㈜클라우드 시스템개발 및 도입보안지침은 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
시스템개발 및 도입보안 지침

2019. 01. 01

㈜클라우드

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

본 문서는 시스템 개발 및 도입보안 지침에 대한 예시이며, 클라우드컴퓨팅서비스 제공자는 자사의 서비스 형태, 운영환경 등을 고려하여 작성하여야 한다.

제1장 총칙

제1조(목적) 이 지침은 ㈜클라우드의 「정보보호정책서」에 의거 구성원의 시스템 개발 및 도입과 관련한 보안사항을 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. “시스템”이라 함은 클라우드컴퓨팅 서비스 제공을 목적으로 도입, 구축, 운영하는 시스템을 말한다.
2. “외주위탁”이라 함은 개발 등 특정 업무를 외부업체에 위탁하여 처리하는 방식을 말한다.
3. “이관 담당자”라 함은 개발된 응용프로그램에 대한 최종 이관 담당자로서 별도 지정이 없는 경우 개발 관련 부서장이 담당한다.

제2장 시스템 개발

제4조(보안요구사항 정의) ① 신규 시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안취약점, 정보보호 기본요소(기밀성, 무결성, 가용성) 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용하여야 한다.

※ 참고사항

- 홈페이지 SW(웹) 개발보안 가이드 (KISA)
- 웹서버구축 보안점검 안내서 (KISA)
- 웹어플리케이션 보안 안내서 (KISA)
- 소프트웨어 개발보안(시큐어 코딩) 관련 가이드(JAVA, C, Android-JAVA) (행정자치부)
- 행정기관 및 공공기관 정보시스템 구축 · 운영 지침 (행정자치부)

제5조(인증 기능) ① 설계 시 사용자 인증에 대한 보안 요구사항을 정의하여 반영하여야 한다.

- 인증 시기 : 이용자의 서비스 접근 시, 관리자의 관리페이지 접근 시, 기타 중요 서버 및 DB 등에 접근하는 경우
- 패스워드 관련 : 패스워드 잠김 임계치(실패 5회) 설정, 패스워드 암호화(SHA 2 적용), 패스워드 길이(9자 이상) 및 조합규칙(숫자, 문자, 특수문자 조합), 패스워드 변경 주기(분기별) 등
- 바이오 정보 : 바이오 정보의 종류(지문 등)

- 인증서 관련 : 사설인증서 허용 여부, 인증서 발급 방법, 인증서 유효성 검증 방법 등
- 접근 권한 : 동일사용자 동시접근 제한, 동일권한 동시접근 제한, 접근 IP 또는 MAC 제한
- 세션 관리 : 관리자 등 접근 후 관리활동을 수행하지 않는 경우 타임아웃 설정 등
- 추가적인 사용자 인증절차 : 중요한 시스템(예 : 개인정보처리시스템 등)의 경우 추가적인 인증(예 : OTP, 공인인증서 등) 요구

② 중요정보의 입·출력(저장 및 조회) 시 암호화가 요구되는 경우 법적 요구사항을 고려하여 중요정보에 대해 안전성이 입증된 알고리즘과 키 길이를 사용하여 암호화하여야 한다.

③ 개인정보 및 인증정보 등의 중요한 정보 전송 시 기밀성 및 무결성을 지원하는 안전한 채널을 통하여 송·수신하여야 한다.

제6조(보안로그 기능) ① 클라우드시스템 설계 시 보안관련 로그, 감사증적 등을 확보할 수 있는 기능을 반영하여야 한다.

- 사용자 및 관리자의 접속기록 (로그인 및 로그아웃)
- 사용자 권한 부여, 변경, 말소 기록
- 중요정보에 대한 접근 및 다운로드 기록
- 특수 권한으로의 접근 기록
- 주요 업무 관련 행위에 대한 로그 등

② 클라우드시스템 설계 시 보안로그의 비인가된 변조 및 삭제를 방지하기 위한 대책을 마련하여야 한다.

- 로그에 대한 접근통제
- 로그에 대한 무단변경 방지
- 이용자 또는 관리자라 하더라도 로그에 대한 변경이나 삭제를 할 수 없어야 함

③ 보안로그의 생성일시를 동기화하기 위하여 표준시각을 동기화하는 기능을 제공하여야 한다.

④ 감사기록 저장소의 한계를 초과하기 전에 관리자에게 경보를 보낼 수 있는 기능을 고려하여 설계하여야 한다.

⑤ 감사기록 저장소의 고갈로 인하여 감사증적이 유실되는 것을 차단할 수 있는 기능 또는 관리적 수단을 고려하여 설계하여야 한다.

제7조(접근권한 기능) ① 클라우드 시스템 설계 시 업무 성격, 프로세스, 보안 요구사항에 따라 다음과 같은 기준을 고려하여 접근권한 부여 기능을 구현하여야 한다.

- 사용자별

- 사용자 업무 역할별
- 기능별
- 메뉴별 등

② 클라우드 시스템에 접근이 가능한 사용자에 대하여 분류하여야 하고 각 사용자의 역할에 따라 접근범위, 접근 권한을 부여할 수 있도록 설계하여야 한다.

제8조(시각 동기화) ① 로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 클라우드 시스템 시각을 공식 표준시각으로 정확하게 동기화하고 주기적으로 점검하여야 한다.

② 공식적인 NTP 서버와의 연동이 불가능한 환경일 경우 내부망의 특정 서버를 타임 서버로 운영할 수도 있다.

제9조(구현) ① 시스템 및 어플리케이션에서 알려진 기술적 보안취약점으로 인한 위협을 최소화하기 위하여 안전한 코딩표준 및 규약을 마련하여야 하며, 이에 따라 클라우드 시스템을 구현하여야 한다.

- 사용자가 입력한 데이터의 유효성 확인 및 안전한 오류 처리
- SQL 삽입 방지
- 검증되지 않은 URL 리다이렉션 방지
- 안전한 세션 관리 등

② 코딩 완료 후 안전한 코딩표준 및 규약 준수 여부를 점검하고 기술적 보안 취약점이 존재하는지 확인하여 취약점 발견 시 재코딩을 하여야 한다.

- 시스템 및 어플리케이션이 안전한 코딩표준에 따라 구현하는지 소스코드 검증(소스코드 검증도구 활용 등)
- 코딩이 완료된 프로그램은 운영환경과 동일한 환경에서 취약점 점검도구 또는 모의진단을 통한 취약점 노출 여부를 점검

제10조(시험) ① 시스템 및 애플리케이션 구현 완료 후 사전 정의된 보안 요구사항을 충족하는지 확인하기 위하여, 시험 시나리오, 체크리스트 등을 작성하여 시험을 수행하여야 한다.

- 예상치 못한 입력에 대한 테스트
- 응용 프로그램의 반응 평가
- 변경 기능에 대한 테스트 수행

② 시험이 수행하기 위해 시험목적, 시험의 대상 기능, 시험환경(도구 포함), 시험절차 등이 포함된 시험계획을 수립하고, 시험계획에 따라 시험을 수행한 후 시험결과를 포함하여 문서로 기록하여야 한다.

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

④ 운영데이터를 시험 환경에서 불가피하게 사용할 경우 책임자 승인 등의 인가 후 제한된 환경에서 사용하여야 한다.

- 운영 데이터 사용 승인 절차 : 데이터 중요도에 따른 보고 및 승인체계 정의
- 시험용 운영 데이터 사용 기한 및 기한 만료 후 폐기 절차
- 중요 데이터 사용에 대한 시험 환경에서의 접근 권한 및 통제 수립
- 운영데이터 복제 및 사용에 대한 모니터링 및 감사

⑤ 시스템 및 어플리케이션이 활성화되기 전에 시험데이터(디버깅 코드 등)와 계정을 제거하여야 한다.

제11조(개발환경 분리 및 이관) ① 원칙적으로 개발/시험 환경과 운영환경은 분리되어야 한다.

② 개발/시험 환경과 운영환경을 분리하기 어려운 경우 다음 사항을 포함한 보안대책을 수립한 후 적용하여야 한다.

- 개발/시험으로 인하여 영향을 받는 부분에 대한 범위 산정
- 개발/시험의 오류로 인하여 발생할 수 있는 장애의 유형 및 복구 대책
- 장애 발생 시 대응을 위한 상세한 시험절차(입력 매개변수 등 포함) 수립
- 개발/시험 중 서비스 운영의 정상 여부를 지속적으로 모니터링하기 위한 대책
- 운영환경에서 개발/시험을 수행하기 전에 정보보호 책임자 등으로부터의 승인
- 운영데이터가 시험데이터로 사용되는 경우 운영데이터 보호를 위한 대책

③ 운영환경으로 이관 절차를 수립하고, 이에 따라 이행하여야 한다.

- 운영환경으로 이관을 수행하기 전에 시험 등을 통해 개발의 정확성 확인
- 이관 담당자 및 책임자 지정
- 이관이 완료된 이후 운영에 오류를 발생시키지 않는지 확인
- 주요한 변경이 적용되는 경우에는 정보보호최고책임자 승인 획득 후 작업 수행

제12조(소스코드 관리) ① 소스 프로그램(이하 “소스 코드”)의 변경(예 : 수정, 추가, 삭제 등)을 관리하고 소스 코드에 대한 접근통제를 수행하기 위한 절차를 수립하여야 한다.

② 소스 코드는 별도의 서버(형상관리 서버)에 보관하고 서버는 안전한 위치에 설치하여 운영하여야 하며, 서버에 대한 접근통제(인가된 담당자에게만 접근허용 등)를 수행하여야 한다.

③ 부득이한 경우를 제외하고 소스 코드는 운영환경과 구분된 내부망에 설치된 서버(형상관

리 서버)에 보관하여야 한다.

제13조(외주개발 보안) ① 시스템 개발을 위한 보안요구사항을 계약서에 명시하여야 한다.

- 내부에서 개발하는 경우 수립된 보안요구사항이 외주 위탁개발의 경우에도 적용될 수 있도록 다음의 사항이 계약서 내에 포함되어야 한다.

  · 설계, 구현, 시험에 대한 요구사항

  · 개발 환경에 대한 요구사항

  · 소스 코드 관리에 대한 요구사항

  · 코딩 표준 및 규약에 대한 요구사항

  · 개발 완료 후 수탁사로의 이관에 대한 요구사항

② 외주 위탁개발을 하는 경우 위탁사가 계약서에 명시된 요구사항을 준수하고 있는지에 대한 관리·감독을 수행하여야 한다.

- 기능적, 기술적 보안요구사항의 반영 여부
- 개발 보안가이드 준수 여부(시큐어 코딩 등)
- 테스트 시 보안요구사항 준수여부 확인 절차 포함 여부
- 개발 완료된 시스템에 대한 취약점 점검 등 수행 여부
- 개발인력 대상 SW개발 보안교육 여부

④ 클라우드 시스템 개발 완료 후 보안요구사항 반영 여부, SW 보안취약점 점검 및 보완 여부, 개발자 계정 및 권한 삭제 여부 등을 확인한 후 검수 또는 인수하여야 한다.

⑤ 외주개발을 수행하며 취득한 모든 내용은 누설하거나 공개하지 않도록 계약서에 명시 또는 보안서약서 징구 등 보안대책을 강구하여야 한다.

제3장 시스템 도입

제14조(시스템 도입 계획) ① 침입차단시스템 및 침입탐지시스템 등의 보안시스템 도입 계획 시에는 조직의 성격, 정책, 네트워크 형태, 시스템의 성능 및 안정성, 사용자 편의성, 관리자의 기술 운용 수준 등의 다양한 요소들을 고려하여야 한다.

- 현재 시스템 자원의 이용률, 사용량, 능력한계에 대한 분석
- 추가 자원의 필요성 및 시기에 대한 예상
- 성능, 안전성, 신뢰성, 보안성, 법규 등을 포함한 시스템 자원의 기능적, 운영적 요구사항
- 기존 시스템과의 호환성, 상호 운영성, 기술표준에 따른 확장성

② 시스템보안관리자는 도입 시 기술적인 보안성 검토를 할 수 있으며, 검토하여야 하는 사

항은 다음 각 호와 같다.

1. 기본 보안설정 이상의 보안 기능 제공 및 보장

2. 기밀성, 무결성 및 가용성 보장 확인

제15조 (시스템 도입 및 인수) ① 시스템 인수 여부를 판단하기 위하여 시스템의 기본 보안 설정 등이 반영된 인수 승인 기준을 수립하여야 한다. 또한 시스템 구매계약서 등에 반영하여 도입 과정에서 인수기준을 준수하도록 함으로써, 기본 보안 설정 미흡으로 발생할 수 있는 보안취약점을 최대한 제거한 후 인수할 수 있어야 한다.

② 시스템을 인수하기 전 사전 정의한 인수기준과의 적합성 여부를 테스트 등을 통해 확인한 후 인수여부를 결정하여야 한다.

③ 시스템보안관리자는 서버를 설치할 경우 준수하여야 하는 사항은 다음 각 호와 같다.

1. 설치 또는 변경되는 하드웨어 목록을 유지 및 관리하기 위하여 별지 제5호 서식 ‘시스템 이력카드‘를 작성하여 보유 현황 관리

2. 시스템는 물리적인 접근통제가 가능한 공간에 설치

3. 정확한 기록을 위해 시스템의 시각 동기화 및 로그 관리

④ 시스템에 소프트웨어를 설치할 경우에 준수하여야 하는 사항은 다음 각 호와 같다.

1. 시스템에 설치된 소프트웨어의 현황 작성 및 관리

2. 시스템에는 업무용 목적으로 사용되는 프로그램 이외의 불필요한 프로그램의 설치 금지

[별지 제1호 서식] 시험서(샘플 양식)

<table>
<tr><td colspan="2">시험항목</td><td colspan="2">시험 대상 보안 기능 서술(예: 관리자 로그인 기능)</td></tr>
<tr><td colspan="2">시험자</td><td colspan="2"></td></tr>
<tr><td colspan="2">시험목적</td><td colspan="2">관리자 로그 시 입력값 검증, 연속인증 실패 대응, 피드백 보호 등 확인</td></tr>
<tr><td colspan="4">시험환경 및 시험도구</td></tr>
<tr><td colspan="4">시험을 수행한 네트워크 환경 등 서술
시험에 사용된 시험 도구(도구의 버전까지 표시)</td></tr>
<tr><td>단계</td><td colspan="3">시험절차</td></tr>
<tr><td>1</td><td colspan="3">시험절차는 반복이 가능하도록 상세하게 서술</td></tr>
<tr><td>2</td><td colspan="3"></td></tr>
<tr><td>3</td><td colspan="3"></td></tr>
<tr><td>4</td><td colspan="3"></td></tr>
<tr><td>5</td><td colspan="3"></td></tr>
<tr><td colspan="4">시험결과</td></tr>
<tr><td rowspan="2">1 차
시험</td><td>시험일</td><td colspan="2"></td></tr>
<tr><td>시험결과</td><td colspan="2">시험결과가 시험목적에 맞는지 명확히 서술</td></tr>
<tr><td rowspan="2">2 차
시험</td><td>시험일</td><td colspan="2"></td></tr>
<tr><td>시험결과</td><td colspan="2"></td></tr>
</table>

[별지 제2호 서식] 시험데이터 사용 요청서(샘플 양식)

시험데이터 사용 요청서

확인	정보보호담당자	정보보호관리자

작성일 : 년 월 일

신청인 정보	소속 구분	□ 내부자 □ 외부자	관리담당자 (외부자 경우)	
	소속		직급	
	성명	(서명)	연락처	

시험데이터 사용 정보	사용 목적			
	요청 데이터 상세			
	개인정보 항목			
	관리방안			
	사용 기간		폐기 예정일	

[별지 제3호 서식] 검수확인서(샘플 양식)

검수확인서

위 탁 명			
계약번호			
착수일자		완료일자	

1. 위탁사업 내용

2. 위탁개발 내역

클라우드서비스	기 능 점 검		부적합 시 내용
	적 합	부 적 합	
업무 분석단계			
업무 설계단계			
S/W 개발단계			
테스트 단계			

3. 검수자 종합의견

수탁기관과 체결한 계약에 의거하여 추진한 클라우드서비스 시스템 개발이 완료되었으며, 시스템 및 최종 산출물을 검수한 결과 이상이 없음을 확인합니다.

2019 년 월 일

검 수 자 : (서명)

[별지 제4호 서식] 보안서약서(샘플 양식)

보 안 서 약 서

본인은 ___년 ___월 ___일부로 _____관련 용역사업(업무)을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 _____관련 업무 중 알게 될 일체의 내용이 직무상 기밀 사항임을 인정한다.
2. 본인은 이 기밀을 누설함이 ㈜클라우드에 위해가 될 수 있음을 인식하여 업무수행 중 습득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.
3. 본인이 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다.
4. 본인은 하도급업체를 통한 사업 수행 시 하도급업체로 인해 발생하는 위반사항에 대하여 모든 책임을 부담한다.

년 월 일

서 약 자 업 체 명 :
(업체 대표) 직 위 :
성 명 : (서명)

서약집행자 소 속 :
(담당 직원) 직 위 :
성 명 : (서명)

[별지 제5호 서식] 시스템 이력카드

시스템 이력카드

관리번호			장비명	
구입일자			제조사	
규 격	CPU			
	MEMORY			
	HDD			
	OS			
분야/용도				
교정주기				
설치일자				
설치장소				
특이사항				
수리 및 교정 이력	일자	내역		비고