㈜클라우드 네트워크보안관리지침은 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
네트워크 보안관리지침

2019. 01. 01

㈜클라우드

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

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

제1장 총칙

제1조(목적) 이 지침은 ㈜클라우드의 「정보보호정책서」에 의거 구성원의 네트워크 보안관리에 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. “내부 네트워크”라 함은 외부에서 직접 접근이 불가능한 네트워크 영역으로 내부IP체계에 따라 운영되는 네트워크 영역을 말한다.
2. “네트워크시스템”이라 함은 유 무선 네트워크 서비스 제공을 위해 사용되는 시스템을 말한다.
3. “네트워크보안관리자“라 함은 네트워크 관리 업무를 총괄하는 자를 말한다.

제2장 네트워크 보안

제4조(네트워크 보안 정책 수립) ① 내·외부 네트워크를 통한 클라우드시스템의 접근을 통제하는 정책을 수립하여야 한다.

② 내부 네트워크를 통해 클라우드시스템을 운영하거나 관리자 페이지에 접속하는 경우, 관리자는 지정된 단말을 통해서만 접근할 수 있도록 통제하여야 한다.

③ 외부 네트워크(인터넷 등)를 통한 정보시스템 원격운영은 원칙적으로 금지하여야 하며 긴급 장애 대응, 유지보수 등과 같이 부득이한 경우 다음과 같은 보안대책을 마련하여야 한다.

- 원격운영에 대한 정보보호 책임자 승인절차
- 접속 단말 및 사용자 인증절차
  (ID/PW 외 강화된 인증방식(공인인증서, OTP 등) 적용 권고. 법적 요구사항 의무적 반영)
- 한시적 접근권한 부여 : VPN 계정, 시스템 접근권한 등
- VPN 등의 전송구간 암호화
- 백신 설치, 보안패치 적용 등 접속 단말 보안
- 원격운영 현황 지속적인 모니터링
- 원격접속 기록 로깅 및 주기적 분석
- 원격운영 관련 보안교육 등

④ 스마트기기(스마트 패드, 스마트폰 등)를 통한 클라우드시스템 원격운영은 원칙적으로 금지하여야 한다. 다만 부득이한 경우 스마트기기에 대한 보안대책을 마련하고 책임자의 승

인 후 사용하여야 한다.

⑤ 네트워크 장비 등 신규 전산장비 도입 시 기본(default)계정을 삭제 또는 변경하고 시스템 운영을 위한 관리자 계정 별도 생성하여야 한다.

제5조(네트워크 모니터링 및 통제) ① DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요 정보 유출 등을 막기 위해 네트워크를 모니터링하고 통제하여야 한다.

② 내부 네트워크를 구성하는 주요자산 목록, 구성도, IP 현황을 최신으로 유지하고 대외비 이상으로 안전하게 관리하여야 한다.

③ 내부망의 주소 체계는 사설 IP주소 체계를 사용하고, 내부 주소체계를 외부에 유출되지 않도록 하여야 하며, 외부 네트워크와의 연결지점에 NAT(Network Address Translation) 기능을 적용하여야 한다.

④ 사설 IP 주소를 할당하는 경우 국제표준에 따른 사설IP 주소대역을 사용하여야 한다.

⑤ DDoS, 비인가 접속 등의 서비스 중단 및 중요 정보 유출 등을 예방하기 위해 네트워크 모니터링 방안을 수립하고 이행하여야 한다.

제6조(네트워크 정보보호시스템 운영) ① 정보보호시스템은 정보통신망을 통하여 수집•저장•검색 및 송•수신되는 정보의 훼손•변조 •유출 등을 방지하기 위한 장치로서 침입차단시스템(FW), 침입탐지시스템(IDS), 침입방지시스템(IPS), 웹방화벽, DB 접근통제시스템, 내부정보유출방지시스템(DLP), 가상사설망(VPN), 패치관리시스템(PMS) 등을 포함하여야 한다.

② 외부침입 탐지 및 차단, 내외부자에 의한 정보유출 방지 등을 위하여 도입•운영하고 있는 보안시스템에 대한 운영절차를 수립하여야 한다.

- 정보보호시스템 유형별 책임자 및 관리자 지정
- 정보보호시스템 정책(룰셋 등) 적용(등록, 변경, 삭제 등) 절차
- 최신 정책 업데이트
- 정보보호시스템 이벤트 모니터링 절차
- 정보보호시스템 접근통제 정책
- 정보보호시스템 운영현황 주기적 점검 등

③ 정보보호시스템 관리자 등 접근이 허용된 인원을 최소화하고 비인가자 접근을 엄격하게 통제하여야 한다.

④ 정보보호시스템별 정책(룰셋 등) 신규 등록, 변경, 삭제 등 절차를 수립하고 정책의 타당성 검토를 주기적으로 수행하여야 한다.

⑤ 주기적인 보안시스템 접속로그 분석, 정책 타당성 검증을 통해 비인가자에 의한 접근시도 등 위협, 정책의 타당성을 확인하고 적절한 조치를 하여야 한다.

제7조(네트워크시스템 운영관리) ① 네트워크보안관리자는 네트워크시스템을 신규 설치 변경한 후 별지 제1호 서식 ‘네트워크시스템 이력 관리대장’을 작성하여 변경사항을 기록, 유지한다.

② 네트워크보안관리자는 네트워크시스템의 구성 정보 등의 변경은 다음 각 호에 따른다.

1. 네트워크시스템 변경을 위한 작업계획 수립 및 보고
2. 필요시 관련 업무 담당자에게 문서 발송
3. 작업수행 및 검증 테스트
4. 완료보고서 작성 및 보고

③ 네트워크시스템 구성 정보는 장애 등에 대비하기 위하여 백업을 하여야 한다.

④ 부서별보안담당자는 유·무선 네트워크 장비(공유기, 무선 AP 등)의 추가 설치 및 실습실 네트워크 구성 변경 등이 필요한 경우에는 정보보호관리자와 사전 협의를 하여야 한다.

⑤ 부서별보안담당관은 연구실, 실습실 등에서 IP 주소가 추가로 필요한 경우에는 정보보호관리자와 사전 협의를 하여야 하며, 사전 협의 대상은 다음 각 호와 같다.

1. 독자적으로 IP 주소, 도메인 사용이 필요한 경우
2. 대량으로 IP 주소 할당이 필요한 경우
3. 많은 트래픽 발생이 예상되는 경우
4. 서비스의 추가 또는 변경 등이 필요한 경우

⑥ 정보보호관리자는 사전 협의 없이 교내 네트워크 서비스에 영향을 주는 경우 네트워크 사용을 제한할 수 있다.

⑦ 무선네트워크 환경을 구축(AP 설치)할 경우 허가(승인), 보안성 검토 등 절차를 마련하고 구축에 따른 (주요) 보호대책을 적용하여야 한다.

⑧ 외부인에게 제공하는 무선네트워크를 내부네트워크(업무망)와 분리하여야 한다.

제8조(네트워크시스템 주소관리) ① 모든 네트워크사용자는 자동으로 부여된 IP 주소를 사용한다. 다만, 고정 IP 주소가 필요한 경우는 정보보호관리자의 승인을 득하여야 한다.

② 네트워크보안관리자는 네트워크시스템에서 사용하는 IP 주소를 체계적으로 관리하여야 한다.

③ 네트워크보안관리자는 IP 주소 및 환경정보, 구성도 등은 외부로 유출되지 않도록 대외비로 관리한다.

제9조(네트워크시스템 접근관리) ① 네트워크보안관리자는 별지 제2호 서식 ‘네트워크시스템 계정 및 비밀번호 관리대장’을 유지하고 주기적으로 계정, 비밀번호 및 권한에 대한 현황을 점검하여야 한다.

② 네트워크보안관리자는 최소한의 계정만을 생성하여 제한된 사용자만이 사용하도록 하여야 한다.

③ 네트워크시스템에 설치 시 기본적으로 생성되는 불필요한 계정을 삭제하고, 해당 계정이 필요한 경우 비밀번호를 변경하여 사용하여야 한다. 다만, 해당 기능이 없는 장비인 경우는 제외한다.

④ 네트워크시스템의 관리자 계정 접속은 콘솔포트 및 특정 PC에서만 접근 가능하도록 설정한다. 다만, 해당 네트워크시스템에 접속 제한 기능이 없는 경우는 별도의 보안대책을 강구한다.

⑤ 네트워크시스템의 비밀번호 및 인증에 관한 사항은「응용프로그램보안관리지침」으로 따로 정한다.

제10조(네트워크시스템 보안관리) ① 네트워크보안관리자는 네트워크시스템 운용을 위하여 적용할 보안조치 사항은 다음 각 호와 같다.

1. 네트워크시스템에 대한 원격접속은 원칙적으로 금지하며, 불가피한 경우 장비 관리용 목적으로 내부 특정 IP·MAC 주소에서의 접속은 허용
2. 물리적으로 안전한 장소에 설치하여 비인가자의 무단 접근통제
3. 최초 설치 시 보안취약점을 점검하여 제거하고 주기적으로 보안패치 실시
4. 불필요한 서비스 포트 제거

② 클라우드컴퓨팅서비스 제공자의 관리 영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리하여야 한다.

제11조(네트워크시스템 보안설정) ① 클라우드 시스템에서 중요정보가 이동하는 구간에 대해서는 VPN 등 암호화된 통신 채널을 사용하여야 한다.

② 네트워크시스템은 관리자 계정외의 별도 계정 생성을 금지한다.

③ 네트워크시스템은 각 모드별로 암호를 설정하여 필요 이상의 권한을 차단하여야 한다.

④ 유무선 네트워크시스템을 설치한 후, IP별 접근제어 정책을 적용하여 네트워크사용자가 네트워크시스템에 접근할 수 없도록 보안 설정을 적용한다.

⑤ 네트워크시스템의 SNMP(Simple Network Management Protocol)는 다음 각 호와 같이 설정하여야 한다.

1. 기본 Community 문자열(Public)을 사용하지 않음을 원칙으로 한다.
2. 읽기권한(Read Only)만을 허용한다. 필요시 정보보호관리자의 승인 후에 RW(Read Write) community를 한시적으로 설정하여 사용하고 SNMP 정보는 해당 부서에서만 볼 수 있도록 한다.

⑥ 네트워크시스템의 다음 각 호와 같이 불필요한 서비스는 Disable 한다.

1. Small-servers
2. echo
3. disable
4. daytime

⑦ 네트워크보안관리자는 무선랜을 사용하는 경우 무선 중계기(AP)와 관련하여 자체 보안대책 수립 시 다음 각 호의 사항을 포함하여야 한다.

1. 네트워크이름(SSID: Service Set IDentifier) 브로드캐스팅 중지
2. 추측이 어려운 복잡한 SSID 사용
3. WPA2이상의 암호체계를 사용하여 자료 암호화
4. MAC 주소 및 IP 필터링 설정
5. RADIUS(Remote Authentication Dial-In User Service) 인증 사용

제12조(네트워크시스템 보안패치관리) ① 새로운 취약성에 대한 보안패치가 발표되면 해당 네트워크시스템의 보안사고 예방을 위한 보안조치 사항은 다음 각 호와 같다.

1. 보안패치 정보를 주기적으로 확인하여 적용한다.
2. 주요 보안패치에 대해서는 적용일 등 패치정보를 별지 제3호 서식 ‘네트워크시스템 보안패치 관리대장’을 작성하여 관리한다.

② 패치적용 대상 네트워크시스템 별로 보안패치 방법 및 절차는 다음 각 호와 같다.

1. 네트워크시스템 성능 및 환경의 문제로 패치를 못하는 경우에는 해당 사유와 이를 보완하기 위해 적용한 대체수단이나 방법을 기록한다.
2. 패치는 업무시간 종료 이후에 적용함을 원칙으로 한다.
3. 테스트 장비가 존재할 경우에는 테스트 장비에서 먼저 패치를 적용하여 이상 여부를 확인한 후 운영 장비에 적용한다.
4. 다수의 장비에 동시 적용하는 경우 1개의 장비에 먼저 패치를 적용하여 안정성을 확인한 후 나머지 장비에 확대 적용한다.
5. 네트워크시스템의 보안패치 적용은 일정을 수립하여 패치를 적용한다.
6. 패치 적용 후 네트워크시스템이 정상작동 되는지에 대해 테스트를 수행하고, 장애발생 시 원상 복구한다.

제13조(네트워크시스템 유지관리) ① 네트워크보안관리자는 유 무선 네트워크시스템의 가용성을 보장하기 위해 유지보수 업체에 예방점검을 요청하여 정기점검을 실시하여야 한다.

② 네트워크보안관리자는 네트워크시스템의 안정적인 운용을 위해 최신 운영체제 중 가장 안전한 버전을 사용하여야 하며, 새로운 운영체제 적용 시에는 모든 보안취약점을 제거하

여야 한다.

③ 유지보수 수행 과정에서 네트워크시스템 정보가 유지보수 인력에 의해 유출되지 않도록 조치하여야 한다.

제14조(네트워크 모니터링)

① 네트워크보안관리자는 분기별로 네트워크시스템의 사용량에 대해서 검토하고, 특이사항이 있을 경우 정보보호관리자에게 보고한다.

② 네트워크시스템에 대한 최적의 용량 확보, 용량부족으로 인한 서비스 지연, 장애 등을 방지하기 위하여 수행하여야 하는 사항은 다음 각 호와 같다.

1. 네트워크시스템 자원에 대한 이용도 분석 및 응답시간 지연 시 원인분석

2. 네트워크시스템의 사용현황 파악 및 추이분석을 통한 네트워크시스템의 가용성 확보

③ 네트워크 모니터링을 위한 담당자를 지정하고 24시간 네트워크 이상유무를 점검할 수 있는 체계를 갖추어야 한다.

[별지 제1호 서식]네트워크시스템 이력 관리대장

네트워크시스템 이력 관리대장

no	장비명	용도	IP	설치위치	작업내용	작업일	작업자

[별지 제2호 서식]네트워크시스템 계정 및 비밀번호 관리대장

네트워크시스템 계정 및 비밀번호 관리대장

no	장비명	용도	IP	설치 위치	관리자명	ID	password	제조사	비고

[별지 제3호 서식]네트워크시스템 보안패치 관리대장

네트워크시스템 보안패치 관리대장

no	장비명	용도	IP	설치 위치	관리자명	패치내역	패치일	비고