㈜클라우드 침해사고관리지침은 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
물리적 보안지침

2019. 01. 01

㈜클라우드

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

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

제1장 총 칙

제1조(목적) 이 지침은 ㈜클라우드의 「정보보호정책서」에 의거 정보통신설비 및 시설 등에 대해 물리적보안 관리에 필요한 사항을 규정함을 목적으로 한다.

제2조(적용범위) 본 지침은 회사의 안전 유지에 필요한 사항을 규정하고, 회사의 시설 및 정보통신설비에 접근권한을 가진 임직원과 협력업체에 적용한다.

제3조(용어의 정의) 본 지침에서 사용하는 용어의 정의는 다음 각 호와 같다.

① "보호구역"이라 함은 비밀 또는 중요시설에 대한 비인가자의 접근을 방지하기 위하여 그 출입에 안내가 요구되는 물리적 경계 내의 모든 영역을 말한다. (예: 사무실 등)

② "일반구역"이라 함은 보호구역 내 통제구역 및 제한구역을 제외한 전 구역을 말한다.

③ "제한구역"이라 함은 회사 내부에 외부자의 접근을 방지하기 위해 설정된 장소로서 출입의 안내가 요구되는 지역을 의미하며, 일반구역을 제외한 회사 전체구역이 이에 해당된다.

④ "통제구역"이라 함은 서버 등 정보시스템 및 통신장비와 같이 중요시설물 및 기밀자료 등을 운용하거나 보관하는 곳을 말하며, 비인가자의 출입이 금지되는 보안상 극히 중요한 구역을 말한다. (예: 전산실, 문서고 등)

⑤ "출입통제시스템"이라 함은 보호구역에 대한 출입을 통제하기 위한 시스템으로 개인별 출입통제 기능과 출입에 대한 로그 기록 및 이에 대한 검색기능을 제공한다. 개인에 대한 인식은 지문 등의 생체정보나 카드 등을 사용한다. 이 지침에서는 별도의 언급이 없는 경우 카드를 사용하는 출입통제시스템을 의미한다.

⑥ "휴대용저장매체"라 함은 디스켓(FD), 이동형 하드디스크(HDD), USB 메모리, Flash 메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 또는 IC칩 등에 정보를 저장할 수 있는 모든 것으로 정보통신망과 분리할 수 있는 기억장치를 말한다.

제4조(책임 및 역할) ① 정보보호책임자의 역할은 다음 각 호와 같다.

1. 보호구역의 지정 및 해제
2. 통제구역 출입권한에 대한 최종 승인

② 물리적 보안담당자의 역할은 다음 각 호와 같다.

1. 보호구역에 대한 출입통제 설비 설치
2. 제한구역 출입자에 대한 ID카드 발급, 변경, 삭제 관리
3. 제한기록 출입기록 유지
4. 공용 사무기기 관리

③ 정보보호담당자의 역할은 다음 각 호와 같다.

1. 전산실 출입설비에 대한 관리
2. 전산실 출입자에 대한 출입권한 등록, 변경, 삭제 관리
3. 전산실 출입기록 유지 및 검토

제2장 보호구역 지정 및 관리

제5조(물리적 보호구역의 구분) ① 중요 정보 및 정보처리시설을 보호하기 위한 물리적 보안 구역(예 : 주요 정보처리 설비 및 시스템 구역, 사무실, 외부인 접견실 등)을 지정하고, 각 보안 구역에 대한 보안 대책을 마련하여야 하며, 각 구역에 대한 의미는 다음의 각 호와 같다.

1. 일반구역 : 통제구역과 제한구역을 제외한 회사 내 모든 구역(예 : 접견구역, 회의실 등)
2. 제한구역 : 비 인가자의 불필요한 접근을 방지하기 위하여 출입통제가 필요한 구역(예 : 사무실 등)
3. 통제구역 : 인가 받은 자 이외의 불필요한 인원의 출입이 금지되는 구역(예 : 전산실, 통신장비실, 관제실, 전원실 등)

제6조(물리적 보호구역의 통제 방안) ① 일반구역의 출입통제는 다음 각 호와 같이 운영한다.

1. 업무 및 그 외 목적으로 방문하는 외부인의 경우에는 일반구역으로 지정된 장소에만 출입할 수 있다.

② 제한구역의 출입통제는 다음 각 호와 같이 운영한다.

1. 비 인가자의 출입을 통제하기 위해 출입통제시스템 등을 설치 및 운영한다.
2. 출입통제를 위해 ID카드 등의 출입통제 장치를 설치 운영한다.
3. 퇴직, 전환배치 등으로 접근권한이 변경된 임직원에 대한 불필요한 접근권한을 지체 없이 해제한다.
4. 제한구역으로 반출입 되는 가방, 서류, 기타 휴대용 전산 장비 등은 필요 시 검색할 수 있다.
5. 외주업체 직원의 제한 구역 내 출입은 업무상 필요에 따라 결정되어야 하며, 제한 구역 내 장기간 출입할 경우, 담당 직원에 의해 이들의 활동을 지속적으로 감독한다.

③ 통제구역의 출입통제는 다음 각 호와 같이 운영한다.

1. 최소한의 인가된 인원들에 대해서만 출입이 통제되고 출입통제시스템과 CCTV 등을 설치 및 운영한다.
2. 통제구역에 상시로 출입하는 인원은 정보보호 최고책임자의 승인을 받은 인원으로 제한한다. 그 외의 외부인력 등이 통제구역에 출입하기 위해서는 정보보호 최고책임자의 별도 승인을 받고 담당자의 인도하에 통제구역에 출입한다.

제7조(출입권한 통제) ① 제한구역 및 통제구역에 대해 출입이 필요한 직원은 출입권한 신청서를 작성하여 해당 부서(팀)장의 승인을 득한 후 물리적 보안담당자에게 신청하여야 한다.

② 물리적 보안담당자는 출입권한의 적정성을 판단하여 출입관리시스템에 등록한다.

③ 물리적 보안담당자는 분기 1회 이상 등록된 출입권한에 대해 적정성을 검토한 후 출입권한 검토 결과서를 작성하여 정보보호책임자에게 보고하여야 한다.

④ 통제구역 중 전산실에 대한 출입신청 및 출입권한 검토는 본 지침 제3장 전산실 보안에서 정한다.

⑤ 관련 서식은 “(별지 제1호 서식)” 출입권한신청서, “(별지 제2호 서식)출입권한 검토”를 참조한다.

제8조(물리적 보호구역 내 작업) ① 클라우드시스템 도입, 유지보수 등으로 보호구역 내 작업이 필요한 경우 작업신청 및 수행 관련 절차를 수립하고 작업기록을 주기적으로 검토하여야 한다.

② 클라우드시스템이 위치한 통제구역 내 모바일기기(노트북, 스마트기기 등) 사용 방지 및 불법적인 활동을 모니터링(예: CCTV) 하기위한 대책을 마련하고 불가피하게 사용해야 하는 경우 책임자의 사전 승인 및 보안성 검토 등 적법한 절차를 수행한 후 사용하여야 한다.

제9조(사무실 등 내부 시설 보호) ① 공용으로 사용하는 사무장비 및 시설에 대한 보호대책을 수립•이행하고 관리자를 지정하여 준수여부를 주기적으로 검토하여야 한다.

② 공공장소 및 기타 외부시설은 내부 시설로부터 분리하여 통제 및 관리하여야 한다.

③ 미승인 기기(노트북 등 모바일 기기)의 반출입을 통한 중요정보 유출, 내부망 악성코드 감염 등의 보안사고 예방을 위하여 보호구역 내 임직원 및 외부인력 모바일 기기 반출입 통제절차를 수립하고 기록・관리하여야 한다.

제10조(정보처리시설의 배치) ① 클라우드시스템의 특성을 고려하여 배치 장소를 분리하여야 한다.

② 실제 물리적 위치를 손쉽게 확인할 수 있는 방안(배치도, 자산목록 등)을 마련하여야 한다.

제11조(보호설비) ① 각 보호구역의 중요도 및 특성에 따라 화재, 전력 이상 등 인재 및 자연재해 등에 대비하여 필요한 설비를 갖추고 운영절차를 수립•관리하여야 하며, 지속적으로 점검하여야 한다.

② 재해(화재 등) 발생 시 임직원이 대피절차에 따라 안전하게 대피할 수 있도록 비상벨, 비상등, 비상통로 안내표지 등을 설치•운영하여야 한다.

③ 주요 정보시스템을 외부 집적정보통신시설(IDC)에 위탁 운영하는 경우, 물리적 보호에 필요한 요구사항을 계약서에 반영하고 운영상태를 주기적으로 검토하여야 한다.

④ 시설 및 장비의 가용성 및 무결성 보장하기 위해 지속적으로 유지보수를 수행하여야 한다.

제3장 전산실 보안

제12조(전산실 관리) ① 중요 정보시스템이 위치한 전산실의 보호를 위해 다음 각 호와 같은 시설 및 설비를 갖추어야 한다.

1. 방수, 방화, 방진, 도청 및 외부 침입 방지 등 전산실 요건에 맞도록 시설을 구비한다.
2. 상시 출입문은 한 곳으로 정하고 출입문은 이중 안전장치로 보호하여야 하며, 외벽이 유리인 경우 유리창문을 통한 접근이 가능하지 않도록 보호대책을 강구하여야 한다.
3. 화재발생 시 조기 진압을 위한 소화기 및 자동소화 설비 등을 설치・운영한다
4. 자동으로 항온・항습을 유지할 수 있는 설비를 설치・운영한다.
5. 전산실의 출입사항은 무인 감시카메라 및 출입통제시스템에 의해 사후확인이 가능하도록 하며 그 기록을 1년 이상 보관하여야 한다.
6. 정보통신・설비 및 시설 목록은 항상 최신의 자료를 유지한다.

② 전산실 담당자는 분기 1회 이상 점검을 실시하고 그 결과를 정보보호 책임자에게 보고하여야 한다.

③ 관련 서식은 “(별지 제6호 서식)보호설비점검”을 참조한다.

제13조(전산실 내 정보시스템의 보호) ① 정보시스템은 환경상의 위협을 최소화할 수 있도록 가능한 건물 외벽과 거리를 두고 배치하고, 가능한 취사시설, 화장실 등으로부터 거리를 두고 배치한다.

② 일시적인 전력중단이나 기타 전기적 이상으로부터 정보시스템의 가용성을 확보할 수 있도록 비상 발전기, UPS 등 대체 전력 공급원을 확보하여야 한다.

② 지속적인 서비스 지원을 위해 전력공급 및 정보 전달을 위한 케이블은 물리적인 차단이나 손상으로부터 보호한다.

③ 데이터를 송수신하는 통신 케이블이나 전력을 공급하는 케이블은 손상이나 도청으로부터 보호하여야 한다.

④ 전산실 내에는 무선통신망을 설치하지 않아야 한다.

⑤ 정보시스템별 유지보수 내역과 의심되는 결함은 기록・관리한다.

제14조(전산실 출입통제) ① 전산실 상시 출입권한은 업무상 필요한 최소한의 인원에게만 부여하여야 한다.

② 전산실 상시 출입권한이 필요한 임직원은 “전산실 출입권한 신청서”를 작성하여 정보보호담당자에게 신청한다.

③ 정보보호담당자는 신청한 출입권한의 적정성을 검토 후 정보보호책임자의 최종 승인 후 출입권한을 부여한다.

④ 정보보호담당자는 월 1회 이상 전산실 출입권한 현황과 출입기록 내역을 검토하여 그 결과를 정보보호책임자에게 보고하여야 한다.

⑤ 상시 출입권한이 없는 임직원 및 외부인원이 업무상 필요에 의하여 전산실에 출입하여야 하는 경우 사전에 정보보호책임자의 승인 후 출입이 이루어지도록 하고 출입일시, 출입목적 등을 출입관리대장에 기록 보관하여야 한다.

⑥ 전 항의 경우 비인가자의 출입 시에는 관련 담당자가 반드시 동행하여 업무를 수행하여야 한다.

⑦ 관련 서식은 “(별지 제1호 서식)” 출입권한신청서, “(별지 제2호 서식)출입권한 검토”를 참조한다.

제15조(전산실 작업) ① 전산실 내에서의 작업을 24시간 모니터링할 수 있도록 CCTV를 설치하고 녹화기록을 잠금 장치가 설치된 안전한 장소에 3개월 이상 보관하여야 한다.

② 정보보호담당자는 CCTV 녹화 기록을 검토하여 이상 유무를 분기 1회 이상 정보보호책임자에게 보고한다.

③ 정보보호담당자는 필요할 경우 CCTV 녹화기록과 출입대장을 비교하여 검토 결과를 정보보호책임자에게 보고한다.

④ 정보보호담당자는 외부인력 등 출입권한이 없는 자가 전산실 내에서 작업하고자 할 경우 항상 동행하여야 한다.

⑤ 전산실 내에서 정보시스템 도입 및 폐기 등 중요한 작업을 수행하는 경우 작업계획서를 작성하여 정보보호책임자에게 보고하고, 작업 완료 후 결과보고서를 작성하여 정보보호책임자에게 보고하여야 한다.

제4장 휴대용 저장매체 및 사무기기 보안

제16조(휴대용 저장매체의 관리) ① 휴대용 저장매체는 회사에서 인가한 저장매체만을 사용하여야 한다.

② 정보보호담당자는 사내에서 사용하는 휴대용 저장매체의 현황을 최신화하여 기록·관리하여야 하며, 인가되지 않은 휴대용 저장매체의 사용 차단, 모니터링 등의 기술적 보호대책을 강구하여야 한다.

③ 휴대용 저장매체를 통해 바이러스, 악성코드가 유포되지 않도록 휴대용 저장매체가 연결되는 단말기에 다음과 같은 대책을 적용하고 주기적으로 점검하여야 한다.

1. 자동실행 기능 해지

2. 바이러스 및 악성코드 사전(자동) 검사

3. 숨김파일 및 폴더 등이 표시되도록 PC 등 단말기 옵션 변경 등

④ 조직의 중요정보(개인정보, 기밀정보 등)의 경우 휴대용 저장매체 저장을 제한하고 업무상 저장이 필요한 경우에는 암호화 등의 보호대책을 마련하여 매체 분실, 도난 등에 따른 중요정보 유출을 방지하여야 한다.

제17조(사무기기 보안) ① 공용 프린터를 이용하여 출력하고자 하는 경우 다음 각 호의 사항을 준수하여야 한다.

1. 출력되는 문서는 즉시 회수

2. 불필요한 출력을 최소화하고 필요한 자료만 출력

3. 프린터 내 프린트 된 문서가 저장되는 경우 정보가 유출되지 않도록 주기적 점검 및 관리

② 전 항의 경우 정보보호담당자는 중요문서 출력 시 관련 정보(출력자, 출력일시 등)가 표시되도록 프린터의 워터마킹 기능을 적용할 수 있다.

③ 복사기를 이용하여 문서를 복사하는 경우 다음 각 호의 사항을 준수한다.

1. 업무상 필요한 최소한의 부수만 복사

2. 복사 후 원본 및 복사본이 복사기에 남겨져 있지 않도록 관리

3. 복사기 내 복사한 문서가 저장되는 경우 정보가 유출되지 않도록 주기적 점검 및 관리

④ 팩스를 통한 송・수신 시에는 다음 각호의 사항을 준수한다.

1. 악의적인 용도나 불순한 목적으로 사용금지

2. 문서 생성자가 직접 팩스를 전송하고 전송되는 원본 문서는 즉시 회수

3. 팩스 내 전송한 문서가 저장되는 경우 정보가 유출되지 않도록 주기적 점검 및 관리

⑤ 공용 PC 사용

1. 일정 시간 미사용 시 화면 보호 기능을 사용하며 모니터링 등 연속적으로 사용하여야 하는 PC는 예외

2. 로그인 시 암호 설정

3. 개인별 계정을 사용하고 공용 계정을 사용 시 승인 후 사용

4. 패스워드를 주기적으로 변경

5. 중요 정보를 저장하지 않도록 주의

⑥ 파일서버

1. 부서별, 업무별 디렉토리 접근 권한을 부여

2. 불필요한 정보가 공개되지 않도록 주의

3. 기타 공용 PC의 보안대책 적용

제5장 정보자산 반출・입 관리

제18조(장비 반출•입 및 폐기) ① 보호구역 내 중요한 장비, 문서, 매체 등에 대한 반출입 관련 정책 및 절차를 수립•이행하여야 한다.

② 장비 폐기에 대한 절차를 수립•이행해야 하며, 폐기 및 재사용 시 정보가 복구되지 않도록 처리하여야 한다.

③ 자체적으로 저장매체를 폐기할 경우 관리대장을 통해 폐기 이력을 남기고 폐기확인 증적을 함께 보관하여야 한다.

④ 외부업체를 통해 저장매체를 폐기할 경우 폐기 절차를 계약서에 명시하고 완전한 폐기에 대한 확인하여야 한다.

제19조(정보자산 반출・입 관리) 미승인 반출•입을 통한 중요정보 유출, 악성코드 감염 등의 침해사고 예방을 위하여, 보안 구역 내 직원 및 외부 업무 관련자에 의한 장비 반출•입 절차, 절차를 수립하고, 기록 및 관리하여야 한다.

① 정보자산에 대해 사전 승인 없이 외부 반출을 금지한다. 다만, 업무상 반출이 필요한 경우에는 해당 부서장의 사전 승인 후 반출하여야 한다.

② 전산실 내에 반입 및 반출되는 모든 정보자산은 사전에 정보보호책임자의 승인을 득한 후 반출・입이 이루어지도록 한다.

③ 통제구역에서의 정보자산 반출 시 정보자산 반출신청서에 반출 자산명, 반출목적, 반출지, 재반입 예정일 등을 기록하여 정보보호책임자의 승인 후 반출하여야 한다.

④ 통제구역 내에 전산 단말, 휴대용 저장매체 등의 반입은 원칙적으로 금지한다. 다만, 업무상 부득이하게 반입하여야 하는 경우에는 정보보호책임자의 승인을 받아야 한다.

⑤ 관련 서식은 “(별지 제3호 서식) 자산 반출입 신청서”, “(별지 제4호 서식) 자산반출/입 관리대장”을 참조한다.

제20조(장비 폐기) 장비 또는 저장매체를 폐기하고자 하는 경우에는 정보보호책임자의 사전 승인 하에 폐기하여야 하며, 폐기처리 시에는 다음 각 항의 사항을 준수하여 폐기 처리한다.

① 중요한 정보를 담고 있는 저장장치는 물리적으로 파괴하거나 저장된 정보가 완전하게 제거 될 수 있는 방법을 사용한다.

② 저장매체를 포함하고 있는 모든 종류의 장비는 폐기되기 전에 데이터가 삭제되었는지 확인한다.

③ 전 항에 해당하는 장비를 폐기하는 경우 반드시 폐기에 대한 증적을 기록(폐기이력, 사진 등)으로 유지하고, 정보보호 책임자에게 보고하여야 한다.

④ 자체적으로 불가능한 경우 전문 파기 업체와의 계약을 통하여 파기를 실시할 수 있다. 이

경우 파기 업체와의 계약은 『인적보안지침』에서 정하는 용역사업에 대한 보안관리가 이루어지도록 하여야 하고 파기를 수행한 증명 자료는 관리 부서장이 수령, 보관하여야 한다.

⑤ 장비 및 저장매체에 대한 폐기기록은 (별지 제5호 서식) 자산폐기관리대장을 참조한다.

부 칙

제1조(시행일)

이 지침은 정보보호 최고책임자의 승인일로(2014년 8월 25일)부터 시행한다.