㈜클라우드 인적보안지침은 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
인적보안지침

2019. 01. 01

㈜클라우드

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

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

제1장 총칙

제1조(목적) 이 지침은 ㈜클라우드의 「정보보호정책서」에 의거 구성원의 인적보안 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. “임직원”이라 함은 회사 내에 임원 및 직원, 계약직, 아르바이트 등 회사에 속하는 자를 말한다.
2. “외부인력”이라 함은「직제규정」에서 정한 “직원“이 아닌 자로서 특정한 업무수행을 위한 계약에 의해 업무를 수행하는 자를 말한다.
3. “외부위탁”이라 함은 특정 업무를 외부업체에 위탁하여 처리하는 방식을 말한다.

제2장 임직원 인적 보안

제4조(채용 및 계약) ① 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 고용 계약서에 정보보호 정책 및 관련 법률을 준수하도록 하는 조항 또는 조건을 조건이 포함되어야 한다.

③ 제출된 정보보호서약서는 시건장치가 되어 있는 안전한 장소에 별도 보관 및 관리하여야 한다.

④ 정보보호담당자는 필요시 정보보호서약서를 요청할 수 있으며, 이 경우 인사관리담당자는 정보보호서약서의 사본을 전달한다.

제5조(기밀준수) ① 정보보호와 개인정보보호 등을 위해 필요한 사항을 비밀유지서약서에 정의하고 주기적으로 갱신하여야 한다.

② 직원 채용 시 사내 기밀사항에 관하여 직원이 지켜야 할 사항을 명시한 별지 제1호 서식 ‘비밀유지서약서’를 징구하여야 한다.

③ 보안서약서에는 업무상 취득한 정보에 대하여 어떠한 경우에도 공개하지 않으며, 이를 위반하였을 때에는 민・형사상 책임과 관계 법령에 의한 조치에 따를 것을 명시하여야 한다.

④ 정보보호 책임자는 주기적(연 1회)으로 ‘비밀유지서약서’를 징구하여야 한다.

⑤ 정보보호 책임자는 직무변경, 휴직, 퇴직 등으로 인한 인사변경이 발생한 임직원에게 추가적으로 ‘비밀유지서약서’를 징구하여야 한다.

제6조(상벌 규정) ① 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 직원으로서 회사의 발전에 공적이 있는 자 또는 근무성적이 탁월한 자에 대하여 포상을 한다.

③ 관계 법령 및 회사의 제규정을 위반하거나 재산상 손해를 끼치는 경우 징계 조치할 수 있다.

제7조(퇴직 및 계약해지) ① 퇴직 시 개인 소유를 제외한 본 회사에서 지급된 모든 자산을 정보보호 담당자에게 반납하여야 한다.

② 각종 시스템 접근 권한을 가지고 있는 직원이 퇴직 시 권한을 즉시 삭제하여야 한다.

③ 직원의 퇴직 시 정보보호담당자는 다음 각 호의 임무를 수행하여야 한다.

1. 모든 회사 관련 정보 및 자산의 반납 확인
2. 시스템 관리자에게 퇴직자의 권한 삭제 통보
3. 퇴직자의 업무 수행권한 종료
4. 별지 제1호 서식 ‘비밀유지서약서’를 징구

제8조(인사이동 시 보안조치) ① 인사이동 시에는 업무권한 등에 대한 계정 접근권한을 신규 부여함을 원칙으로 한다.

제9조(주요 직무자 지정) ① 중요 정보자산(정보, 시스템 등)을 취급하는 직무를 정의하고 해당 직무를 수행하는 주요 직무자를 지정하여야 한다.

② 클라우드 서비스 개발, 운영, 보안, 고객정보에 접근해야 하는 업무는 주요 직무로 지정하여야 한다.

③ 직무의 권한 오남용을 예방하기 위하여 주요 직무를 분리하고 직무별 역할 및 책임을 명확하게 기술하여야 한다.

④ 중요정보를 취급하는 주요 직무자는 최소한으로 지정하고 주기적으로 주요 직무자 현황을 관리하여야 한다.

⑤ 조직 규모가 작거나 인적 자원 부족 등의 사유로 인해 불가피하게 개발과 운영 직무 분리가 어려운 경우, 직무자간의 상호 검토, 상위관리자의 주기적인 직무수행 모니터링 및 변경 사항 검토/승인, 직무자의 책임추적성 확보 등의 보완통제를 마련하여야 한다.

제10조(보안교육) ① 모든 임직원 및 외부 업무 관련자를 포함하여 연간 정보보호 교육 프로그램을 수립하여야 한다.

② 정보보호 최고책임자는 임직원을 대상으로는 년 1회 이상 정보보호 관련 교육을 실시하여야 하며, 신규 직원 채용 시 보안교육을 실시하여야 한다.

③ 집합교육, 온라인교육, 전달교육 등 다양한 교육방법을 통해 효과적인 방법을 선택할 수 있다.

④ 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.

⑤ 개인정보관리책임자 및 개인정보취급자는 정기적으로 개인정보보호 교육을 이수하여야 한다. (기본 정보보호 교육에 개인정보보호 내용을 포함할 수 있다.)

⑥ 클라우드 운영자 및 정보보호 직무자는 기본 정보보호 교육 이외에 클라우드 관련 보안 교육을 별도로 연 1회 이상 이수하여야 한다.

제3장 외부인력 보안

제11조(외부위탁 계약 시 보안요구 사항) ① 외부인력(외부유지보수직원, 외부용역자 포함)에 의한 정보자산 접근 등과 관련된 보안요구사항을 계약에 반영하여야 한다.

② 외부위탁 계약 시 사전에 요구되는 보안사항을 점검하여야 한다.

③ 조직의 업무 중 서비스 제공을 위한 시스템 통합(SI), 운영(SM), 유지보수, 고객상담 등 업무를 위탁하는 경우, 업무 형태에 따라 다음과 같은 보안요구사항을 정의하여 계약 시 반영하여야 한다.

1. 정보보호 관련 법률 준수 (개인정보 처리 관련 등)
2. 정보보호서약서 제출 (비밀유지, 정보보호 책임 등)
3. 위탁 업무 수행 직원 대상 주기적인 정보보호 교육 수행
4. 업무수행 관련 취득한 중요정보 유출 방지 대책
5. 외부인력 내부네트워크(업무망) 연결 시 인터넷접속 제한
6. 외부인력 사무실 공간에 대한 물리적 보호조치 (장비 및 매체 반출입, 출입통제 등)
7. 외부인력 직원 PC 등 단말 보안 (백신설치, 안전한 패스워드 설정 및 주기적 변경, 화면보호기 설정 등)
8. 과도한 권한이 부여되지 않도록 접근권한 부여 및 해지 절차
9. 주기적 보안점검 수행
10. 무선네트워크 구축 및 사용 제한 (필요 시 위험분석을 통한 대책 마련 후 책임자 승인)
11. 재위탁 하도급 계약 시 본 계약 수준의 보안요구사항 정의
12. 보안요구사항 위반 시 처벌, 손해배상 책임
13. 보안사고발생에 따른 보고 의무 등

④ 계약사항에는 보안요구사항에 대한 위반 시 처벌 및 손해배상에 대한 조항이 포함되어야

한다.

⑤ 외부인 계약 시 계약서에는 외부인의 보안준수와 관련된 내용이 반드시 포함되어야 하며 계약서를 사전에 작성하여 정보보호 최고책임자와 협의하여야 한다.

⑥ 외부인 계약 시에는 다음 각 호의 사항을 고려하여야 한다.

1. 직무수행 능력 (학력, 자격, 경력 등)
2. 직무수행 경험 (유사업무 수행 경험)
3. 용역 외주업체와의 인력 교체 가능 여부 및 교체 시기의 신속성
4. 외부인 적격심사에 따른 책임사항 명문화

제12조 (외부인 보안관리) ① 계약서에 명시한 보안요구사항 준수 여부를 주기적으로 점검하고 위반사항이나 침해사고 발생 시 적절한 조치를 수행하여야 한다.

② 프로젝트 개발, 전산업무 관리 등 외부 위탁을 시행 시 업무 성격상 본 대학 기밀사항이나 고객 정보에 관한 사항을 접할 수 있는 경우 외부인으로부터 보안유지 및 책임에 관한 별지 제1호 서식 ‘비밀유지서약서’를 징구하여야 한다.

③ 외부인으로 인해 발생할 수 있는 보안, 장애, 사고의 위험을 평가한다.

④ 외부인의 고의, 부주의 등으로 인한 보안. 장애사고를 미연에 방지하고, 발생 시 책임 추적성을 명확히 할 수 있도록 통제방안을 수립하여 적용한다.

⑤ 정보보호 최고책임자는 사내에 6개월 이상 상주하는 외부인력을 대상으로 보안준수 여부를 검사하여야 한다.

제13조(외부인 보안교육) ① 모든 임직원 및 외부 업무 관련자를 포함하여 연간 정보보호 교육 프로그램을 수립하여야 한다

② 정보보호최고책임자는 외부용역 착수 전 후에 외부인에게 다음 각 호의 내용으로 교육을 실시할 수 있다.

1. 외부용역 관리 업무 기준 및 보안 특수조건
2. 기타 외부용역 업무를 수행함에 있어서 외부인이 알아야 할 사항 등

③ 장기적인 상주근무(1년 이상)하는 외부인력에 대하여 내부인력과 동일한 보안교육을 실시하여야 한다.

제14조(전산자료의 보안관리) ① 정보보호최고책임자는 전산자료의 보안관리를 위해 외부위탁업체로 하여금 보안규칙 및 보안관련 지침의 준수와 전산자료 보안관리 계획서 제출을 요청할 수 있다.

② 전산망도 IP현황, 개인정보 등 외부용역업체에 제공하는 대외비자료는 별지 제2호 서식

‘자료관리대장’을 작성하여 인계자(정보보호최고책임자)와 인수자(외부용역업체 관리책임자)가 직접 서명한 후 인계인수를 한다.

③ 사업 관련 자료 및 사업과정에서 생성된 모든 산출물은 파일서버에 저장하거나 분야별 보안담당자가 지정한 PC에 저장 관리한다.

제15조(외부인의 사무실 장비에 대한 보안관리) ① 사업 수행 장소는 시건과 통제가 가능한 공간을 제공하거나, 협의를 통해 동일한 환경이 구축된 외부 사무실을 사용할 수 있다.

② 외부 사무실을 사용할 경우 업무를 수행하는 공간에 대하여 보안점검을 최초 및 주기적으로 실시하고, 별지 제3호 서식 ‘사무실 보안점검 일지’을 작성한다.

[별지 제1호 서식] 비밀유지서약서

비밀 유지 서약서

상기 본인은 회사의 정보보호정책서 및 관련 지침을 충분히 숙지, 이해하였으며 아래의 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 회사의 비밀 보호와 관련된 회사의 모든 조치사항을 성실히 이행하겠습니다.

2. 본인은 회사 재직 시 취득한 회사의 비밀을 재직 중은 물론 퇴직 후에도 회사의 허가 없이 사용하거나 제3자에게 무단 누설하지 않겠으며, 특히 경쟁 회사에 유출하지 않도록 하겠습니다.

3. 본인이 퇴사 등으로 회사의 업무 수행을 중단하게 되는 경우, 본인은 회사으 비밀이 포함된 유형의 수령물을 회사에 반납하며, 이와 관련하여 작성된 복사본 기타 유/무형의 모든 정보를 폐기하여 회사의 비밀이 외부에 유출되지 않도록 만전을 기하겠습니다.

4. 만약 이 서약내용을 위반할 경우, 본인은 이로 인한 모든 민/형사상의 책임을 부담하며, 형법 및 부정경쟁방지 및 영업비밀보호에 관한 법률에 의거한 어떠한 처벌도 감수하겠습니다.

20 년 월 일

서약자 소속 직급 생년월일

직위 성명 인

㈜클라우드 대표이사

[별지 제2호 서식] 자료 관리대장

자료 관리대장

연번	자료명	인계 및 인수 정보				자료반납	
		인계자	인수자	날짜	장소	확인자	반납일

[별지 제3호 서식] 사무실 보안점검 일지

사무실 보안점검 일지

사업명 :
점검일 :
점검자 : (서명)

번호	점검항목	점검결과
1	사업에 참여하는 모든 인력으로부터 비밀유지서약서를 징구하였는가?	
2	사업에 참여하는 모든 인력에게 보안교육을 실시하였는가?	
3	사업관련 자료에 대한 보안대책을 수립하여 이행하고 있는가?	

[별지 제4호 서식] 연간교육 계획서

<table>
<tr>
<td>

2019년 정보보호 교육 계획(안)

2019. 1.

㈜클라우드

</td>
<td>

I. 교육 목표

■ 전문성 제고 및 글로벌 경쟁력 강화

- 전문성 제고

- 글로벌 경쟁력 강화

</td>
</tr>
<tr>
<td>

II. 2019년 교육 운영 계획

■ 내부 교육

- 정보보안교육(1차)
  - 일정 :
  - 장소 :
  - 대상 :
  - 교육내용
- 정보보안교육(2차)
  - 일정 :
  - 장소 :
  - 대상 :
  - 교육내용
- 개인정보보호교육
  - 일정 :
  - 장소 :
  - 대상 :
  - 교육내용

</td>
<td>

■ 외부 교육

- KISA 아카데미 교육
  - 과정명 :
  - 일정 :
  - 교육내용
- KISA 아카데미 교육
  - 과정명 :
  - 일정 :
  - 교육내용

</td>
</tr>
</table>

[별지 제5호 서식] 교육 참석자 목록

정보보안교육(1차) 참석자 명부

□ 교육 일시 : 00년 00월 00일 00시 ~ 00시

□ 교육 장소 :

No	직급	성명	서명
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

[별지 제6호 서식] 교육 이수증

교육 이수증			
성 명		소 속	
사 번		직 급	
교육과정명	2019년 정보보안교육(1차)		

귀하는 본사에서 수행하는 2019년 정보보안교육(1차) 과정을
이수하였음을 확인합니다.

2019. 07. 01

㈜클라우드 정보보호최고책임자 홍길동 (서명)

[별지 제7호 서식] 주요 가상 정보시스템 계정 및 권한 관리 대장

정보시스템 계정 및 권한 관리 대장

No	시스템	계정	사용자	부서	용도	기간	비고
1	DB서버	root	홍길동	개발팀	DB 관리	무기한	
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							