외 사용 등의 경우에도 접근권한 사용 현황을 검토하여 다음과 같은 조치를 취해야 한다.

- 장기 미사용(3개월 권고) 계정 및 접근권한 삭제
- 직무변경 시 기존 권한을 회수하고 신규 업무에 적합한 권한을 부여
- 휴직(병가, 출산 등) 시 계정 및 권한 회수
- 퇴직 시 지체없이 계정을 삭제
  (단, 계정삭제가 어려운 경우 권한 회수 한 후 계정을 정지)

제10조(외부인 접근통제) ① 클라우드시스템 관리자는 업무적인 필요성에 의하여 외부인에게 계정을 부여하는 경우, 별지 제1호 서식 ‘사용자계정(신규, 변경, 삭제) 신청서’를 제출받아 정보보호 관리자의 승인을 득한 후에 부여한다.

② 클라우드시스템 관리자는 외부인의 출입현황을 관리하고, 입회 감독하에 작업을 수행하도록 하여야 한다.

③ 기타 외부인에 대한 세부적인 보안 준수사항은「인적보안지침」과「접근통제관리지침」에 따른다.

[별지 제1호 서식]사용자 계정(신규, 변경, 삭제) 신청서

사용자 계정(신규, 변경, 삭제, 공용) 신청서

신청부서		신청인	(서명)
신청일		완료요청일	
전화번호(HP)		이메일	
신청구분		신청사유	
신청ID		비밀번호	
사용기간			
세부사항			
서비스구분			
서버명			
원격작업	출발지 IP		
	목적지 IP		
작업내역			

[별지 제2호 서식]원격접속 보안서약서

원격접속 보안서약서

본인은 (주)클라우드에 년 월 일부로 원격접속을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 회사의 제한구역 및 통제구역에 무단으로 출입하지 않는다.
2. 회사의 자산을 불법으로 유출, 변조하거나 훼손하지 않는다.
3. 회사의 자산을 개인적인 목적이나 이익을 위하여 사용하지 않으며, 허가된 용도로만 사용한다.
4. 허용되지 않은 정보자산에 접근을 시도하거나 정보보안 기능을 우회하는 시도를 하지 않는다.
5. 업무상 취득한 대학 또는 제3자 소유의 정보를 대학의 승인 없이 누설하지 않는다.
6. 회사의 통신망을 이용하여 외부인 접근이 금지된 타 대학이나 기관의 통신망 또는 시스템에 임의로 접속을 시도하지 않는다.
7. 회사의 자산(정보 포함)을 사용 후에는 즉시 대학에 전부 반환한다.
8. 기타 회사의 정보보안 관련 규정을 준수한다.

본인은 위의 사항을 숙지하여 이를 성실히 준수할 것이며 만일 이를 위반하였을 경우 민·형사상의 책임을 감수함은 물론 대학에 끼친 손해에 대해 지체 없이 변상·복구할 것을 서약합니다.

2019년 00월 00일

서 약 자 정보

성 명 : (서명)

소 속 :

연락처 :

(주)클라우드 귀하

[별지 제3호 서식]서버 관리자계정 관리대장

대외비

서버 관리자계정 관리대장

확인	서버보안담당자	정보보호관리자

No	서버명	서버담당자	IP	용도	사용자	사용자 ID	Password

[별지 제4호 서식]특수권한 관리자 계정관리 대장

대외비

특수권한 관리자 계정관리 대장

확인	서버보안담당자	정보보호관리자

No	계정	사용자	부서	업무목적	대상서버	등록일	ID

[별지 제5호 서식]접근권한 점검대장

접근권한 점검대장

확인	정보보호담당자	정보보호관리자

시스템명	NO	점검기준	점검결과	결과상세
	1	공식적인 절차에 따른 접근권한 부여 여부		
	2	접근권한 분류체계의 업무목적(직무) 및 보안규정 부합 여부		
	3	접근권한 부여 승인자에 대한 적절성		
	4	직무변경 시 기존 권한 회수 후 신규업무에 적합한 권한부여 여부		
	5	업무 목적 이외의 과도한 접근권한 부여 여부		
	6	사용하지 않은 유휴계정 존재 여부		
	7	특권자 계정 사용의 적절성 여부		

[별지 제6호 서식]공용계정 관리대장

대외비

공용계정 관리대장

확인	서버보안담당자	정보보호관리자

No	서버명	서버담당자	IP	용도	사용자	사용자 ID	Password