클라우드서비스(IaaS)
보안인증기준 해설서

2023. 3

과학기술정보통신부

KISA 한국인터넷진흥원

<목 차>

제 1 장 클라우드서비스(IaaS) 보안인증 개요 ····· 1
1. 인증제도 소개 ····· 2
2. IaaS 인증 평가 ····· 2
제 2 장 인증기준(IaaS) 해설 ····· 3
1. 정보보호 정책 및 조직 ····· 4
1.1 정보보호 정책 ····· 4
1.2 정보보호 조직 ····· 9
2. 인적보안 ····· 13
2.1 내부인력 보안 ····· 13
2.2 외부인력 보안 ····· 21
2.3 정보보호 교육 ····· 25
3. 자산관리 ····· 29
3.1 자산 식별 및 분류 ····· 29
3.2 자산 변경관리 ····· 36
3.3 위험관리 ····· 40
4. 서비스 공급망 관리 ····· 46
4.1 공급망 관리 정책 ····· 46
4.2 공급망 변경관리 ····· 49
5. 침해사고 관리 ····· 51
5.1 침해사고 대응 절차 및 체계 ····· 51
5.2 침해사고 대응 ····· 56
5.3 사후관리 ····· 60
6. 서비스 연속성 관리 ····· 62
6.1 장애대응 ····· 62
6.2 서비스 가용성 ····· 68
7. 준거성 ····· 74
7.1 법 및 정책 준수 ····· 74
7.2 정보 시스템 감사 ····· 77
8. 물리적 보안 ····· 81
8.1 물리적 보호구역 ····· 81
8.2 정보처리 시설 및 장비보호 ····· 88
9. 가상화 보안 ····· 96
9.1 가상화 인프라 ····· 96
9.2 가상 환경 ····· 105
10. 접근통제 ····· 109

10.1 접근통제 정책 ····109
10.2 접근권한 관리 ····112
10.3 사용자 식별 및 인증 ····117
11. 네트워크 보안 ····123
11.1 네트워크 보안 ····123
12. 데이터 보호 및 암호화 ····134
12.1 데이터 보호 ····134
12.2 매체 보안 ····141
12.3 암호화 ····145
13. 시스템 개발 및 도입 보안 ····149
13.1 시스템 분석 및 설계 ····149
13.2 구현 및 시험 ····155
13.3 외주 개발 보안 ····159
13.4 시스템 도입 보안 ····160
14. 국가기관등의 보안요구사항 ····162
14.1 관리적 보호조치 ····162
14.2 물리적 보호조치 ····168
14.3 기술적 보호조치 ····170

제 1 장 클라우드서비스(IaaS) 보안인증 개요

1. 인증제도 소개

클라우드컴퓨팅서비스(이하 ‘클라우드서비스’) 보안인증제도는 클라우드서비스 제공자가 제공하는 서비스에 대해 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조의2에 따라 정보보호 수준의 향상 및 보장을 위하여 보안인증기준에 적합한 클라우드컴퓨팅서비스에 대하여 보안인증을 수행하는 제도이다.

클라우드서비스 보안인증제도는 상,중,하등급 인증으로 구분되고 인증유효기간은 5년이다.
클라우드컴퓨팅서비스 보안인증에 관한 고시(2023.01.31.)의 부칙 제1조에 따라서 상, 중등급은 별도 기준 마련후 시행한다.
또한 동 고시 부칙 제3조에 따라 상, 중등급 시행전까지 기존 IaaS, SaaS(간편등급, 표준등급), DaaS 인증에 대해서 신청할 수 있다.

클라우드서비스 보안인증의 대상은 클라우드컴퓨팅 기술을 이용하여 정보 시스템의 인프라, 응용프로그램, 개발환경 중 어느 하나 이상을 제공하는 클라우드서비스가 해당된다.

클라우드서비스 보안인증제도는 국가·공공기관에게 안정성 및 신뢰성이 검증된 민간클라우드서비스를 공급하고, 객관적이고 공정한 클라우드서비스 보안인증제도를 통해 이용자의 보안 우려를 해소하고 클라우드서비스의 경쟁력을 확보하는데 그 목적이 있다.

2. IaaS 인증 평가

- 유효기간 : 5년
- 인증대상 : 서버, 저장장치, 네트워크 등을 제공하는 서비스
- 통제항목 : 116개 통제항목
- 평가 종류 : 최초평가 => 사후평가(4회) => 갱신평가

제 2 장 인증기준(IaaS) 해설

1. 정보보호 정책 및 조직

1.1 정보보호 정책

통제항목	1.1.1 정보보호 정책 수립		
세부통제내용	정보보호 정책을 문서화하고, 정보보호 최고책임자의 승인 후 정책에 영향을 받는 모든 임직원 및 외부 업무 관련자에게 제공하여야 한다.		
점검항목	1) 클라우드 정보보호 정책을 수립하고, 정책 시행을 위한 관련 지침, 절차, 매뉴얼 등을 문서화하고 있는가? 2) 클라우드 정보보호 정책은 정보보호 최고책임자로부터 제 • 개정 시 승인을 받고 있는가? 3) 클라우드 정보보호 정책에 영향을 받는 모든 임직원 및 외부 업무 관련자에게 정책의 내용을 이해하기 쉬운 형태로 최신본으로 전달하고 있는가?		
신청기관 준비사항 (관련증적)	• 정보보호 정책서 • 정보보호 시행문서 • 정보보호 최고책임자의 승인을 확인할 수 있는 내부 결재문 또는 서명본 • 정책 및 지침의 배포 증적 (공지사항 게시판 이용 등)	참고사항 (샘플자료)	• 정보보호 정책서 • 정보보호 시행문서
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

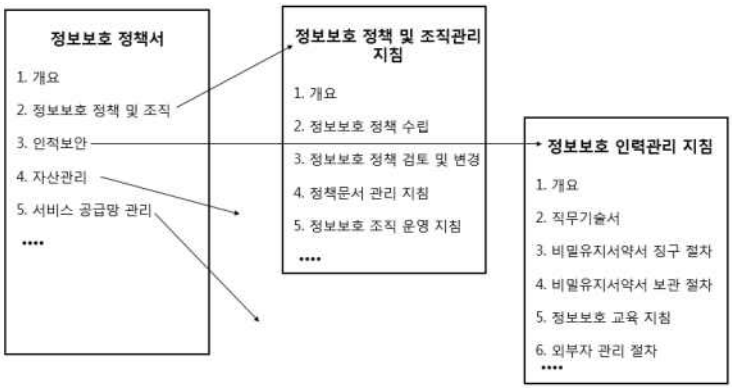
점검항목 해설

➪ **점검항목 1)**

■ 클라우드컴퓨팅서비스 제공자(CSP)는 클라우드 서비스 운영에 필요한 모든 정보보호 활동의 근거가 될 수 있는 정보보호 정책과 이를 시행하기 위한 세부적인 방법, 절차 등을 포함한 시행문서[1](지침/절차/매뉴얼 등)를 수립하여 문서화하여야 한다.

- 정책서와 시행문서에 포함된 내용은 일관성이 있어야 하며, 시행문서는 정보보호 정책에서 수립한 정책을 실제 수행하기 위한 지침서이므로 정보보호 활동 인력이 지침을 기반으로 정보보호 활동을 수행할 수 있도록 상세하게 작성하여야 한다.

1) 시행문서란 정보보호 정책서에 귀속되는 지침 또는 절차 또는 매뉴얼을 모두 포함한다.



⇨ 점검항목 2)

■ 정보보호 정책서 및 시행문서는 정보보호 최고책임자로부터 제·개정 시 승인을 받아야 한다.

- 최고책임자의 승인은 내부결재를 통해 승인을 받아야 하며, 최고책임자 승인과 관련한 증적으로는 내부결재 문서 또는 최고책임자가 정보보호 정책문서에 직접 서명 또는 직인을 할 수 있다.

문 서 명 : 개발 및 도입 절차서 작성일자 : 2019-08-12
문서번호 : KSEL-OP-M-DEVELOPMENT 페이지수 : 1/1

본 절차서는 클라우드컴퓨팅서비스를 제공하기 위한 운영문서로서 검토 및 승인되었다.

구분	직위	성명	일자	서명
승인	정보보호 최고책임자	홍길동	2019. 08. 16	
검토	정보보호 담당자	책임자	2019. 08. 12	

⇨ 점검항목 3)

■ 정보보호 정책서 및 시행문서는 최신으로 유지되고, 임직원 등 관련자가 쉽게 접근하여 활용할 수 있도록 하여야 한다.

- 정보보호 정책을 주기적으로 검토하고 법 개정·보안사고 등이 발생 시 반영
- 메일 또는 사내 게시판 등을 활용하여 배포 등

<table>
<tr><th>통제항목</th><th colspan="3">1.1.2 정보보호 정책 검토 및 변경</th></tr>
<tr><td>세부통제내용</td><td colspan="3">정보보호 정책의 타당성 및 효과를 연 1회 이상 검토하고, 관련 법규 변경 및 내·외부 보안사고 발생 등의 중대한 사유가 발생할 경우에는 추가로 검토하고 변경하여야 한다.</td></tr>
<tr><td>점검항목</td><td colspan="3">1) 클라우드컴퓨팅서비스 제공자는 클라우드 정보보호 정책 및 정책 시행 문서에 대한 타당성 검토를 최소 연 1회 이상 수행하고 있는가?
2) 중요한 변경 발생시 클라우드 정보보호정책 및 정책시행 문서의 변경 여부를 검토하여 필요 시 변경을 하고 있는가?
3) 클라우드 서비스 이용자에게 변경된 보안정책, 주요 보안 이슈 등을 공유하는가?</td></tr>
<tr><td>신청기관
준비사항
(관련증적)</td><td>• 정보보호정책 검토회의록
• 정보보호 정책/지침 검토 및 개정이력
• 주요 변경사항 공유 예시</td><td>참고사항
(샘플자료)</td><td>• 정보보호 정책서
• 정보보호 시행문서</td></tr>
<tr><td colspan="2">ISMS-P 인증 취득 시 심사 생략 가능 대상</td><td colspan="2">X</td></tr>
</table>

점검항목 해설

⇨ **점검항목 1)**

■ 정보보호 정책 및 시행문서는 최소 연 1회 이상 검토하여야 하고, 검토에 대한 이력을 회의록 등에 기록하고 보관하여야 한다.

■ 다음의 경우를 포함하여 클라우드컴퓨팅서비스의 환경변화에 따른 정보보호정책 및 시행문서의 정합성 및 타당성을 검토하여야 한다.
- 정보보호 및 개인정보 관련 법적 요구사항
- 공공기관의 보안요구사항이 반영된 계약서, SLA 내용
- 보안감사 결과 발견된 사항에 대한 보완조치
- 중대한 보안사고 결과
- 새로운 위협 또는 취약점
- 정보보호 환경의 중대한 변화
- 조직 사업 환경의 변화

■ 정보보호 정책 및 시행문서 검토 시에는 정보보호 실무조직 인원과 이해관계자가 참여하여 검토하여야 한다.

⇨ **점검항목 2)**

■ 정기적인 검토 이외에 다음과 같은 상황이 발생한 경우 추가적인 검토를 수행하여야 한다.

- 중대한 보안사고 발생
- 정보보호 및 개인정보, 클라우드컴퓨팅 관련 법령 제·개정
- 새로운 위협 또는 취약점 발견
- 공공기관의 보안요구사항의 변화
- 클라우드서비스 운영을 위한 제반 사항(네트워크 구성의 변경) 변경 등

■ 정기적인 검토 또는 관련 법규 변경 및 내·외부 보안사고 발생, 보안점검 및 내부감사 결과 반영 등으로 정보보호 정책 및 시행문서의 변경이 필요한 경우 이를 반영하여 개정하여야 한다.

⇨ 점검항목 3)

■ 정보보호 정책(지침)의 변경 및 주요 보안 이슈 발생 시 이용자에게 공지하여야 한다.

- 보안정책 지침
- 주요 보안 이슈 등

통제항목	1.1.3 정보보호 정책문서 관리		
세부통제내용	정보보호 정책 및 정책 시행문서의 이력관리 절차를 수립하고 시행하며, 최신본으로 유지하여야 한다.		
점검항목	1) 클라우드 정보보호 정책 및 정책 시행문서의 제정, 개정, 배포, 폐기 등의 이력을 확인할 수 있도록 관리절차를 수립・이행하고 있는가? 2) 클라우드 정보보호 정책 및 정책 시행문서는 최신본으로 관리하고 있는가?		
신청기관 준비사항 (관련증적)	• 정보보호 정책서 및 시행문서의 이력 관리 내역 • 정보보호 정책서 및 시행문서 최신본 배포 증적	참고사항 (샘플자료)	• 정보보호 정책서 • 정보보호 시행문서
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ 점검항목 1)

■ 클라우드 정보보호 정책 및 정책 시행문서의 제정, 개정, 폐기 시 이력(일자, 내용, 작성자 등)을 확인할 수 있는 관리절차를 수립하고 적용하여야 한다.

- 다음 예제와 같이 제・개정되는 문서에 개정 이력을 확인, 관리할 수 있는 관리대장을 포함하여 작성할 수 있다.

문서 제・개정 이력				
번호	날짜	쪽	내용	담당자
1	2008-10-01	-	최초 작성	홍길동
2	2009-04-06	2	정보보호 최고책임자 변경	장길산
3	2009-07-01	10	망법 개정사항 반영 - 이용자 고지방법 변경	장길산
4	2010-08-12	2	정보보호 최고책임자 변경	장길산

⇨ 점검항목 2)

■ 클라우드 정보보호 정책 및 시행문서는 최신본으로 유지하여야 하며, 관련자가 최신본의 문서에 쉽게 접근하여 활용할 수 있도록 하여야 한다.

■ 클라우드컴퓨팅서비스 보안인증기준의 이행여부 확인이 가능하도록 운영기록(증적)을 확보하고 있어야 한다.

- 생성된 각종 양식, 대장, 로그, 결재문서 등 운영기록의 보관방법, 보호대책, 유지기간, 접근통제 등 관리절차 마련

1.2 정보보호 조직

통제항목	1.2.1 조직 구성		
세부통제내용	정보보호 활동을 계획, 실행, 검토하는 정보보호 전담조직을 구성하고 정보보호 최고책임자를 임명하여야 한다.		
점검항목	1) 클라우드컴퓨팅서비스 제공자는 안전한 서비스 제공을 위해 별도의 실무조직 구성과 정보보호 최고책임자를 임명하고 있는가? 2) 정보보호 전문성을 고려하여 실무조직 구성원을 임명하고 있는가?		
신청기관 준비사항 (관련증적)	• 정보보호 조직 구성도 • 정보보호 최고책임자 임명장 또는 승인문서 • 직무 기술서	참고사항 (샘플자료)	• 정보보호 정책서 • 정보보호조직관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ 점검항목 1)

■ 최고경영자는 조직 내에서 정보보호 관리 활동을 효과적으로 추진하기 위하여 이를 총괄 관리할 수 있는 정보보호 최고책임자(CISO)를 인사발령 등의 공식적인 지정절차를 거쳐 지정하여야 한다.

- 정보보호 최고책임자는 임원급으로 지정
- 정보보호 최고책임자는 다른 직무와의 겸직을 금지
- 정보보호 최고책임자 임명 후 과학기술정보통신부 장관에게 신고

※ 정보보호 최고책임자 지정 및 신고에 대한 상세한 사항은 정보통신망법 제45조의3 및 동법 시행령 제36조의6, 제36조의7을 참고한다.

■ 최고경영자는 조직의 규모 및 클라우드서비스의 중요도에 따라 필요인력, 예산 등을 분석하여 정보보호 실무조직을 구성하여야 한다.

- 조직의 규모에 따라 정보보호 조직은 전담 또는 겸임조직으로 구성할 수 있으며 겸임조직으로 구성하더라도 정보보호 조직에 대한 공식적인 선언 또는 지정이 필요함
- 정보보호 담당자(실무 담당자)는 정보보호 전문성을 보유한 자로 지정하여야 하며, 정보보호 담당자(실무 담당자)가 해당 업무를 충실히 수행할 수 있도록 제반 사항을 지원
- 정보자산과 보안에 관련된 모든 임직원은 정보보호 역할과 책임을 명확하게 정의

➪ **점검항목 2)**

■ 정보보호를 위한 실무조직을 구성하는 경우 구성원의 전문적 지식 보유여부, 실무경력, 직무 관련 교유 이수 이력 등을 고려하여 전문성이 확보된 인력으로 구성하여야 한다. 전문성에 대한 기준은 내부 지침으로 정할 수 있다.

예시) 정보보호 실무조직의 구성원을 임명하는 경우 다음의 조건을 검토하여 임명한다.

- 정보보호 관련 전문 지식 보유 여부 (관련 학위 또는 자격 (보안기사, ISMS-P 등) 보유)
- 정보보호 관련 실무경력
- 정보보호 관련 직무교육 이수
- 개인정보 담당자의 경우 개인정보 보호 관련 교육 이수 등

통제항목	1.2.2 역할 및 책임 부여		
세부통제내용	정보자산과 보안에 관련된 모든 임직원 및 외부 업무 관련자의 정보보호 역할과 책임을 명확하게 정의하여야 한다. 또한, 서비스 이용자의 정보보호 역할과 책임도 서비스 수준 협약 등을 통해 명확하게 정의하여야 한다.		
점검항목	1) 정보보호 최고책임자와 정보보호 관련 담당자의 역할 및 책임을 정의하고 있는가? 2) 정보보호 최고책임자와 정보보호 관련 담당자의 활동을 평가할 수 있는 체계를 수립하고 있는가? 3) 클라우드서비스 수준 협약(SLA) 또는 계약서에 이용자의 정보보호 역할과 책임이 반영되어 있는가?		
신청기관 준비사항 (관련증적)	• 직무기술서 • 정보보호활동 평가 지표 • SLA 또는 이용자와의 계약서	참고사항 (샘플자료)	• 정보보호 정책서 • 정보보호조직관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 정보보호 정책서 또는 시행문서(정보보호 조직 구성지침 등)에서 규정하고 있는 정보보호 최고책임자 등 정보자산 및 정보보호와 관련된 모든 임직원의 역할 및 책임을 직무기술서 등을 활용하여 구체적으로 정의하여야 한다.

■ 정보보호 담당자로 외부 인원이 포함되는 경우 외부 인원의 역할 및 책임도 구체적으로 정의하여야 한다.

⇨ **점검항목 2)**

■ 정보보호 최고책임자 및 정보보호 실무 담당자의 책임과 역할을 평가할 수 있는 지표를 개발하여 주기적으로 평가할 수 있는 체계를 구축하여야 한다.
- 평가 주기는 내부적으로 수립(연도별 또는 반기별 또는 분기별 등)
- 평가체계는 가급적이면 정량화하여 투명한 평가가 이루어질 수 있도록 수립
- 직무기술서에 정의된 역할의 수행 여부를 판단할 수 있는 지표 산정(회사의 운영환경 등 고려)

⇨ **점검항목 3)**

■ 클라우드 서비스 수준 협약(SLA) 또는 계약서에 이용자에게 부과되는 정보보호 역할과 책임이 명시되어야 한다.

- 이용자에게 부과되는 정보보호 역할과 책임은 이용자가 이해할 수 있도록 상세하고 명확하게 기술되어야 한다.

※ 이용자 부과 역할 및 책임 예시

제공자의 의무	이용자의 의무
제OO조 (제공자의 의무) ① 제공자는 본 약관이 정하는 바에 따라 지속적이고 안정적인 서비스를 제공하는데 최선을 다합니다. ② 제공자는 항상 이용자의 개인정보를 포함한 이용자 정보에 대하여 관리적, 기술적 안전조치를 강구하여 정보보안에 최선을 다합니다. ③ 제공자는 공정하고 건전한 운영을 통하여 전자상거래 질서유지에 최선을 다하고 지속적인 연구개발을 통하여 양질의 서비스를 제공함으로써 고객만족을 극대화하여 인터넷 사업 발전에 기여합니다. ④ 제공자는 이용자로부터 제기되는 불편사항 및 문제에 대해 정당하다고 판단될 경우 우선적으로 그 문제를 즉시 처리합니다. 단, 신속한 처리가 곤란할 경우, 이용자에게 그 사유와 처리일정을 즉시 통보합니다. ⑤ 제공자는 소비자 보호단체 및 공공기관의 소비자 보호업무의 추진에 필요한 자료 등의 요구에 적극 협력합니다.	제OO조 (이용자의 의무) ① 아이디와 비밀번호에 관한 모든 관리의 책임은 이용자에게 있습니다. ② 이용자는 아이디와 비밀번호를 제 3 자가 알 수 있도록 해서는 안 됩니다. ③ 이용자는 다음 행위를 하여서는 안됩니다. 1. 신청 또는 변경 시 허위내용의 등록 2. 타인의 정보도용 3. 제공자가 게시한 정보의 변경 4. 제공자가 정한 정보 이외의 정보(컴퓨터 프로그램 등) 등의 송신 또는 게시 5. 제공자 와 기타 제 3 자의 저작권 등 지적재산권에 대한 침해 6. 제공자 및 기타 제 3 자의 명예를 손상 시키거나 업무를 방해하는 행위 7. 외설 또는 폭력적인 메시지, 화상, 음성, 기타 공서양속에 반하는 정보를 서비스에 공개 또는 게시하는 행위 8. 기타 불법적이거나 부당한 행위

2. 인적보안

2.1 내부인력 보안

통제항목	2.1.1 고용계약		
세부통제내용	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.		
점검항목	1) 고용 계약서에 정보보호 정책 및 관련 법률을 준수하도록 하는 조항 또는 조건이 포함되어 있는가? 2) 새로 채용하거나 합류한 근무 인력이 고용 계약서에 서명 후 클라우드컴퓨팅서비스의 설비, 자원, 자산에 접근이 이루어지고 있는가?		
신청기관 준비사항 (관련증적)	• 고용 계약서 • 정보보호서약서 및 비밀유지서약서	참고사항 (샘플자료)	• 정보보호 정책서 • 인적보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ **점검항목 1)**

■ 고용 계약서에 정보보호 정책 및 관련 법률을 준수하도록 하는 조항 또는 조건이 포함되어야 한다.

> **제9조(보안의무)**
> "근로자"는 "사용자"의 업무수행상 얻은 기밀에 대해서 계약기간 중은 물론 후에라도 일절 누설하여서는 안되며 상기 사항의 위반으로 인한 민, 형사상의 책임을 진다.

- 고용 계약서 내에 정보보호 정책 및 법률 준수에 대한 상세 내용을 포함하기 어려운 경우 별도 정보보호서약서 등을 추가 작성 가능

⇨ **점검항목 2)**

■ 신규 고용인력 및 합류한 근무 인력이 클라우드컴퓨팅서비스의 설비, 자원, 자산에 접근이 허용되기 전에 고용 계약서가 작성되어 있어야 한다.

통제항목	2.1.2 주요 직무자 지정 및 감독		
세부통제내용	클라우드컴퓨팅서비스의 시스템 운영 및 개발, 정보보호 등에 관련된 임직원의 경우 주요 직무자로 지정하여 관리하고, 직무 지정 범위는 최소화하여야 한다.		
점검항목	1) 클라우드컴퓨팅서비스를 제공하기 위한 중요 정보자산(정보, 시스템 등)을 취급하는 직무를 정의하고 해당 직무를 수행하는 주요 직무자를 지정하고 있는가? 2) 중요정보를 취급하는 주요 직무자는 최소한으로 지정하고 주기적으로 주요 직무자 현황을 관리하고 있는가?		
신청기관 준비사항 (관련증적)	• 주요 직무자 현황 • 직무기술서 • 주요 가상 정보 시스템 계정 및 권한 관리 대장	참고사항 (샘플자료)	• 정보보호 정책서 • 정보보호조직관리지침 • 인적보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 다음을 주요 직무로 분류할 수 있으며 이 업무를 수행하는 임직원을 주요 직무자로 지정하여야 한다.

- 정보보호최고책임자
- 중요정보(개인정보, 인사정보, 영업비밀, 산업기밀, 재무정보 등) 취급
- 주요 정보 시스템(서버, 가상화 시스템, DB, 응용 프로그램 등) 운영 및 개발
- 사용자 및 이용자 클라우드 포탈 담당자
- (개인) 정보보호 업무 기획 및 정보보호시스템 담당자 (정보보호 관련 정책/지침 관리, 침해사고대응, 보안관제, 정보보호시스템 운영자 등)
- 네트워크 관리
- 암호키 관리
- 인사, 물리, 법무 담당자 등

⇨ **점검항목 2)**

■ 주요 직무자의 경우 업무 범위 및 목적에 벗어나는 정보처리 권한을 부여하지 않도록 관련 직무자를 최소한으로 지정하여야 한다.

■ 주요 직무자의 현황을 주기적으로 관리하여 직무자 별 업무 성격에 따라 적정한 권한이 부여되었는지 여부를 검토하여야 한다.

■ 인증 통제항목 ‘10.2.1 사용자 등록 및 권한 부여’ 에서는 클라우드컴퓨팅시스템 각각에 대해 사용자 등록 시 직무별, 역할별 접근권한 분류체계를 수립하고 업무상 필요한 최소한의 권한 부여를 요구

■ 인증 통제항목 ‘2.1.2 주요 직무자 지정 및 감독’ 에서는 각각의 중요 정보자산(정보, 시스템, 시설 등)을 취급하는 모든 직무를 식별하고 주요 직무자에 대해 최소화 지정 및 주기적인 현황 검토를 수행하는 등 전체적으로 통합 관리하는 측면을 요구

■ 조직도, 자산관리대장, 직무기술서, 시스템 등록된 사용자 현황, 업무분장표 등을 통해 인증범위 내 주요 직무자 식별 및 주요 직무자의 최소한 지정, 주기적 검토 여부, 각 증적들간의 상호 정합성 등을 판단 가능

통제항목	2.1.3 직무 분리		
세부통제내용	권한 오남용 등 내부 임직원의 고의적인 행위로 발생할 수 있는 잠재적인 위협을 줄이기 위하여 직무 분리 기준을 수립하고 적용하여야 한다.		
점검항목	1) 직무의 권한 오남용을 예방하기 위하여 정보보호 관련 주요 직무 분리 기준을 수립하고 직무별 역할과 책임을 명확하게 기술하고 있는가? 2) 직무 분리가 어려운 경우 직무자 간 상호 검토, 상위관리자 정기 모니터링 및 변경사항 승인, 책임추적성 확보 방안 등의 보완통제를 마련하고 있는가?		
신청기관 준비사항 (관련증적)	• 직무 분리 기준 • 직무기술서 • 주요 직무자 현황 • 직무 미분리 시 보완통제 현황	참고사항 (샘플자료)	• 정보보호 정책서 • 정보보호조직관리지침 • 인적보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 직무별 권한과 책임을 분산시켜 직무 간 상호견제를 할 수 있도록 직무 분리 기준을 수립하여야 한다.

※ 직무 분리 기준 예시

직무 분리 대상 업무
개발과 운영 직무 분리
정보 시스템(서버, DB, 네트워크 등)간 운영직무 분리
정보보호 관리와 정보 시스템 운영직무 분리
정보보호 관리와 정보 시스템 개발직무 분리
민간 및 공공기관 클라우드컴퓨팅시스템 간 운영직무 분리 등

⇨ 점검항목 2)

■ 조직 규모가 작거나 인적 자원 부족 등의 사유로 인해 불가피하게 직무 분리가 어려운 경우, 직무자 간의 상호 검토, 상위관리자의 주기적인 직무수행 모니터링 및 변경사항 검토/승인, 직무자의 책임추적성 확보 등의 보완통제를 마련하여야 한다.

통제항목	2.1.4 비밀유지서약서		
세부통제내용	정보보호와 개인정보보호 등을 위해 필요한 사항을 비밀유지서약서에 정의하고 주기적으로 갱신하여야 한다.		
점검항목	1) 직원 채용, 직무 변경, 고용 해지 시 정보보호 책임이 명시된 정보보호서약서 및 비밀유지서약서를 받고 있는가? 2) 임시직원 혹은 외주용역과 같은 외부인력에게 정보자산에 대한 접근권한을 부여할 경우, 정보보호에 대한 책임을 계약서에 명시하고 이에 대한 정보보호서약서를 받고 있는가? 3) 정보보호서약서 및 비밀유지서약서는 법적 분쟁 발생 시 증거자료로 사용할 수 있도록 안전하게 보존하고 용이하게 찾아볼 수 있도록 관리하고 있는가?		
신청기관 준비사항 (관련증적)	• 정보보호서약서 및 비밀유지서약서 (임직원 및 외부인력) • 외주 용역 계약서 • 서약서 등 중요 문서 보관	참고사항 (샘플자료)	• 정보보호 정책서 • 인적보안지침 • 인사규정
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ 점검항목 1)

■ 신규로 채용된 인력은 조직의 중요정보 취급 및 관리 시 정보보호의 필요성과 책임에 대해 명시된 정보보호서약서에 서명하고 제출하여야 한다.

■ 정보보호서약서의 제출 의무에 대해 신규 인력 채용 절차 중 기본적인 사항으로 인식하고 관리부서를 지정하여 정보보호서약서를 관리하여야 한다.
- 보안서약서 징구절차와 대상 확인

■ 직무상 알게 된 조직의 중요정보에 대해 누출 방지를 위하여 인력 퇴사 절차 내 비밀유지서약서를 징구하고 누출 발생 시 그에 따르는 법적 책임이 있음을 상기시켜야 한다.

■ 직무변경과 같이 인력의 고용조건에 변화가 발생한 경우 이전에 습득한 비밀정보를 누출하지 않도록 정보보호서약서를 제출하여야 한다.

※ 보안 서약서 예시

보안 서약서

회사의 전 임직원 및 자회사, 협력회사, 입사직에 종사하는 사원들은 지켜야 할 보안사항을 숙지했음을 입증하는 서약서에 서명해야 합니다. 입직원들은 근무기간 뿐 아니라 근무기간 후(종업증, 경쟁업체 2년 내 취업금지)에도 동일하게 적용됨을 인식하고 서명하기 전 숙독하여 주시기 바랍니다.

1. 나는 주식회사 OOOO(이하 회사라 함)에 관한 정보와 회사가 비밀유지 대상으로 지정한 정보를 업무에 한해 이용할 것이다.
2. 나는 회사로부터 제공받은 각종 서류, 사진, 자료, 전산장비 등 정보를 기록매체에 대해 주의 깊게 사용, 보관함으로서 무단변조, 복사, 훼손, 분실 등으로부터 안전하게 관리한다.
3. 나는 상대가 누구이건 간에 알 필요가 없는 자에게 회사 혹은 제3자 소유정보를 누설하지 않는다.
4. 나는 허가받지 않은 정보나 시설에 접근하지 않는다.
5. 나는 나의 업무나 회사와 관련된 업무를 수행하는 경우에만 사내 데이터 처리시설을 사용할 것이며 정보자산의 외부 발신시 회사의 통제절차를 준수할 것이다.
6. 나는 회사의 전산장비에 사적 정보나 회사가 아닌 타 기업 정보 및 회사와 관련되지 않은 데이터를 보관하지 않겠다.
7. 나는 나에게 할당된 사원증, 사용자 ID 및 패스워드가 중요한 보안사항임을 인식하여 오직 나만이 사용할 것이며 타인에게 대여 또는 누설하지 않겠다.
8. 나는 회사의 보안규정 및 정책을 준수할 것이다.

나는 상기사항을 숙지하여 이를 성실히 준수할 것을 동의하며, 서약서의 보안사항을 위배하였을 경우 부정경쟁방지법 등 관련 법령에 의한 민, 형사상의 책임 이외에도 회사의 사규나 관련 규정에 따른 징계조치 등 어떠한 처벌도 감수할 것이며 회사에 끼친 손해에 대해 지체없이 변상 복구시킬 것을 서약합니다.

년 월 일

성 명 : (인)
주민등록번호 :

(주)OOOO 귀중

➪ **점검항목 2)**

■ 임시직원 혹은 외주용역업체 직원과 같은 외부인력에게 정보자산에 대한 접근권한을 부여할 경우 정보보호 책임, 조직 내 정보보호 규정 준수 의무, 정보보호 의무에 미준수로 인한 사건•사고 발생 시 손해배상 책임 등의 내용을 정보보호 서약서에 명시하고 서명을 받아야 한다.

- 임시직원, 외부인력 등에 대한 정보보호서약서 징구절차와 대상 확인

※ 상황별 비밀유지서약서 징구 예시

대상	상황
내부 인력	입사, 퇴사
	고용 조건의 변경 및 변경사항 발생
	전보 및 직무 변경
	프로젝트 및 TF 참여
외부 인력	사업 시작
	사업 종료

- 인증심사 대상 내의 임직원 및 임시직원, 외주용역업체 직원 등 관련자들에 대해서 정보보호서약서가 징구 관리되어야 함

■ 계약서에 정보보호 책임을 명시하는 부분은 '2.2.1. 외부인력 계약', '4.1.2. 공급망 계약'에서 계약서를 검토하고 명시한다.

⇨ 점검항목 3)

■ 정보보호서약서 및 비밀유지서약서는 법적 분쟁 발생 시 법률적 책임에 대한 증거자료로 사용할 수 있기 때문에 필요 시 용이하게 찾아볼 수 있는 형태로 안전하게 보관하여야 한다.

■ 정보보호서약서 및 비밀유지서약서에 개인정보가 포함될 경우 비인가 된 제 3 자에게 누출되지 않도록 물리적으로 안전한 장소에 보관하여야 한다.

<table>
<tr><th>통제항목</th><th colspan="3">2.1.5 퇴직 및 직무변경</th></tr>
<tr><td>세부통제내용</td><td colspan="3">임직원의 퇴직 또는 직무 변경에 관한 책임을 명시적으로 정의하고 수행하여야 한다. 또한 이에 대한 접근권한도 제거하여야 한다.</td></tr>
<tr><td>점검항목</td><td colspan="3">1) 부서 및 직무변경, 휴직, 퇴직 등으로 인한 인사변경 내용이 인사부서, 정보보호부서, 정보시스템 운영부서 간에 공유되고 있는가?
2) 조직 내 인력(정규직 임직원, 임시직원, 외주용역업체 직원 등)의 직무변경 혹은 퇴직 시 정보자산 반납, 접근권한 조정•회수, 결과 확인 등 수립된 절차에 따라 지체 없이 이행하고 있는가?</td></tr>
<tr><td>신청기관 준비사항 (관련증적)</td><td>• 퇴직 및 직무변경 절차서
• 퇴직자 보안점검 체크리스트 및 점검 내역
• 퇴직 시 자산 반납관리대장
• 보안서약서</td><td>참고사항 (샘플자료)</td><td>• 정보보호 정책서
• 인적보안지침
• 인사규정</td></tr>
<tr><td colspan="2">ISMS-P 인증 취득 시 심사 생략 가능 대상</td><td colspan="2">X</td></tr>
</table>

점검항목 해설

⇨ **점검항목 1)**

■ 부서 및 직무변경, 휴직, 퇴직 등 인사변경 발생 시 정보자산 반납, 접근권한의 변경•회수 조치가 신속하게 이루어질 수 있도록 인사부서는 변경내용을 정보보호부서, 정보 시스템 운영부서 등에 공유하여야 한다.

- 관련 조직 및 시스템 간에 인사 변경 내용이 신속하게 공유될 수 있도록 절차 수립•이행

■ 이용자에게 담당자 퇴직 및 직무변경 시 알려야 하는 정보(예: 고객 서비스 담당자 변경사항 등)를 통지하여야 한다.

⇨ **점검항목 2)**

■ 조직 내 인력(정규직 임직원, 임시직원, 외주용역업체 직원 등)의 직무변경 혹은 퇴직 발생 시 정보자산 반납, 접근권한의 조정•회수 등을 수립된 절차에 따라 시행하고 결과를 확인하여야 한다.

- 퇴직, 휴직자의 계정, 권한 반납, 회수 처리 이행여부 점검

■ 직무변경자 혹은 퇴직자와 불가피하게 정보 시스템 및 정보보호시스템 계정을 공유하여 사용한 경우 계정의 비밀번호를 즉시 변경하여야 한다.

2.2 외부인력 보안

통제항목	2.2.1 외부인력 계약		
세부통제내용	외부인력(외부유지보수직원, 외부용역자 포함)에 의한 정보자산 접근 등과 관련된 보안요구사항을 계약에 반영하여야 한다.		
점검항목	1) 정보처리 업무를 외부인력에게 위탁하는 경우 보안요구사항을 정의하여 계약 시 반영하고 있는가?		
신청기관 준비사항 (관련증적)	• 위탁 계약서 • 정보보호 협약서 • RFP, 외주용역 평가표	참고사항 (샘플자료)	• 정보보호 정책서 • 인적보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ **점검항목 1)**

■ 조직의 업무 중 서비스 제공을 위한 시스템 통합(System Integration, SI), 운영(System Maintenance, SM), 유지보수, 고객상담 등 외부인력에게 업무를 위탁하는 경우, 외부인력의 업무 형태에 따라 다음과 같은 보안요구사항을 정의하여 계약시 반영하여야 한다.

- 정보보호 관련 법률 준수 (개인정보 처리 관련 등)
- 정보보호서약서 제출 (비밀유지, 정보보호 책임 등)
- 위탁 업무 수행 직원 대상 주기적인 정보보호 교육 수행
- 업무수행 관련 취득한 중요정보 유출 방지 대책
- 외부인력 내부 네트워크(업무망) 연결 시 인터넷접속 제한
- 외부인력 사무실 공간에 대한 물리적 보호조치 (장비 및 매체 반출입, 출입통제 등)
- 외부인력 PC 등 단말 보안 (백신 설치, 안전한 패스워드 설정 및 주기적 변경, 화면보호기 설정 등)
- 조직 중요정보 시스템 접근 허용 시 과도한 권한이 부여되지 않도록 접근권한 부여 및 해지 절차
- 주기적 보안점검 수행
- 무선 네트워크 구축 및 사용 제한 (필요 시 위험분석을 통한 대책 마련 후 책임자 승인)
- 재위탁 하도급 계약 시 본 계약 수준의 보안요구사항 정의
- 보안요구사항 위반 시 처벌, 손해배상 책임
- 보안사고발생에 따른 보고 의무 등

※ 다만 외부자 업무형태에 따라 세부점검항목에서 제시하고 있는 보안요구사항을 계약서에 반영하지 못하는 경우 타당한 사유가 있어야 한다.

통제항목	2.2.2 외부인력 보안 이행 관리		
세부통제내용	계약서에 명시한 보안요구사항 준수 여부를 주기적으로 점검하고 위반 사항이나 침해사고 발생 시 적절한 조치를 수행하여야 한다.		
점검항목	1) 외부인력이 계약서에 명시한 보안요구사항을 준수하고 있는지 주기적으로 점검 또는 감사를 수행하고 문제점 발견 시 개선할 수 있는 보호대책을 수립•이행하고 있는가?		
신청기관 준비사항 (관련증적)	• 업무 위탁 계약서 • 보안점검 체크리스트 등 점검 결과 • 보안 조치 및 교육 내역 (결과, 명단, 교재 등)	참고사항 (샘플자료)	• 정보보호 정책서 • 인적보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ **점검항목 1)**

■ 외부인력 관리 직무를 맡은 담당자는 외부인력과 계약 시 정의한 보안요구사항을 준수하고 있는지 주기적으로 점검 또는 감사를 수행하여야 한다.

■ 또한 외부인력이 자체적으로 정보보호책임자를 지정하여 보안점검을 수행한 경우 그 결과를 주기적으로 보고받고 문제점 발생 시 유사한 문제가 재발하지 않도록 추가적인 보호대책을 수립하고 이행하여야 한다.

- 외부자의 보안요구사항의 지속적인 유지 여부 점검
- 점검결과 및 이행조치 현황 등을 기록 및 관리
- 정보시스템 및 업무에 변경사항 발생 시 보안요구사항 이행여부 점검
- 내부지침 개정 등으로 보안요구사항 변경 필요 시 계약서 등 변경

<table>
<tr><th>통제항목</th><th colspan="3">2.2.3 계약 만료 시 보안</th></tr>
<tr><td>세부통제내용</td><td colspan="3">외부인력과의 계약 만료 시 자산 반납, 접근권한의 회수, 중요정보 파기, 업무 수행 시 알게 된 정보에 대한 비밀 유지서약 등을 확인하여야 한다.</td></tr>
<tr><td>점검항목</td><td colspan="3">1) 위탁사가 위탁 업무 수행과정에서 담당자 퇴직 등의 변경사항이 발생할 경우 위탁사 관련부서에 보고하고 공식적인 절차에 따라 정보자산 반납, 접근계정 삭제 등의 조치를 하고 있는가?
2) 외부인력과의 계약 만료, 업무 종료 시 공식적인 절차에 따라 정보자산의 반납, 정보 시스템 접근계정 삭제, 중요정보 파기, 물리적 출입권한 삭제 업무 수행 시 알게 된 정보의 비밀유지서약서 작성 등을 확인하고 있는가?</td></tr>
<tr><td>신청기관
준비사항
(관련증적)</td><td>• 보안점검 체크리스트 등 점검 결과
* (정보 및 개인정보 파기 확인)
• 비밀유지 확인서</td><td>참고사항
(샘플자료)</td><td>• 정보보호 정책서
• 인적보안지침</td></tr>
<tr><td colspan="2">ISMS-P 인증 취득 시 심사 생략 가능 대상</td><td colspan="2">O</td></tr>
</table>

점검항목 해설

➪ **점검항목 1)**

■ 위탁 업무 수행과정에서 외부인력의 관련 업무 담당자가 변경될 수 있으며 변경이력에 대한 보고 및 적절한 보호조치가 지체없이 이루어질 수 있도록 관리하여야 한다.

- 담당조직이 외부자 계약만료, 업무 종료, 담당자 변경이 발생했음을 신속하게 인지할 수 있도록 정보 공유

➪ **점검항목 2)**

■ 외부인력과의 계약 만료, 업무 종료에 따른 공식적인 정책 및 절차가 수립되어야 하며 정책 및 절차를 통해 정보자산 반납 및 업무 중 사용하였던 모든 접근계정 삭제 및 비밀유지서약서 작성이 보장되어야 한다.

- 외부인력 등에 제공한 자료, 최종 산출물 등의 제반자료는 전량 회수하고 외부업체에 복사본 등의 별도 보관 금지

※ 외부인력 변경 또는 업무 종료 시 체크리스트 예시

번호	확인 사항	담당자 확인 결과
1	관련 부서에 변경 사항 통지 여부 (인력 변경 시)	
2	지급된 정보자산 반납 여부	
3	시스템 접근계정 삭제	
4	제공된 데이터 및 문서의 반납 또는 파기	
5	단말기 내 저장매체 데이터 삭제	
6	출입카드 반납	
7	서약서 작성	
8	담당부서 책임자 확인	

2.3 정보보호 교육

통제항목	2.3.1 교육 프로그램 수립		
세부통제내용	모든 임직원 및 외부 업무 관련자를 포함하여 연간 정보보호 교육 프로그램을 수립하여야 한다.		
점검항목	1) 내부의 모든 직원과 외부인력(외주용역)을 위한 정보보호 교육, 훈련, 인식 프로그램이 수립되어 있는가?		
신청기관 준비사항 (관련증적)	• 연간 교육계획서	참고사항 (샘플자료)	• 정보보호 정책서 • 인적보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ **점검항목 1)**

■ 정보보호 교육의 시기(예 : 분기별, 반기별 등), 기간, 대상, 내용, 방법 (예 : 온라인, 집합교육 등) 등의 내용이 포함된 연간 정보보호교육 계획을 수립하여야 한다.

- 교육 유형 : 정보보호 인식제고 교육, 주요직무자,/개인정보취급자/수탁자 교육, 전문 교육 등
- 교육 대상 :임직원 및 관련 외부자 포함
- 교육 시기 : 반기 1회 또는 연 1회 등

■ 교육의 대상, 내용, 기간 등에 따라 효과적으로 교육을 수행할 수 있는 방법 (예 : 집합교육, 온라인 교육, 전달 교육 등)을 선택하여야 한다.

- 교육 대상자의 수준 및 업무특성과 환경 고려

■ 정보보호 인식제고를 위하여 보안의 날 지정, 포스터 또는 뉴스레터를 제작할 수도 있다.

■ 정보보호 및 클라우드 서비스와 관련하여 직무별 전문성 제고를 위한 별도의 교육을 받을 수 있도록 하여야 한다.

- 컨퍼런스, 세미나, 워크샵 등 참고, 전문 교육기관 위탁 교육, 외부 전문가 초빙 등

통제항목	2.3.2 교육 시행		
세부통제내용	모든 임직원 및 외부 업무 관련자를 대상으로 연 1회 이상 정보보호 교육을 시행하고 정보보호 정책 및 절차의 중대한 변경, 내•외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생하면 추가 교육을 실시하여야 한다.		
점검항목	1) 내부의 모든 직원과 외부인력(외주용역)을 대상으로 연 1회 이상 기본 정보보호 교육을 수행하고 있는가? 2) 정보보호 정책 및 절차의 중대한 변경, 조직 내•외부 보안사고 발생, 정보보호 및 클라우드 관련 법률 변경 등이 발생 시 이에 대한 추가 교육을 수행하고 있는가?		
신청기관 준비사항 (관련증적)	• 연간 교육계획서 • 교육 참석자 목록 • 교육 이수증 • 교육 수행 관련 자료	참고사항 (샘플자료)	• 정보보호 정책서 • 인적보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 정보보호 담당자는 정보보호 연간 교육계획서를 작성하여 정보보호 최고책임자의 승인을 받아 시행하여야 한다.

- 클라우드 서비스를 운영하는 모든 정규직 임직원, 임시직원, 외부인력 등을 대상으로 연 1회 이상 기본 정보보호 교육 시행
- 정보보호 교육계획에는 교육대상, 시행일정, 내용 및 방법 등의 내용 포함
- 자체적인 교육여건이 불가능한 경우 외부의 전문교육기관을 통해 교육 이수 가능

■ 개인정보관리책임자 및 개인정보취급자는 개인정보보호 교육을 별도로 이수하여야 한다.

- 기본 정보보호 교육에 개인정보보호 내용을 포함된 경우 별도 추가 교육 이수 불필요

■ 인증범위 내의 주요직무자로 식별된 인원에 대해서 정보보호 교육을 실시하여야 하며 정보보호 교육에 참여하지 못한 경우 미참여자에 대한 방안을 수립하여야 한다.

- 전파교육, 대체방안 등 마련

⇨ 점검항목 2)

■ 정보보호 정책 및 절차의 중대한 변경, 내·외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생하면 추가적인 교육을 실시하여야 한다.
- 중요하지 않은 사안일 경우 게시판 공지, 이메일 안내 등으로 대체 가능

■ 기본 정보보호 교육 이외에 다음과 같은 상황이 발생할 경우 추가적인 정보보호 교육을 수행하여야 한다.
- 정보보호(개인정보 포함) 및 클라우드 관련 법률 변경
- 조직 내 정보보호 관련 정책 및 절차 변경
- 조직 내•외부 보안사고 발생
- 업무환경의 중대한 변화 발생

통제항목	2.3.3 평가 및 개선		
세부통제내용	정보보호 교육 시행에 대한 기록을 남기고 결과를 평가하고 개선하여야 한다.		
점검항목	1) 정보보호 교육, 훈련, 인식 프로그램의 수행 결과를 평가하고 있는가? 2) 평가 결과를 분석하여 새로운 정보보호 요구사항을 도출하고 프로그램의 개선에 반영하고 있는가?		
신청기관 준비사항 (관련증적)	• 연간 교육계획서 • 교육 참석자 목록 • 교육 이수증 • 교육 결과보고서 • 교육 자료	참고사항 (샘플자료)	• 정보보호 정책서 • 인적보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 교육 시행 후, 교육 공지, 교육자료, 출석부 등과 같은 기록을 남기고 미리 마련된 평가기준에 따라 설문 또는 테스트 등을 통해 교육 내용의 적절성과 효과성을 평가하여야 한다.

- 직무 특성 및 수준을 고려하여 적절한 교육 내용, 방법, 주기 등에 반영
- 교육 미참여자 최소를 위한 방안 개선
- 교육내용과 교육방법이 각 직무별 보안기준 준수역량 제고에 적합한지 확인 등

⇨ 점검항목 2)

■ 교육평가 결과 내용에서 도출된 문제점에 대해 개선 대책을 마련하고 차기 교육계획 수립 시 반영하여야 한다.

- 직무 관련 특화 교육 실시 등

3. 자산관리

3.1 자산 식별 및 분류

통제항목	3.1.1 자산 식별		
세부통제내용	클라우드컴퓨팅서비스에 사용된 정보자산(정보 시스템, 정보보호시스템, 정보 등)에 대한 자산분류기준 수립하고 식별된 자산의 목록을 작성하여 관리하여야 한다.		
점검항목	1) 정보자산(정보 시스템, 소프트웨어 등)의 분류기준을 수립하고 클라우드서비스를 제공하기 위한 모든 정보자산을 식별하고 있는가? 2) 식별된 정보자산을 별도 목록으로 관리하고 있는가? 3) 정기적으로 정보자산 현황을 조사하고 정보자산목록을 최신으로 유지하고 있는가?		
신청기관 준비사항 (관련증적)	• 정보자산 분류기준 • 정보자산 목록	**참고사항 (샘플자료)**	• 정보보호 정책서 • 정보자산관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ **점검항목 1)**

■ 클라우드컴퓨팅서비스 제공자는 제공하는 서비스의 특성에 적합한 분류기준을 수립하고, 이에 따른 정보자산을 식별하여야 한다.

- 정보자산에 대한 조사는 누락되는 자산이 발생하지 않도록 전수 조사를 수행하고 식별된 정보자산은 분류 기준에 따라 분류함

※ 정보자산 분류 예시

분류	설명
정보 시스템	서버, PC 등 단말기, 보조저장매체, 네트워크 장비, 응용 프로그램 등 정보의 수집, 가공, 저장, 검색, 송수신에 필요한 하드웨어 및 소프트웨어
정보보호 시스템	정보의 훼손, 변조, 유출 등을 방지하기 위하여 구축된 시스템으로 침입차단시스템, 침입탐지시스템, 침입방지시스템, 개인정보유출방지시스템 등을 포함
정보	문서적 정보와 전자적 정보 모두를 포함
가상자원	가상 인프라를 통해 가상화된 가상 머신(CSP 소유의 자산), 가상 스토리지, 가상 소프트웨어(예: 배포 이미지 등) 등을 포함
가상 인프라	가상 환경을 제공하기 위해 필요한 하이퍼바이저, 클라우드 플랫폼 등을 포함

⇨ 점검항목 2)

■ 식별된 정보자산은 정보를 확인할 수 있도록 목록화하여 관리하여야 한다.

- 다만, 목록은 자산관리시스템, 문서 등 다양한 형태로 관리 가능
- 공공클라우드서비스를 위한 DR 센터의 정보자산 포함 (위치에 DR 센터 상세 위치 표시)

※ 정보자산 목록 예시

서버 시스템 목록(하이퍼바이저)

자산분류	서버시스템
Description	Cloud 서비스 제공하기 위한 목적으로 사용되는 서버 시스템

구분	자산상세내역								관리형태	
번호	호스트명	VM / Hardware	OS	OS버전	IP	추가 IP (IPMI)	용도 (목적 및 기능)	관리부서	운용자	위치 (상세위치)
1	NX-Certified-01	Hardware	CentOS	7.0	10.80.3.101, 10.80.3.11	10.80.1.101	HCI 서버	클라우드인증팀	홍길동	한국인터넷진흥원/6F/공공클라우드존

서버 시스템 목록 (OS-Linux)

자산분류	서버시스템
Description	Cloud 서비스 제공하기 위한 목적으로 사용되는 서버 시스템

구분	자산상세내역								관리형태	
번호	호스트명	VM / Hardware	OS	OS버전	IP	추가IP	용도 (목적 및 기능)	관리부서	운용자	위치 (상세위치)
1	KISA-Syslog	Hardware	Ubuntu	14.04	10.20.11.75	N/A	시스템로그 적재	클라우드인증팀	홍길동	한국인터넷진흥원/6F/공공클라우드존
2	ESRS_VE	VM	SUSE Linux	Enterprise Server 11 SP3	10.80.10.10	N/A	EMC ECS 장비 헬스 체크 모니터링	클라우드인증팀	홍길동	한국인터넷진흥원/6F/공공클라우드존
3										

서버 시스템 목록 (OS-Windows)

자산분류	서버시스템
Description	Cloud 서비스 제공하기 위한 목적으로 사용되는 서버 시스템

구분	자산상세내역							관리형태		
번호	호스트명	VM / Hardware	OS	OS버전	IP	추가IP	용도 (목적 및 기능)	관리부서	운용자	위치 (상세위치)
1	WIN-LOCHQ24CI08	VM	Windows 2012 R2	6.3.9600 N/A Build 9600	10.64.24.33	N/A	SEP 매니저	클라우드인증팀	홍길동	한국인터넷진흥원/6F/공공클라우드존

스토리지 시스템 목록

자산분류	스토리지
Description	Cloud 서비스 제공하기 위한 목적으로 사용되는 스토리지 시스템

구분	자산상세내역							관리형태		
번호	호스트명	VM / Hardware	OS	OS버전	IP	추가 IP	용도 (목적 및 기능)	관리부서	운용자	위치 (상세위치)
1	ecsn01	Hardware	ECS Version3	3.2.0.1	10.80.5.12	10.80.1.51	스토리지	클라우드인증팀	홍길동	한국인터넷진흥원/6F/공공클라우드존

WEB Application 목록

자산분류	WEB Application
Description	Cloud 서비스 제공하기 위한 목적으로 사용되는 WEB Application

구분	자산상세내역						관리형태		
번호	자산명 (관리명칭)	호스트명	VM / Hardware	s/w version	IP	용도 (목적 및 기능)	관리부서	운용자	위치 (상세위치)
1	ESRS VE	VM	SUSE Linux	Apache 2.2.34	10.80.10.10	EMC ECS 장비 헬스 체크 모니터링	클라우드인증팀	홍길동	한국인터넷진흥원/6F/공공클라우드존
2	NX-Certified-01	VM	CentOS 7.0	Apache 2.4.6	10.80.3.101	CVM 관리 웹	클라우드인증팀	홍길동	한국인터넷진흥원/6F/공공클라우드존

WAS 목록

자산분류	WAS
Description	Cloud 서비스 제공하기 위한 목적으로 사용되는 WAS

구분	자산상세내역						관리형태		
번호	호스트명	VM / Hardware	OS	s/w version	IP	용도 (목적 및 기능)	관리부서	운용자	위치 (상세위치)
1	NX-Certified-01	VM	Apache 2.4.6	Tomcat 8.0.44	10.80.3.101	PRISM 관리용 마스터	클라우드인증팀	홍길동	한국인터넷진흥원/6F/공공클라우드존

DBMS 목록

자산분류	DB
Description	Cloud 서비스 제공하기 위한 목적으로 사용되는 DBMS 시스템 자산 입력

구분	자산상세내역				관리형태		
번호	DBMS명 (종류)	설치 서버 호스트명	IP	용도 (목적 및 기능)	관리부서	운용자	위치 (상세위치)
1	PostgreSQL	ESRS_VE	10.80.10.10	EMC ECS 장비 헬스 체크 모니터링	클라우드인증팀	홍길동	한국인터넷진흥원/6F/공공클라우드존

네트워크 장비 목록

자산분류	네트워크
Description	Cloud 서비스 제공하기 위한 목적으로 사용되는 네트워크 장비 등 자산 입력

구분	자산상세내역						관리형태		
번호	호스트명	OS	버전	IP	추가 IP	용도 (목적 및 기능)	관리부서	운용자	위치 (상세위치)
1	apic1	aci-apic-dk9.3.2.2o	3.2(2oi	10.80.1.11	10.80.1.41	SDN Controller	클라우드인증팀	홍길동	한국인터넷진흥원/6F/공공클라우드존

PC 및 VDI 목록

자산분류	PC&VDI
Description	Cloud 서비스 제공하기 위한 목적으로 사용되는 PC, 노트북, VDI 등 자산 입력

구분	자산상세내역					관리형태
번호	모델명	OS	PC IP / VDI IP	용도	소속팀	사용자 (소속/명)
1	Desktop PC	Windows 10	10.101.130.12	업무용 PC	클라우드인증팀	홍길동

가상머신이미지 목록

자산분류	가상머신이미지
Description	Cloud 서비스 운영 관리 등을 위해 라이선스를 구매한 업무용 소프트웨어 등(배포 이미지)

구분	자산상세 내역			관리형태			
번호	자산명	수량	용도 (목적 및 기능)	관리부서	관리자	물리적 위치 (상세위치)	보관위치
1	TEMPLATE-CENTO 87.5	3	템플릿 VM	클라우드인증팀	홍길동	한국인터넷진흥원/B1F/공공클라우드존	한국인터넷진흥원/6F/사무실

기타 자산 목록

자산분류	기타
Description	Cloud 서비스 제공하기 위한 목적으로 사용되는 기타 보안장비 등 자산 입력

구분	자산상세내역						관리형태			비고
번호	구분	자산명	OS	버전	IP	용도 (목적 및 기능)	관리부서	운용자	위치 (상세위치)	
1	보안소프트웨어	Safer Zone	Windows Server 2012	ver.5.0	10.101.130.12	접근통제 관리	클라우드인증팀	홍길동	한국인터넷진흥원/3F/서버실	

⇨ 점검항목 3)

■ 신규 도입, 변경, 폐기되는 정보자산 현황을 확인할 수 있도록 정기적으로 정보자산 조사를 수행하고 정보자산목록을 최신으로 유지하여야 한다. 클라우드 컴퓨팅 서비스에 사용된 자산(시설, 장비, SW 등)의 변경을 지속적으로 모니터링하여 허가받지 않은 변경을 탐지하고 최신 변경 이력을 유지하여야 한다.

※ 인증심사를 위한 자산 식별 절차

- 클라우드컴퓨팅서비스 제공자는 자체 문서 형식 또는 시스템을 이용하여 전체 정보자산을 분류기준에 따라 식별, 목록화, 최신화 등 관리
- 클라우드컴퓨팅서비스 제공자는 인증심사 전 서비스 제공을 위해 필요한 모든 정보자산을 인증심사용 정보자산관리대장 엑셀 파일을 이용하여 식별하고, 인증심사팀은 정보자산관리대장 엑셀 파일을 이용하여 CCE, CVE, 소스코드진단, 모의해킹 등을 위한 자산을 최종 확정
- 확정된 자산에 대해서 CCE, CVE, 소스코드진단, 모의해킹 등 수행
- 진단을 위해 공공 및 민간을 위한 공용자산, 개발 자산 등은 인증심사팀의 판단에 따라 진단 대상에서 제외 가능

통제항목	3.1.2 자산별 책임할당		
세부통제내용	식별된 자산마다 책임자 및 관리자를 지정하여 책임소재를 명확히 하여야 한다.		
점검항목	1) 식별된 정보자산에 대한 책임자 및 관리자(또는 담당자)를 지정하고 있는가?		
신청기관 준비사항 (관련증적)	• 정보자산 분류기준 • 정보자산 목록 (책임자/관리자 지정 현황 포함)	참고사항 (샘플자료)	• 정보보호 정책서 • 정보자산관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ **점검항목 1)**

■ 정보자산 도입, 변경, 폐기, 반출입 등의 책임을 질 수 있는 책임자 및 정보자산을 실제 관리•운영하는 관리자(또는 담당자)를 지정하여 책임소재를 명확하게 하여야 한다.

- 정보자산 별 책임자 및 관리자를 지정하고 자산목록에 기록
- 퇴직, 전보 등 인사이동이 발생하거나 정보자산의 도입, 변경, 폐기 등으로 현황이 변경될 경우 정보자산 별 책임자 및 담당자를 파악하여 자산목록에 반영

통제항목	3.1.3 보안등급 및 취급		
세부통제내용	기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 자산의 보안등급을 부여하고, 보안등급별 취급 절차에 따라 관리하여야 한다.		
점검항목	1) 기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 정보자산의 중요도를 평가하기 위한 기준을 수립하고 있는가? 2) 정보자산별로 중요도를 평가하고 각 자산별 특성에 적합한 보안등급을 부여하고 보안등급을 쉽게 확인할 수 있도록 하고 있는가? 3) 정보자산의 보안등급에 따른 취급절차(생성, 저장, 이용, 파기 등)를 정의하고 이행하고 있는가?		
신청기관 준비사항 (관련증적)	• 정보자산 분류기준 • 정보자산 목록 • 정보자산 보안등급 부여 현황 • 보안등급별 취급 절차 및 보안통제 현황	참고사항 (샘플자료)	• 정보보호 정책서 • 정보자산관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ **점검항목 1)**

■ 정보자산의 유출, 장애 및 침해 발생 시 조직의 업무에 미치는 영향을 고려하여 식별된 정보자산의 중요도를 평가할 수 있도록 기준을 수립하여야 한다.

■ 일반적으로 기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 평가기준을 마련할 수 있다. 그 외에 서비스 영향, 이익손실, 고객 상실, 대외 이미지 등도 추가적으로 고려할 수 있다.

- 정보자산을 대상으로 중요도 평가 기준 수립
- 정보자산 중요도 평가 시 타 자산과의 연관성 고려

⇨ **점검항목 2)**

■ 정보자산 중요도 평가기준에 따라 정보자산별로 중요도를 평가하여야 한다. 또한 정보자산별 특성에 따라 보안등급을 부여하고 다음과 같이 임직원이 보안등급을 쉽게 식별할 수 있도록 하여야 한다.

- (전자)문서 : 기밀, 대외비, 일반 표시
- 서버 등 하드웨어 자산 : 자산번호 또는 바코드 표시를 통한 보안등급 확인

⇨ 점검항목 3)

■ 정보자산의 보안등급에 따라 취급절차(생성, 저장, 이용, 파기 등)를 정의하고 이에 따른 접근통제 등 적절한 보안통제를 이행하여야 한다.

※ 정보자산 보안등급에 따른 보안통제 예시

- 정보자산 분류 및 중요도 평가기준에 따른 보안등급 평가
- 자산 담당자 지정 및 담당자 외의 시스템 접근 제한 등 차별 적용
- 데이터 저장 및 처리, 전송 시 인증 및 권한관리, 암호화, 접근통제, 개인정보 마스킹, 접근기록 생성/보관 등 보안등급 및 저장, 처리, 전송 하는 정보에 따라 차별된 보안통제 적용
- 파기 시 저장매체 내의 중요 데이터를 복구 불가능하도록 삭제 등 차별 조치

3.2 자산 변경관리

통제항목	3.2.1 변경관리		
세부통제내용	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경이 필요한 경우 보안 영향평가를 통해 변경사항을 관리하여야 한다. 또한 이용자에게 큰 영향을 주는 변경에 대해서는 사전에 공지를 하여야 한다.		
점검항목	1) 클라우드 시스템 관련 자산(시설, 장비, 소프트웨어 등) 변경에 관한 절차를 수립•이행하고 있는가? 2) 클라우드 시스템 관련 자산 변경을 수행하기 전 성능 및 보안에 미치는 영향을 분석하고 있는가? 3) 클라우드서비스 관련 자산 변경 중 이용자에게 큰 영향을 주는 변경에 대해서는 사전에 공지하고 있는가?		
신청기관 준비사항 (관련증적)	• 자산 변경 절차 • 변경 요청/승인 이력 • 보안영향평가 결과 • 이용자 고지 이력	참고사항 (샘플자료)	• 정보보호 정책서 • 정보자산관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 운영체제 업그레이드, 상용 소프트웨어 설치, 운영 중인 응용프로그램 기능 개선, 네트워크 구성 변경, CPU/메모리/저장장치 증설 등 정보 시스템 관련 자산 변경이 필요한 경우 변경요청, 책임자 검토•승인, 변경확인, 변경이력관리 등의 공식적인 절차를 수립하고 이행하여야 한다.
- 변경의 규모를 고려하여 영향분석 대상 기준을 자체적으로 정할 수 있다.

■ 다음과 같은 사항은 변경에 포함하여야 한다.
- 시스템 및 보안 구성 변경
- 하드웨어 장치 및 보안 패치
- 소프트웨어 업데이트 등

■ 클라우드시스템 관련 정보자산 변경이 필요한 경우 변경에 따른 보안, 성능, 업무 등에 미치는 영향을 분석하여 변경에 따른 영향을 최소화할 수 있도록 변경을 이행하고 변경 실패에 따른 복구방안을 사전에 고려하여야 한다.
- 변경의 규모를 고려하여 영향분석 대상 자체 선정 가능

⇨ 점검항목 2)

■ 클라우드시스템 관련 정보자산 변경이 필요한 경우 변경에 따른 보안, 성능, 업무 등에 미치는 영향을 분석하여 변경에 따른 영향을 최소화 할 수 있도록 변경을 이행하고 변경 실패에 따른 복구방안을 사전에 고려하여야 한다.

- 변경의 규모를 고려하여 영향 분석 대상 기준을 자체적으로 수립 가능
- 변경에 따른 잠재적 요인들이 시스템 안정성에 미치는 영향 분석

⇨ 점검항목 3)

■ 클라우드서비스 관련 정보자산 변경 시 이용자에게 큰 영향을 주는 변경에 대해서는 사전에 다음의 내용을 이용자에게 공지하여야 한다.

- 변경 내용(자산변경, 작업 등) 및 일시
- 영향 범위
- 긴급연락처 등

통제항목	3.2.2 변경 탐지 및 모니터링		
세부통제내용	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경을 지속적으로 모니터링 하여 허가 받지 않은 변경을 탐지하고 최신의 변경 이력을 유지하여야 한다.		
점검항목	1) 클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경을 지속적으로 모니터링 하여 허가받지 않은 변경을 탐지하고 최신의 변경 이력을 유지하고 있는가?		
신청기관 준비사항 (관련증적)	• 변경이력 내역서 • 변경관리 대장 • 미승인 변경 탐지 방안 (Checksum)	참고사항 (샘플자료)	• 정보보호 정책서 • 정보자산관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ 점검항목 1)

■ 클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)에 대해서 최신 변경이력을 유지하여야 한다.

■ 중요 시스템에 대해서는 보안 모니터링 도구 등을 사용하여 허가받지 않은 변경을 탐지하여야 한다.

통제항목	3.2.3 변경 후 작업검증		
세부통제내용	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경 후에는 보안성 및 호환성 등에 대한 작업 검증을 수행하여야 한다.		
점검항목	1) 클라우드 시스템 관련 자산 변경 후 보안성, 호환성에 대한 작업검증을 수행하고 있는가?		
신청기관 준비사항 (관련증적)	• 보안영향평가 결과 • 작업내역서 • 사전영향 평가서	**참고사항 (샘플자료)**	• 정보보호 정책서 • 정보자산관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 클라우드 시스템 관련 자산 변경 후 클라우드 서비스 영향도, 정상 동작 여부확인 등 보안성, 호환성에 대한 작업 검증을 수행하여야 한다.

3.3 위험관리

통제항목	3.3.1 위험관리계획 수립		
세부통제내용	관리적, 기술적, 물리적, 법적 분야 등 정보보호 전 영역에 대한 위험 식별 및 평가가 가능하도록 위험관리 방법과 계획을 사전에 수립하여야 한다.		
점검항목	1) 관리적, 물리적, 기술적, 법적 분야 등 다양한 측면에서 발생할 수 있는 위험을 식별하고 평가할 수 있는 방법을 정의하여 문서화하고 있는가? 2) 매년 위험관리를 수행하기 위하여 전문 인력 구성, 기간, 대상, 방법, 예산 등을 구체화한 위험관리계획을 수립•이행하고 있는가?		
신청기관 준비사항 (관련증적)	• 위험 평가 방법론 • 위험 평가 계획서	**참고사항 (샘플자료)**	• 정보보호 정책서 • 정보자산관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ **점검항목 1)**

■ 관리적, 기술적, 물리적, 법적 분야 등 조직 전 영역에 대한 위험 식별 및 평가가 가능하도록 각 영역별 특성을 반영한 위험관리 방법을 선정하여야 하며 그 방법과 절차를 지침으로 규정하여야 한다.

※ 클라우드 위험 관리 프로그램 고려사항 예시

- 정보 시스템 자산, 가상화된 정보 시스템과 서비스(적용 가능한 경우) 및 보안 위협과 취약성 식별
- 부정사용 또는 공격의 가능성 추정
- 위험 이벤트와 관련된 잠재적 손실 평가
- 자산 보호를 위한 적절한 보안 대책과 통제 구현

■ 핵심자산에 대한 기술적 위험분석의 경우 상세 위험분석을 수행하는 것이 바람직하다. (자산 중요도, 위협, 취약점 등)

➪ **점검항목 2)**

■ 위험관리 방법 및 절차에 따라 매년 위험관리계획을 수립하고 이행하여야 하며 계획에는 다음과 같은 내용을 포함하여야 한다.

- 위험관리 대상 : 클라우드 서비스를 제공하기 위한 핵심자산 및 서비스를 누락 없이 포함

※ 공공 및 민간 클라우드 서비스 제공을 위해 공동으로 이용하는 자산, 임직원 등이 이용하는 단말기에 공통으로 적용되는 보안통제 솔루션 등에 대해서 클라우드컴퓨팅서비스 제공자가 별도 식별, 위험평가 등을 수행하고 있다면 클라우드 인증에서는 제외 가능

- 위험관리 수행인력 : 위험관리 방법, 조직의 업무 및 시스템에 대한 전문성을 갖춘 인력과 관련 부서 실무책임자가 참여 (위험관리 전문가, 정보보호관리자, 클라우드 서비스 운영자, 현업부서 실무 책임자 등)
- 위험관리 기간 등

통제항목	3.3.2 취약점 점검		
세부통제내용	취약점 점검 정책에 따라 주기적으로 기술적 취약점(예 : 유•무선 네트워크, 운영체제 및 인프라 응용 프로그램 취약점 등)을 점검하고 보완하여야 한다.		
점검항목	1) 클라우드서비스 취약점 점검 절차를 수립하여 연1회 이상 점검을 수행하고 있는가? 2) 인터넷 및 클라우드 서비스 관리 네트워크에서 침투테스트를 실시하고 있는가? 3) 발견된 취약점에 대한 조치를 수행하고 그 결과를 책임자에게 보고하는가?		
신청기관 준비사항 (관련증적)	• 취약점 점검 계획서 • 침투테스트 계획 및 결과 • 취약점 점검 결과보고서 • 취약점 보완 보고서	참고사항 (샘플자료)	• 정보보호 정책서 • 정보자산관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ 점검항목 1)

■ 취약점 점검 정책과 절차를 다음과 같은 내용을 포함하여 수립하여야 한다.
- 취약점 점검 대상 (예 : 서버, 네트워크 장비 등)
- 취약점 점검 주기
- 취약점 점검 담당자 및 책임자 지정
- 취약점 점검 절차 및 방법 등

■ 다음과 같은 내용을 포함하여 취약점 점검을 실시하여야 한다.
- 라우터, 스위치 등 네트워크 장비 구성, 설정 취약점
- 서버 OS, WEB/WAS, DBMS 등에 대한 보안 설정 취약점 및 알려진 취약점
- 방화벽 등 정보보호시스템 취약점
- 애플리케이션 취약점
- 웹 및 모바일 서비스(모바일 앱 등) 취약점
- 사용자 단말기(PC), 스마트 기기 취약점
- 가상 인프라 및 가상 자원 취약점 등
- 소스코드 보안약점 및 형상서버 등
- 인터페이스 및 API 취약점

■ 취약점 점검 시 이력관리가 될 수 있도록 '점검일시', '점검대상', '점검방법', '점검내용 및 결과', '발견사항', '조치사항' 등이 포함된 보고서를 작성하여야 한다.

■ 클라우드 서비스에 대한 취약점 점검을 주기적(연 1회 이상)으로 수행하여야 한다.
- 외부의 취약성 점검 전문업체를 활용하여 취약성 점검을 수행하는 것도 가능하다.

⇨ 점검항목 2)

■ 인터넷 및 클라우드 서비스 관리 네트워크에서 침투테스트를 실시하여야 한다.
- 대상 대상 : 클라우드 서비스 관련 인프라 및 애플리케이션
- 대상 시점 :
  . 중요한 인프라 변경 시
  . 애플리케이션 업데이트 시 등

■ 시스템 변경이 없는 경우, 최소 연1회 이상 침투테스트를 실시하여야 한다.

■ 침투테스트 시 이력관리가 될 수 있도록 '점검일시', '점검대상', '점검방법', '점검내용 및 결과', '발견사항', '조치사항' 등이 포함된 보고서를 작성하여야 한다.

⇨ 점검항목 3)

■ 취약점 점검 결과 발견된 취약점별로 대응방안 및 조치결과를 문서화하여야 하며 조치결과서를 작성하여 책임자에게 보고하여야 한다.
- 불가피하게 조치를 할 수 없는 취약점의 경우 그 사유를 명확하게 확인하고 책임자에게 보고
- 조치 불가능한 취약점에 대해 보고 후에도 대체 보안기능(기능사용 제한, 주기적인 모니터링 등)을 적용하여 해당 취약점으로 인한 위험관리 수행

통제항목	3.3.3 위험분석 및 평가		
세부통제내용	위험관리 방법 및 계획에 따라 정보보호 전 영역에 대한 위험 식별 및 평가를 연 1회 이상 수행하고 그 결과에 따라 수용 가능한 위험수준을 설정하여 관리하여야 한다.		
점검항목	1) 클라우드 서비스 제공과 관련된 전 영역에 대한 위험분석 및 평가를 연 1회 이상 수행하고 있는가? 2) 클라우드 서비스에 악영향을 미친다고 판단될 시 수시로 위험평가를 수행하고 있는가?		
신청기관 준비사항 (관련증적)	• 위험 평가 방법론 • 위험 분류표 • 위험 분석 및 평가 계획서 • 위험 분석 및 평가 결과서	참고사항 (샘플자료)	• 정보보호 정책서
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ **점검항목 1)**

■ 클라우드 서비스 제공과 관련된 전 영역을 대상으로 위험 식별과 평가를 수행하여야 하며 기 적용된 정보보호대책의 실효성 검토도 함께 이루어져야 한다.

■ 다음과 관련된 사항은 위험에 포함되어야 한다.
- 클라우드 관리 방식
- 클라우드 인프라 보안
- 클라우드 운영 관리
- 클라우드 서비스 관리
- 클라우드 사용자 접근
- 가상화로 인한 보안 위험 등

➪ **점검항목 2)**

■ 클라우드 서비스에 악영향을 미치는 취약점 발견 시 수시 위험평가를 수행하여야 한다.
- 서버, WEB/WAS, DBMS, 네트워크 장비, 가상화 관련 인프라, 정보보호시스템 등 클라우드 관련 주요 정보자산에 대해 새로운 취약점 발견 시
- 클라우드시스템 관련 자산 변경 등으로 새로운 취약점 및 위험 발생 시

통제항목	3.3.4 위험처리		
세부통제내용	법규 및 계약관련 요구사항과 위험수용 수준을 고려하여 위험평가 결과에 따라 통제할 수 있는 방법을 선택하여 처리하여야 한다.		
점검항목	1) 위험평가의 결과에 따라 통제할 수 있는 방법을 선택하여 처리하여야 하며, 내외부의 환경 변화에 따른 클라우드 서비스 위험을 지속적으로 모니터링을 할 수 있는 프로세스를 수립 및 이행하고 있는가?		
신청기관 준비사항 (관련증적)	• 정보보호책임자 승인결과 • 위험 분석 및 평가 계획서 • 위험 분석 및 평가 결과서	참고사항 (샘플자료)	• 정보보호 정책서
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 위험평가의 결과 선택된 통제 방법을 적용 및 처리하여야 한다.

- 위험을 완화하기 위한 계획은 중요도에 따라 우선순위 설정
- 또한, 계획은 정보보호책임자(CISO 등)의 승인받아 계획을 수행하는 직원에게 정확히 전달

■ 위험 모니터링 및 처리에 대한 프로세스 및 계획을 수립 및 이행하여야 한다.

- 주요 시스템에 대한 모니터링 검토는 최소 월 1회 실시
- 이상 징후의 유형은 시스템 로그의 검토와 최근동향을 고려하여 수립

4. 서비스 공급망 관리

4.1 공급망 관리 정책

통제항목	4.1.1 공급망 관리 정책 수립		
세부통제내용	클라우드컴퓨팅서비스에 대한 접근과 서비스 연속성을 저해하는 위험을 식별하고 최소화하기 위해 공급망과 관련한 보안 요구사항을 정의하는 관리정책을 수립하여야 한다.		
점검항목	1) 클라우드컴퓨팅서비스에 대한 접근과 서비스 연속성을 저해하는 위험을 식별하고 있는가? 2) 식별된 위험을 최소화하기 위한 보안 요구사항을 포함하는 공급망 관리정책을 수립하고 있는가?		
신청기관 준비사항 (관련증적)	• 공급망 현황 • 공급망 계약서 • 공급망의 연속성 저해 가능 위험	**참고사항 (샘플자료)**	• 정보보호 정책서 • 외부자 또는 공급망관리 지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 클라우드서비스 제공자는 클라우드서비스에 대한 접근과 서비스 연속성을 저해할 수 있는 공급망 상의 이해관계자 및 위험을 식별하여야 한다.

- 공급망 상의 이해관계자와 맺은 계약 관계에 따른 위험 식별
- 데이터 및 시설, 서비스에 대해 분실, 도난, 유출, 위조, 변조, 훼손 등의 발생 가능성 검토
- 처리되는 데이터의 종류, 네트워크 환경, 오피스 환경 등으로 인한 위험 식별

※ 공급망의 정의

- 기업이 부품, 원자재 등 재료를 획득하고 이를 제품 및 서비스로 변환하여 고객에게 유통시키는 프로세스의 네트워크
- 참여자 : 고객, 생산업체, 부품 및 원자재 공급업체, 유통업체, 보안매니지드사, 운영위탁사 등

⇨ **점검항목 2)**

■ 식별된 위험을 최소화하기 위한 보안요구사항을 포함한 공급망 관리대책을 수립하여야 한다.

- 데이터의 유출, 위조, 변조, 훼손 위험을 최소화하기 위한 기술적인 보안대책
- 공급망 상의 이해관계자와 맺은 계약의 범위에서 발생 가능한 위험을 최소화하기 위한 보안대책
- 외부 위탁으로 인한 위험을 최소화하기 위한 보안대책
- 시설 및 설비, 서비스, 네트워크 등의 장애로 인한 위험을 최소화하기 위한 보안대책

통제항목	4.1.2 공급망 계약		
세부통제내용	클라우드컴퓨팅서비스 범위 및 보안 요구사항을 포함하는 공급망 계약을 체결하고 다자간 협약시 책임을 개별 계약서에 각각 명시해야 하며, 해당 서비스에 관련된 모든 이해관계자에게 적용하여야 한다.		
점검항목	1) 클라우드서비스 범위 및 보안 요구사항을 공급망 계약에 포함하고 다자간 협약 시 각각의 역할과 책임을 명시하고 있는가?		
신청기관 준비사항 (관련증적)	• 공급망 계약서, 협약서, 부속서 등 (역할 및 책임 명시)	참고사항 (샘플자료)	• 정보보호 정책서 • 외부자 또는 공급망관리 지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 공급망 계약 체결 시 서비스의 범위 및 수립된 보안요구사항을 계약서에 반영하여야 한다.

- 제공자가 제공하는 서비스의 범위
- 역할과 책임
- 제공자가 준수해야 하는 보안요구사항
- 문제 발생 시 대책 및 법적 책임 등 포함

■ 식별된 위험을 해결하기 위한 사항이 계약에 반영되어야 한다.

■ 다자간 협약을 맺는 경우 각각의 역할 및 책임을 명시하여야 한다.

- 협약에 포함된 당사자들의 역할 및 책임을 개별 계약서마다 명시하여야 한다.

※ 클라우드서비스파트너(SW 제공업체)와 계약 시 포함되는 내용 예시

- 기능적, 기술적 보안 요구사항의 반영 여부
- 개발 보안 가이드 준수 여부(시큐어 코딩 등)
- 테스트 시 보안 요구사항 준수 여부
- 개발 완료된 시스템에 대한 취약점 점검 등 수행 여부
- 개발인력 대상 SW개발 보안교육 여부

■ 공공기관의 보안요구사항은 계약서, SLA 등에 반영하여 명시하여야 한다.

- 계약서, SLA 등에 명시된 요구사항은 클라우드컴퓨팅서비스 제공자의 정보보호대책에 구현되어야 함

. 공공기관 클라우드 서비스 운영장소/관련 망은 공공기관 내부 정보시스템에 준하여 보안관리

. 공공기관 클라우드 서비스에 대한 업무 연속성 유지, 안전성 유지 등의 원활한 운영에 대한 클라우드 서비스 제공자의 책임 명시

. 공공기관 클라우드시스템 구축에 도입된 서버, PC, 가상화 솔루션 및 정보보호 제품 중 CC인증이 필수적인 제품군은 CC인증을 받은 제품 도입

. 공공기관 클라우드 서비스의 물리적 위치는 국내로 한정

- 공공기관이 보안요구사항의 준수여부에 대한 증거를 요구하는 경우 관련 자료를 제공하여야 함

4.2 공급망 변경관리

통제항목	4.2.1 공급망 변경 관리		
세부통제내용	정보보호 정책, 절차 및 통제에 대한 수정 및 개선이 필요하다고 판단될 경우 서비스 공급망 상에 발생할 수 있는 위험에 대한 검토를 통해 안전성을 확보 후 계약서 내용 변경 방안을 제시하여야 한다.		
점검항목	1) 공급망 변경과 관련하여 계약서 등을 공급망 상의 이해관계자들에게 제시하고 있는가? 2) 안전성 확보를 위해 필요시 클라우드 공급망에 대한 보안위험을 재평가하고 있는가?		
신청기관 준비사항 (관련증적)	• 공급망 계약서 • 계약변경관리 절차 • 공급망 위험 검토 결과	참고사항 (샘플자료)	• 정보보호 정책서 • 외부자 또는 공급망관리 지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ **점검항목 1)**

■ 사고발생 시 계약해지 및 재계약 통제 등 제재 사항을 포함하는 협력사 변경 가능에 대해 계약서에 명시하고 이를 공급망 상 이해관계자들에게 제시하여야 한다.

※ 계약해지 및 재계약 통제 등 제재 사항 적용 사유 예시

- 제공자가 정당한 사유 없이 서비스를 시작하지 아니한 경우
- 제공자가 서비스 계약에 따른 계약 조건을 이행하지 아니한 경우
- 제공자가 서비스수준협약서에 협의된 목표 수준에 미달되어 개선될 가능성이 없는 경우
- 제공자가 제공하는 서비스가 제안서 및 수행계획과 다르거나 뚜렷하게 차이가 있는 경우 등

➪ **점검항목 2)**

■ 공급망 변경 시 안전성 확보를 위해 필요 시 클라우드 공급망에 대한 보안위험을 재평가하여야 한다.

- 제공자의 임직원이 접근 가능한 정보 및 정보처리 시설 식별, 접근 형태 분석
- 접근 가능한 자산의 중요도 및 보호대책
- 정보자산에 대한 접근방법, 권한 승인 절차
- 변경 관리 절차 및 보고 체계
- 제공자의 임직원 적격성 및 교육 훈련 보장

통제항목	4.2.2 공급망 모니터링 및 검토		
세부통제내용	클라우드컴퓨팅서비스 공급망 상에서 발생하는 기록 및 보고서는 정기적으로 모니터링 및 검토하여야 한다.		
점검항목	1) 서비스 수준 협약의 요구사항에 대한 준수 여부를 모니터링 가능한 체계를 수립하고 주기적으로 검토하고 있는가?		
신청기관 준비사항 (관련증적)	• 공급망 계약서 • 공급망 보안요구사항 • 공급망 위험 검토 결과 • 공급망 운영보고서	참고사항 (샘플자료)	• 정보보호 정책서
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 클라우드컴퓨팅서비스 공급망 상에서 합의된 보안요구사항의 준수 여부를 확인하기 위한 절차를 마련하여야 한다.

- 공급망 서비스 목록 작성 (서비스 내용 및 처리하는 정보 유형, 개인정보 또는 민감정보처리 유무 등)
- 서비스 수준 협약 내의 보안요구사항
- 민감한 데이터 처리 합의
- 정기 운영보고서 검토 또는 실사
- 정기적으로 모니터링 및 검토 수행 등

5. 침해사고 관리

5.1 침해사고 대응 절차 및 체계

통제항목	5.1.1 침해사고 대응 절차 수립		
세부통제내용	침해사고에 대한 효율적이고 효과적인 대응을 위해 신고절차, 유출 금지 대상, 사고 처리 절차 등을 담은 침해사고 대응절차를 마련하여야 한다. 침해사고 대응절차는 이용자와 제공자의 책임과 절차가 포함되어야 한다.		
점검항목	1) 침해사고의 정의 및 범위, 긴급연락체계 구축, 침해사고 발생 시 보고 및 대응절차, 침해사고 대응조직의 구성 등을 포함한 침해사고 대응절차를 수립하고 있는가?		
신청기관 준비사항 (관련증적)	• 침해사고 관리지침 • 침해사고 대응절차 • 침해사고 대응조직	참고사항 (샘플자료)	• 정보보호 정책서 • 침해사고 관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

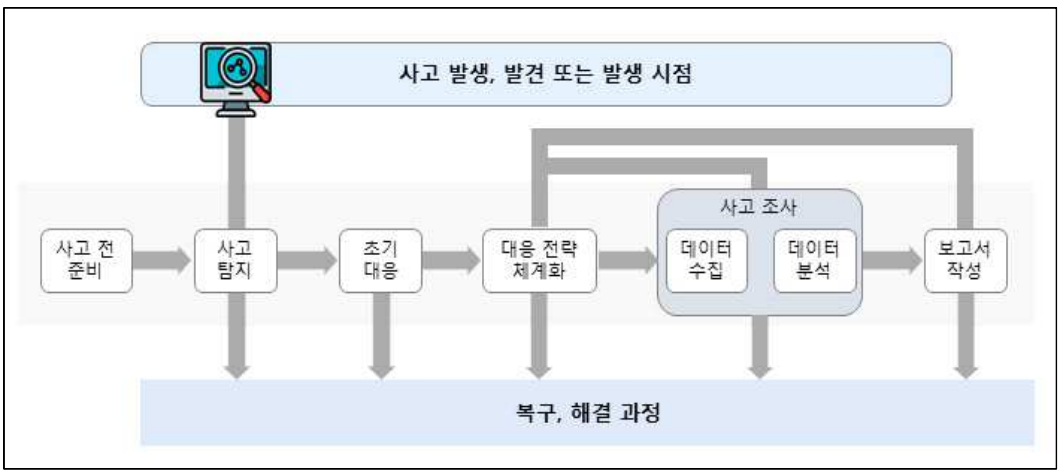
점검항목 해설

➪ 점검항목 1)

■ 다음의 내용을 포함하여 침해사고대응절차를 수립하여야 한다.

- 침해사고의 정의 및 범위 (중요도 및 유형 포함)
- 비상연락체계
- 침해사고 발생 시 기록, 보고 절차
- 침해사고 신고 및 통지 절차 (관계기관, 이용자 등)
- 침해사고 대응 절차 (대응조직 구성 및 구성원의 역할과 책임 포함)

※ 침해사고대응절차 예시



분류	설명
사고 전 준비 과정	사고가 발생하기 전 침해사고 대응팀과 조직적인 대응을 준비
사고 탐지	정보보호 및 네트워크 장비에 의한 이상 징후 탐지. 관리자에 의한 침해사고의 식별
초기 대응	초기 조사 수행, 사고 정황에 대한 기본적인 세부사항 기록, 사고대응팀 신고 및 소집, 침해사고 관련 부서에 통지
대응 전략 체계화	최적의 전략을 결정하고 관리자 승인을 획득, 초기 조사 결과를 참고하여 소송이 필요한' 사항인지를 결정하여 사고 조사 과정에 수사기관 공조 여부를 판단
사고 조사	데이터 수집 및 분석을 통하여 수행. 언제, 누가, 어떻게 사고가 일어났는지, 피해 확산 및 사고 재발을 어떻게 방지할 것인지를 결정
보고서 작성	의사 결정자가 쉽게 이해할 수 있는 형태로 사고에 대한 정확한 보고서 작성
재발방지	차기 유사 공격을 식별 및 예방하기 위한 보안정책의 수립, 절차 변경, 사건의 기록, 장기 보안정책 수립, 기술 수정 계획수립 등을 결정

통제항목	5.1.2 침해사고 대응 체계 구축		
세부통제내용	침해사고 정보를 수집•분석•대응할 수 있는 보안관제 시스템 및 조직을 구성•운영하고, 침해사고 유형 및 중요도에 따라 보고 및 협력체계를 구축하여야 한다.		
점검항목	1) 침해사고를 모니터링 하여 신속하게 대응할 수 있도록 모니터링 및 대응 방법, 절차, 대응조직 및 인력, 보고 및 승인 방법 등을 포함한 중앙 집중적인 대응체계를 수립하고 있는가? 2) 침해사고 유형, 중요도, 긴급성 등에 따라 분류하고 이에 따른 보고 체계를 정의하고 있는가? 3) 외부 관제시스템 업체 등 외부 기관을 통해 침해사고 대응체계를 구축•운영하는 경우 보안사고 대응 절차의 세부사항을 계약서에 반영하고 있는가? 4) 침해사고의 모니터링, 대응 및 처리와 관련된 정부 부처, 외부전문가, 전문 업체, 전문기관(KISA) 등과의 협조체계를 수립하고 있는가?		
신청기관 준비사항 (관련증적)	• 침해사고 관리지침 • 외부 관제 용역 계약서 • 침해사고 대응조직 • 비상연락망(외부기관 포함) • 침해사고 유형 및 중요도 분류 • 침해사고 모니터링 및 대응 조직, 방법, 절차 • 관제 보고서	참고사항 (샘플자료)	• 정보보호 정책서 • 침해사고 관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ **점검항목 1)**

■ 침해사고를 모니터링하고 신속하게 대응할 수 있도록 중앙 집중적인 대응체계를 수립하여야 한다.

- 모니터링 및 대응 방법, 절차
- 대응 조직 및 인력
- 침해사고 보고 및 승인 절차 등

■ 자체적으로 보안관제 시스템을 구축하거나 외부 전문 업체와의 계약을 통해 보안관제 시스템을 구축할 수 있다.

- 외부의 전문 업체를 활용하여 보안관제 시스템을 구축하는 경우 별도의 조직 구성 불필요

➪ **점검항목 2)**

■ 침해사고 유형 및 중요도를 분류하고 이에 따른 보고체계를 정의하여야 한다.

➪ **점검항목 3)**

■ 외부 보안관제 업체와 계약을 맺는 경우 수립된 침해사고대응절차의 내용을 계약서에 반영하여야 한다.

- 침해사고대응절차를 계약서, SLA, RFP 등에 반영
- 침해사고대응절차 내에 보안관제 업체와 서비스 제공자 간의 역할 정의
- 모니터링, 이벤트 등 수집 및 분석, 상황전파, 보안 이슈 및 업계동향 보고, 침해사고 원인 파악 및 피해 분석, 복구 방안 강구 등에 대한 범위 및 역할 정의

➪ **점검항목 4)**

■ 침해사고의 모니터링, 대응 및 처리와 관련된 외부전문가, 전문 업체, 전문기관(KISA) 등과의 연락 및 협조체계를 수립하여야 한다.

- 외부 전문기관과의 비상연락망 유지 등 연락체계를 구축하고 담당자, 연락처 등의 정보를 최신으로 유지
- 자체 긴급연락망 등을 수립
- 침해사고 발생 시 관련 책임자들에게 핫라인 등을 통해 즉각 통지

통제항목	5.1.3 침해사고 대응 훈련 및 점검		
세부통제내용	침해사고 대응과 관련된 역할 및 책임이 있는 담당자를 훈련시켜야 하고, 주기적으로 침해사고 대응 능력을 점검하여야 한다.		
점검항목	1) 침해사고 대응 절차에 관한 년1회 이상 모의훈련 계획을 수립하고 이에 따라 주기적으로 훈련을 실시하고 있는가? 2) 침해사고 대응 모의훈련 결과를 이용자가 요청할 경우 이를 문서화하여 제공하고 있는가?		
신청기관 준비사항 (관련증적)	• 모의훈련 계획서 • 모의훈련 결과보고서 • 침해사고 대응 절차	참고사항 (샘플자료)	• 정보보호 정책서 • 침해사고관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ **점검항목 1)**

■ 정보보호 담당자는 침해사고 발생 시 신속하게 대응하기 위해 매년 모의훈련 계획을 수립하고 이를 시행하여야 한다.

- 침해사고 대응 인력이 모두 포함될 수 있도록 모의훈련 계획을 수립
- 모의훈련 계획은 침해사고 대응과 관련된 담당자의 훈련이 될 수 있도록 문서화하여 책임자의 승인을 받은 후 시행
- 모의훈련 완료 후 결과보고서를 작성하여 보고
- 모의훈련 결과 대응체계의 변경이 필요한 경우 반영 (절차, 문서, 조직, 시스템 등)
- 다양한 모의훈련 시나리오를 수립하여 상황별 신속 대응 능력 향상

➪ **점검항목 2)**

■ 클라우드 서비스를 이용하는 이용자가 모의훈련에 대한 결과를 요청할 경우 모의훈련 결과를 문서화하여 제공하여야 한다.

- 이용자가 요청할 경우 모의훈련 결과를 문서로 제공받을 수 있다는 이용자의 권리를 계약서 또는 SLA 등에 포함

5.2 침해사고 대응

통제항목	5.2.1 침해사고 보고		
세부통제내용	침해사고 발생 시 침해사고 대응 절차에 따라 법적 통지 및 신고 의무를 준수하여야 한다. 또한 클라우드컴퓨팅서비스 이용자에게 발생 내용, 원인, 조치 현황 등을 신속하게 알려야 한다.		
점검항목	1) 침해사고의 징후 또는 침해사고 발생을 인지한 경우 정의된 침해사고 보고절차에 따라 신속하게 보고가 이루어지고 있는가? 2) 침해사고보고서에는 사고 날짜, 사고 내용 등 필요 내용을 모두 포함하고 있는가? 3) 침해사고 발생 시 관련 법률 및 규정에 따라 신고, 통지하는 절차를 따르고 있는가?		
신청기관 준비사항 (관련증적)	• 침해사고 보고서 • 침해사고 관리대장 • 비상연락망 • 침해사고 보고 및 통지 절차 • 침해사고 발생 시 신고, 통지 내용(항목/서식)	**참고사항 (샘플자료)**	• 정보보호 정책서 • 침해사고 관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ **점검항목 1)**

■ 침해사고 징후 또는 침해사고를 인지한 경우 보고절차에 따라 신속하게 보고하여야 한다.

- 침해사고 초기 대응 및 증거 보존 조치
- 접속권한 삭제 및 변경 또는 접속 차단
- 대내외 시스템 보안점검 및 취약점 보완조치
- 침해사고 발생원인(경로) 등

⇨ **점검항목 2)**

■ 침해사고 발생 시 다음 내용을 포함한 침해사고보고서를 작성하여야 한다.

- 침해사고 발생일시
- 보고자와 보고일시
- 사고 내용 (발견사항, 피해 내용 등)
- 사고대응 경과 내용
- 사고대응까지의 소요시간 등

➪ **점검항목 3)**

■ 아래와 같은 침해사고 발생 시 법률이나 규정 등에 따라 관계기관에 신고하여야 하며 개인정보와 관련한 침해사고는 이용자(정보주체)에게 신속하게 통지하여야 한다.

- 개인정보 유출 신고 (1천명 이상 또는 단 1건 이상)
- 침해사고 신고
- 클라우드컴퓨팅서비스 관련 시스템 상의 침해사고 및 이용자 정보 유출, 서비스 중단 등 발생 시 신고
- 통지내용, 통지시점, 통지방법, 통지주체 등에 대해 사전 정의

※ 이용자 정보

- 이용자의 개인정보를 포함하여 클라우드컴퓨팅서비스에서 생산, 저장, 관리되는 이용자의 정보

※ 사고발생 시 신고기관 및 이용자 통지방법

구분	개인정보 유출 신고		침해사고 신고	침해사고 신고 및 이용자 정보 유출 등
근거	개인정보보호법 제34조	개인정보보호법 제39조의4	정보통신망법 제48조의3	클라우드컴퓨팅법
대상	개인정보처리자 (공공 및 민간기업) 정보통신서비스 제공자 제외	정보통신서비스 제공자 제공자로부터 개인정보를 제공받은 자	정보통신서비스 제공자 집적정보통신시설 사업자	클라우드컴퓨팅서비스 제공자
신고기관	개인정보보호위원회 한국인터넷진흥원 (온라인 개인정보보호 포털: https://www.privacy.go.kr/wcp/dcl/spl/splRptInfo.do)		과기정통부 한국인터넷진흥원 (보호나라: https://www.boho.or.kr)	과기정통부 한국인터넷진흥원 (클라우드인증팀, cloud@kisa.or.kr)
신고기준	1천명 이상의 정보주체의 개인정보 유출 시	1건이라도 정보주체의 개인정보 유출 시		침해사고 신고 이용자 정보 유출 서비스 중단
신고기한	지체 없이	지체 없이 (24시간 이내)	즉시	즉시
통지방법	서면 등 방법	서면 등 방법		전화, 휴대전화, 우편, 전자우편, 문자메시지, 클라우드컴퓨팅서비스 접속화면 게시 또는 이와 유사한 방법 컴퓨팅서비스 접속화면을 통해 알리는 경우 15일 이상 게시
통지내용	1. 유출된 개인정보의 항목 2. 유출된 시점과 그 경위 3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보 4. 개인정보처리자의 대응조치 및 피해 구제절차 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처	1. 유출 등이 된 개인정보 항목 2. 유출 등이 발생한 시점 3. 이용자가 취할 수 있는 조치 4. 정보통신서비스 제공자 등의 대응 조치 5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처		1. 발생 내용 2. 발생 원인 3. 클라우드컴퓨팅서비스 제공자의 피해 확산 방지 조치 현황 4. 클라우드컴퓨팅서비스 이용자(이하 “이용자“라 한다)의 피해 예방 또는 확산 방지 방법 5. 담당부서 및 연락처

- 클라우드컴퓨팅서비스 제공자가 침해사고에 의해 이용자 개인정보가 유출되었을 경우, 각각 해당 신고기관에 별도 신고하여야 함

※ 이용자 정보 유출 등 발생 시 정보주체(이용자) 통지 기준

구분	내용
통지내용	발생 내용 발생원인(확인된 경우 지체 없이 통지) 클라우드컴퓨팅서비스 제공자의 피해 확산 방지 조치 현황 클라우드컴퓨팅서비스 이용자의 피해 예방 또는 확산 방지 방법 담당부서 및 연락처
통지 시점	지체 없이
통지 방법*	전화 휴대전화 우편 전자우편 문자메시지 클라우드컴퓨팅서비스 접속화면 (15일 이상 게시) 또는 이와 유사한 방법 중 어느 하나 이상의 방법

** (예외사항) 천재지변이나 그 밖의 불가피한 사유로 상기 통지방법으로 통지가 곤란한 경우에는 「신문 등의 진흥에 관한 법률」 제2조제1호가목에 따른 전국을 보급지역으로 하는 둘 이상의 일반 일간신문에 1회 이상 공고하는 것으로 갈음할 수 있음 (이 경우, 그 사유와 공고 내용을 지체 없이 문서(전자문서를 포함)로 과학기술정보통신부에 통보하여야 함)*

통제항목	5.2.2 침해사고 처리 및 복구		
세부통제내용	침해사고 발생 시 침해사고 대응 절차에 따라 처리와 복구를 신속하게 수행하여야 한다.		
점검항목	1) 침해사고가 발생한 경우 절차에 따라 처리 및 복구를 수행하고 그 기록을 남기고 있는가? 2) 침해사고 대응에 대한 이용자의 요청이 발생되는 경우 침해사고 대응 지원을 할 수 있는 체계를 마련하고 있는가?		
신청기관 준비사항 (관련증적)	• 침해사고 대응 결과보고서 • 침해사고 관리대장 • 침해사고 대응절차 (이용자 요청 지원 포함)	참고사항 (샘플자료)	• 정보보호 정책서 • 침해사고 관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 침해사고 처리와 복구 절차에 따라 침해사고 발생 원인을 파악하고 해당 원인을 제거하는 등 기술적, 관리적 대응 조치를 수행하여야 한다.

■ 침해사고 처리를 완료 후 다음의 내용을 포함한 침해사고 대응결과보고서를 작성하여야 한다.

- 처리 및 복구 일시
- 담당자
- 처리 및 복구 방법
- 처리 및 복구 수행 경과 내용

(예 : 시작부터 종료까지 시간 순으로 작성)

⇨ 점검항목 2)

■ 이용자의 침해사고 대응 요청이 있는 경우 자문, 지원 등 침해사고 대응 지원을 제공하여야 한다.

5.3 사후관리

통제항목	5.3.1 침해사고 분석 및 공유		
세부통제내용	침해사고가 처리 및 종결된 후 발생 원인을 분석하고 그 결과를 이용자에게 알려야 한다. 또한 유사한 침해사고에 대한 신속한 처리를 위해 침해사고 관련 정보 및 발견된 취약점을 관련 조직 및 임직원과 공유하여야 한다.		
점검항목	1) 침해사고가 종결된 후 사고의 원인을 분석하고 그 결과를 이용자에게 고지하고 있는가? 2) 침해사고 정보와 발견된 취약점을 관련 조직 및 인력과 공유하고 있는가?		
신청기관 준비사항 (관련증적)	• 침해사고 관련 이용자 고지 내역 (항목/서식) • 침해사고 대응 결과보고서 • 침해사고 대응절차 (공유)	참고사항 (샘플자료)	• 정보보호 정책서 • 침해사고 관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ **점검항목 1)**

■ 침해사고가 처리되고 종결된 후 사고의 원인을 분석하고 분석결과를 이용자에게 고지하여야 한다.

- 전화, 휴대전화, 우편, 문자메시지, 전자 우편 또는 홈페이지 등을 통해 이용자에게 고지

➪ **점검항목 2)**

■ 침해사고 정보와 발견된 취약점을 관련 조직 및 인력과 공유하여야 한다.

- 침해사고 정보와 발견된 취약점 및 원인, 조치방안 등
- 해당 취약점에 대한 기술적 또는 관리적 대응방안 등

통제항목	5.3.2 재발방지		
세부통제내용	침해사고 관련 정보를 활용하여 유사한 침해사고가 반복되지 않도록 침해사고 재발방지 대책을 수립하고, 필요한 경우 침해사고 대응 체계도 변경하여야 한다.		
점검항목	1) 침해사고 분석을 통해 얻어진 정보를 활용하여 유사 사고가 재발하지 않도록 대책을 수립하고 필요한 경우 침해사고 대응절차 등을 변경하고 있는가?		
신청기관 준비사항 (관련증적)	• 침해사고 재발방지 대책 • 임직원 인식 개선 교육 등 활동	참고사항 (샘플자료)	• 정보보호 정책서 • 침해사고 관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 침해사고 분석을 통해 득(得)한 정보를 활용하여 유사 사고가 반복되지 않도록 하는 재발방지 대책을 수립하여야 한다.

- 침해사고 처리 완료 후 발생 원인에 대한 재발방지 대책 수립
- 수립된 재발방지 대책을 관련 임직원에게 공유 및 교육 실시
- 유사 사고가 발생하지 않도록 발견된 취약점 제거

■ 분석된 결과에 따라 필요한 경우 침해사고 대응 절차, 정보보호 정책 및 절차 등의 사고대응체계 변경을 수행하여야 한다.

- 정보보호 정책 및 절차, 침해사고 대응 절차 변경 시 임직원에게 변경 내용에 대해 교육
- 지속적인 임직원의 정보보호 인식 개선 활동 필요

※ 임직원 정보보호 인식 개선 활동 예시, 침해사고 재발방지 교육 수행

날짜	시간	내용	강사
2019.06.01	13:00 ~ 13:50	정보 유출사고 분석 결과 및 재발방지 교육	정보보호 담당자
	14:00 ~ 14:50	침해사고 대응절차 및 정보보호정책/절차 변경 내용 교육	정보보호 담당자
	15:00 ~ 15:50	정보 유출사고 시 법률적 대응방안	외부전문가

6. 서비스 연속성 관리

6.1 장애대응

통제항목	6.1.1 장애 대응절차 수립		
세부통제내용	관련 법률에서 규정한 클라우드컴퓨팅서비스의 중단으로부터 업무 연속성을 보장하기 위해 백업, 복구 등을 포함하는 장애 대응 절차를 마련하여야 한다.		
점검항목	1) 클라우드 시스템 장애를 즉시 인지하고 대응하기 위한 절차를 수립 • 이행하고 있는가?		
신청기관 준비사항 (관련증적)	• 장애대응 매뉴얼 및 절차 • 비상연락망	**참고사항 (샘플자료)**	• 정보보호 정책서 • 서비스연속성관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ **점검항목 1)**

■ 클라우드컴퓨팅서비스 장애 발생 시 즉각 대응할 수 있는 장애 대응절차를 수립하여야 한다.

- 장애대응절차에는 장애보고, 장애탐지 및 복구, 재발방지, 백업 및 복구 관련 절차 포함
  - 백업 대상, 백업담당자 지정, 백업 주기 및 보존기한, 백업 매체 관리, 복구 테스트, 복구 절차 등
- 장애대응 매뉴얼 및 절차는 매년 정기적으로 점검하고 업데이트 수행

■ 장애 대응절차는 발생 가능한 장애의 유형과 장애의 심각도에 따라 대응할 수 있도록 상세한 절차가 포함되도록 작성한다.

- 장애 유형 및 심각도 정의
- 장애 유형 및 심각도별 보고절차 (재발방지 대책 포함)
- 장애 유형별 탐지 방법 수립 : NMS 등 관리시스템 활용
- 장애대응 및 복구에 관한 책임과 역할 정의
- 장애 유형별 대응 및 복구절차
- 장애 기록 및 분석
- 데이터 백업 및 복구 절차
- 장애에 따른 이용자 통지 및 관계 기관 통보 절차
- 비상연락체계(유지보수업체, 정보 시스템 제조사) 등

※ 장애 유형 예시

관점	유형 예시
프로세스 관점	장애, 문제, 알려진 오류
발생 원인 관점	인적 장애, 자연 장애 시스템 장애, 기반 구조 장애, 기술적 장애, 운영 장애
위협 요소 관점	조직 내부인의 장애, 조직 외부인의 장애, 불규칙적 장애, 규칙적 장애
발생 위치 관점	Data, Process, System, Network 사람, 환경, 기타 유형 무형 자산

※ 장애 분류 및 대응방안

<table>
<tr><th>통제</th><th colspan="3">재해 및 장애</th><th>재해 및 장애의 요인</th><th>장애 대응방안</th></tr>
<tr><td rowspan="2">통제
불가능
요인</td><td colspan="3">자연 재해</td><td>화재(전산실, 사무실), 지진 및 지반침하, 수재, 태풍 등</td><td>재해복구센터 구축을 통한 기기 및 프로그램의 이중화
데이터 백업 및 소산</td></tr>
<tr><td colspan="3">인적 재해</td><td>파업, 폭동, 테러 등</td><td rowspan="2">백업 또는 대체요원 확보</td></tr>
<tr><td rowspan="3">통제
가능
요인</td><td colspan="2">인적 장애</td><td rowspan="2">운영
장애</td><td>시스템운영실수, 단말기 및 저장매체의 파괴 및 절취, 외부 공격자의 침입, 컴퓨터 바이러스의 피해, 자료누출 등</td></tr>
<tr><td rowspan="2">기술적
장애</td><td>시스템
장애</td><td>운영체제 결함, 응용프로그램의 결함, 통신프로토콜의 결함, 통신소프트웨어의 결함, 하드웨어의 손상 등</td><td rowspan="2">전산기기 이중화 및 프로그램 변경통제 강화
재해복구 센터 구축을 통한 기기 및 프로그램의 이중화
통신망 이중화
전력공급 중단에 대비한 무정전설비(UPS) 및 발전설비 구축</td></tr>
<tr><td colspan="2">기반구조
장애</td><td>정전사고, 단수, 설비 장애(항온항습, 공기정화시설, 통신시설, 발전기, 공조기 등), 건물의 손상 등</td></tr>
</table>

통제항목	6.1.2 장애 보고		
세부통제내용	클라우드컴퓨팅서비스 중단이나 피해가 발생 시 장애 대응절차에 따라 법적 통지 및 신고 의무를 준수하여야 한다. 또한 클라우드컴퓨팅서비스 이용자에게도 발생 내용, 원인, 조치 현황 등을 신속하게 알려야 한다.		
점검항목	1) 장애 대응절차에 클라우드 서비스 중단이나 피해 발생 시 법적 통지 및 신고 의무에 따른 장애보고절차가 마련되어 있는가?		
신청기관 준비사항 (관련증적)	• 장애대응 매뉴얼 및 절차 • 신고 및 통보 내역 (서식/항목) • 장애관리 현황(대장)	참고사항 (샘플자료)	• 정보보호 정책서 • 서비스연속성관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 클라우드컴퓨팅 서비스 중단이나 피해발생 시 법적 통지 및 신고 의무를 준수할 수 있도록 관련 사항을 포함하여 장애대응절차를 수립하여야 한다.

※ 장애대응 절차에서 장애 발생 시 이용자에게 통지해야 하는 사항에 대한 참고

○ 클라우드컴퓨팅법 시행령 제16조(통지가 필요한 클라우드컴퓨팅서비스의 중단 기간)
1. 클라우드컴퓨팅서비스의 중단 기간이 연속해서 10분 이상인 경우
2. 클라우드컴퓨팅서비스의 중단 사고가 발생한 때부터 24시간 이내에 클라우드컴퓨팅서비스가 2회 이상 중단된 경우로서 그 중단된 기간을 합하여 15분 이상인 경우

○ 클라우드컴퓨팅법 시행령 제17조(통지의 내용 및 방법)
1. 발생내용
2. 발생원인
3. 클라우드컴퓨팅서비스 제공자의 피해 확산 방지 조치 현황
4. 클라우드컴퓨팅서비스 이용자의 피해 예방 또는 확산 방지 방법
5. 담당부서 및 연락처

** (예외사항) 천재지변이나 그 밖의 불가피한 사유로 상기 통지방법으로 통지가 곤란한 경우에는 「신문 등의 진흥에 관한 법률」 제2조제1호가목에 따른 전국을 보급지역으로 하는 둘 이상의 일반 일간신문에 1회 이상 공고하는 것으로 갈음할 수 있음 (이 경우, 그 사유와 공고 내용을 지체 없이 문서(전자문서를 포함)로 과학기술정보통신부에 통보하여야 함)*

※ 서비스 중단 사고발생 시 신고 및 통지

구분	개인정보 유출 신고		침해사고 신고	침해사고 신고 및 이용자 정보 유출 등
근거	개인정보보호법 제34조	개인정보보호법 제39조의4	정보통신망법 제48조의3	클라우드컴퓨팅법
대상	개인정보처리자 (공공 및 민간기업) 정보통신서비스 제공자 제외	정보통신서비스 제공자 제공자로부터 개인정보를 제공받은 자	정보통신서비스 제공자 집적정보통신시설 사업자	클라우드컴퓨팅서비스 제공자
신고 기관	개인정보보호위원회 한국인터넷진흥원 (온라인 개인정보보호 포털: https://www.privacy.go.kr/wcp/dcl/spl/splRptInfo.do)		과기정통부 한국인터넷진흥원 (보호나라: https://www.boho.or.kr)	과기정통부 한국인터넷진흥원 (클라우드인증팀, cloud@kisa.or.kr)
신고 기준	1천명 이상의 정보주체의 개인정보 유출 시	1건이라도 정보주체의 개인정보 유출 시		침해사고 신고 이용자 정보 유출 서비스 중단
신고 기한	지체 없이	지체 없이 (24시간 이내)	즉시	즉시
통지 방법	서면 등 방법	서면 등 방법		전화, 휴대전화, 우편, 전자우편, 문자메시지, 클라우드컴퓨팅서비스 접속화면 게시 또는 이와 유사한 방법 컴퓨팅서비스 접속화면을 통해 알리는 경우 15일 이상 게시
통지 내용	1. 유출된 개인정보의 항목 2. 유출된 시점과 그 경위 3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보 4. 개인정보처리자의 대응조치 및 피해 구제절차 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처	1. 유출 등이 된 개인정보 항목 2. 유출 등이 발생한 시점 3. 이용자가 취할 수 있는 조치 4. 정보통신서비스 제공자 등의 대응 조치 5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처		1. 발생 내용 2. 발생 원인 3. 클라우드컴퓨팅서비스 제공자의 피해 확산 방지 조치 현황 4. 클라우드컴퓨팅서비스 이용자(이하 “이용자“라 한다)의 피해 예방 또는 확산 방지 방법 5. 담당부서 및 연락처

통제항목	6.1.3 장애 처리 및 복구		
세부통제내용	클라우드컴퓨팅서비스 중단이나 피해가 발생할 경우, 서비스 수준 협약(SLA)에 명시된 시간 내에 장애 대응절차에 따라 해당 서비스의 장애를 처리하고 복구시켜야 한다.		
점검항목	1) 장애 발생 시 서비스 수준 협약에 명시된 시간 내에 장애 대응절차에 따라 조치하고 있는가? 2) 장애 발생 시 절차에 따라 조치하고 장애 조치보고서 등을 통해 기록•관리하고 있는가?		
신청기관 준비사항 (관련증적)	• 장애대응 매뉴얼 및 절차 • 장애조치 보고서 • 서비스 수준협약 (SLA)	참고사항 (샘플자료)	• 정보보호 정책서 • 서비스연속성관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 클라우드컴퓨팅서비스 중단이나 피해가 발생할 경우 서비스 수준 협약(SLA)에 명시된 시간 내에 장애를 처리하고 복구할 수 있도록 대응절차를 수립하여야 한다.

⇨ 점검항목 2)

■ 장애 발생 시 장애대응절차 및 서비스 수준 협약(SLA)에 따라 해당 서비스의 장애를 조치하여야 한다.

■ 장애 처리 완료 후 다음의 내용이 포함된 장애조치 보고서를 작성하고 이력을 관리하여야 한다.

- 장애일시
- 장애 유형 및 심각도 (예 : 상, 중, 하)
- 담당자, 책임자명 (유지보수업체 포함)
- 장애 내용 (장애로 인한 피해 또는 영향 포함)
- 장애 원인
- 조치 내용
- 복구내용
- 재발방지대책 등

통제항목	6.1.4 재발방지		
세부통제내용	장애 관련 정보를 활용하여 유사한 서비스 중단이 반복되지 않도록 장애 재발방지 대책을 수립하고, 필요한 경우 장애대응 절차도 변경하여야 한다.		
점검항목	1) 심각도가 높은 장애의 경우 원인분석을 통한 재발방지대책을 수립·이행하고 있는가?		
신청기관 준비사항 (관련증적)	• 장애조치 보고서 • 재발방지 대책 • 장애대응 절차	참고사항 (샘플자료)	• 정보보호 정책서 • 서비스연속성관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ **점검항목 1)**

■ 장애 복구를 완료한 이후 동일한 장애가 반복적으로 발생하지 않도록 재발방지 대책을 수립하여야 한다.

- 재발방지대책은 장애의 원인을 분석하여 원인을 제거하거나 회피수단을 강구하여 적용
- 재발방지대책이 수립되면 해당 내용을 장애가 발생한 서비스를 운영하는 이해관계자 등에게 교육, 통지 등 수행
- 재발방지대책이 장애 조치보고서에 포함된 경우 장애 조치보고서로 증적 대체 가능
- 장애를 조치하는 동안 적용된 절차가 부적절할 경우 장애 대응절차 변경
- 기존 절차에 포함되어 있지 않거나, 현실적인 내용과 다른 경우 장애분석을 통해 개선된 사항을 반영하여 지침/절차를 변경

6.2 서비스 가용성

<table>
<tr><th>통제항목</th><th colspan="3">6.2.1 성능 및 용량 관리</th></tr>
<tr><td>세부통제내용</td><td colspan="3">클라우드컴퓨팅서비스의 가용성을 보장하기 위해 성능 및 용량에 대한 요구사항을 정의하고, 지속적으로 관리할 수 있는 모니터링 방법 또는 절차를 수립하여야 한다.</td></tr>
<tr><td>점검항목</td><td colspan="3">1) 클라우드 시스템의 성능 및 용량을 지속적으로 모니터링하기 위한 절차를 수립•이행하고 있는가?
2) 클라우드시스템 성능 및 용량 요구사항(임계치)을 초과하는 경우 조치절차를 수립•이행하고 있는가?</td></tr>
<tr><td>신청기관
준비사항
(관련증적)</td><td>• 성능•용량 분석 보고서
• 모니터링 절차서
• 모니터링 대상 및 임계치 현황
• 임계치 초과 시 조치계획</td><td>참고사항
(샘플자료)</td><td>• 정보보호 정책서
• 서비스연속성관리지침</td></tr>
<tr><td colspan="2">ISMS-P 인증 취득 시 심사 생략 가능 대상</td><td colspan="2">O</td></tr>
</table>

점검항목 해설

⇨ 점검항목 1)

■ 고객서비스 및 내부 업무의 연속성을 보장하기 위해 주요 클라우드시스템의 성능 및 용량을 모니터링 하여야 한다.

- 성능 및 용량 관리가 필요한 대상을 식별
- 식별된 관리대상의 네트워크 대역폭, HW 요구사항(CPU, MEM, HDD, NIC 등) 등의 임계치 정의
- 모니터링 방법 수립
- 설정된 임계치에 따라 모니터링 결과 기록 및 보고
- 성능 및 용량 관리를 담당하는 담당자 및 책임자 등의 지정

⇨ 점검항목 2)

■ 정의된 임계치 초과 시 조치절차를 수립하여야 한다.

- 클라우드시스템의 성능 및 용량을 지속적으로 모니터링
- 임계치 초과 시 조치절차 또는 방안 수립
- 조치절차는 가용성 보장절차에 포함하여 수립하거나 별도로 수립 가능
- 시스템, 메모리, 저장장치, 회선 등 증설, 이중화 등

통제항목	6.2.2 이중화 및 백업		
세부통제내용	정보처리설비(예 : 클라우드컴퓨팅서비스를 제공하는 물리적인 서버, 스토리지, 네트워크 장비, 통신 케이블, 접속 회선 등)의 장애로 서비스가 중단되지 않도록 정보 처리설비를 이중화하고, 장애 발생 시 신속하게 복구를 수행하도록 백업 체계도 마련하여야 한다.		
점검항목	1) 백업 대상, 주기, 방법, 절차 등이 포함된 백업 및 복구절차를 수립•이행하고 있는가? 2) 네트워크 차단, 전력 중단 등 외부의 서비스 장애에 대응하기 위한 중요장비를 이중화하고 있는가?		
신청기관 준비사항 (관련증적)	• DR 서비스 계약서 • 시스템 구성도 (이중화) • 서비스 복구 조직 및 절차 • 백업 관리대장 • 백업 절차서	참고사항 (샘플자료)	• 정보보호 정책서 • 서비스연속성관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ 점검항목 1)

■ IT 재해, 장애, 침해사고 등 발생 시 적시에 복구하기 위해 백업 및 복구절차를 수립하고 백업담당자 및 책임자를 지정하여야 한다.
- 백업대상(서버 이미지, DB 데이터, 보안로그 등) 선정
- 백업대상별 백업 주기 및 보존기한 정의
- 백업 담당자 및 책임자 지정
- 백업방법 및 절차 : 백업시스템 활용, 매뉴얼 방식 등(백업매체 관리 포함)
- 복구절차
- 백업이력관리 (백업 관리 대장)
- 백업 소산에 대한 물리적·지역적 사항 고려
- 백업 사이트 구축 및 운영 정책

■ 백업 대상은 대상 정보 및 클라우드시스템의 중요도를 고려하여 선정하여야 하며 정해진 절차에 따라 백업관리를 수행하여야 한다.

■ 주기적으로 백업이력 등을 검토하고 복구 테스트를 통해 정확성과 무결성을 점검한다.

■ 복구절차는 복구 테스트 과정을 통하여 적시에 복구가 가능한 절차를 포함하여야 한다.

■ 공공기관 관련 정보 보관 및 복원을 위한 백업 체계가 수립되어 있는지 확인한다.
- 백업 사이트 구축 및 운영 정책
- 백업 사이트에 대한 위험 관리 정책 등

⇨ 점검항목 2)

■ 클라우드컴퓨팅서비스의 정보처리설비의 중요도 및 복구 우선순위 등에 따라 장애 발생 시 신속하게 복구가 가능하도록 이중화 및 백업체계를 마련하여야 한다.
- 네트워크 회선, 네트워크 장비, 전력선 등 이중화
- 이중화 대상이 되는 주요 정보처리시스템 또는 설비 식별 및 이중화 구축
- 중요정보를 저장하고 있는 스토리지
- 중요 클라우드서비스 관련 시스템

(단 DR 센터에서 운영하는 정보처리설비는 이중화 필수 요건은 아님)

■ 공공기관용 클라우드시스템에 대해서는 장애 및 사고 발생에 대비하여 중요장비를 이중화하는 방안 또는 구축이 되어있는지 확인한다.
- 중요정보가 포함된 스토리지
- 중요 네트워크 장비

통제항목	6.2.3 서비스 연속성 점검		
세부통제내용	서비스 가용성에 대한 영향 평가를 주기적으로 점검하여야 한다.		
점검항목	1) 서비스 장애로부터 서비스 연속성을 확보하기 위해 주기적으로 영향 평가를 통해 점검하고 있는가? 2) 서비스 장애로부터 서비스 연속성을 확보하기 위한 보안대책이 마련되어 있는가?		
신청기관 준비사항 (관련증적)	• DR 서비스 계약서 • 서비스 연속성 계획 • 비즈니스 영향 평가 • 자산 목록 • 네트워크/시스템 구성도 • DR 소개 자료 및 이용자 매뉴얼	**참고사항 (샘플자료)**	• 정보보호 정책서 • 서비스연속성관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 서비스 연속성을 확보하기 위해 주기적으로 비즈니스 영향평가를 검토하고 재해 복구 모의훈련 등을 통해 서비스 연속성을 검증, 미흡한 부분은 보완하여야 한다.

- 핵심 서비스 및 자산 식별
- 성능 및 용량 관리 (시스템 성능, 용량 및 리소스 가용성 등)
- 복구 우선순위 및 복구 목표 시간 등 목표 설정 (RTO, RPO 등)
- 복구 전략 수립 및 보완
- 연 1회 이상 주기적 검토 수행

■ 클라우드 서비스의 재난 상황 발생 시 신속하게 대응하기 위해 재해 복구 절차 및 훈련 계획을 수립하고, 매년 시행하여야 한다.

- 다양한 재난상황(예: 화재, 지진, 수해 등)을 가정하고, 관련 대응 인력이 모두 포함된 재해복구 모의훈련 계획 수립
- 화재 경보기, 가스 경보기, UPS, 자가발전기 등 재난 상황 대비를 위한 설비의 운영 및 정상 작동 점검 결과
- 시설보호계획, 업무연속성 계획 수립 및 이행 여부
- 재난 대비 및 재해 복구 관련 전문기술자 확보 유무
- 통신 중단, 전원 공급망 장애, 화재 등 재해 상황에 대한 재해 복구 모의 훈련 수행 후 결과보고서 작성 및 보고

※ 타 제도에 의해 클라우드 서비스 범위를 포함한 재난 대비 모의훈련을 수행한 경우, 해당 증적으로 재해 복구 상황에 대한 모의훈련 점검 증적 대체 가능

⇨ 점검항목 2)

■ 서비스 연속성 확보를 보장할 수 있도록 물리적으로 떨어진 곳에 DR서비스를 제공하여야 한다.

■ 주센터와 DR센터 간 지리적 거리, 복구시간, 이중화 여부 등을 포함한 자산목록, 네트워크/시스템 구성도, 정책 및 시행문서, DR 소개 자료, DR 이용자 매뉴얼 등을 준비 및 시연하여야 한다.

<재해복구센터 구축 조건>

필수설비	선택사항
· 공공 클라우드 전용 서버, 스토리지 · 네트워크 상면 · 주센터와 물리적 분리	· 소프트웨어, 어플리케이션 · 주센터와 지리적 거리(이격 거리) · DR서비스 복구시간 · DR 센터 내 이중화 구성 여부

<DR센터 체크리스트>

구분	체크리스트	적합여부
서비스 설명	• 다음 항목의 자료가 준비되었는가?	
	- DR 소개 자료 ※ 주센터와 DR센터 간 지리적 거리, 복구시간, 이중화 여부 등 포함	적합□ 부적합□
	- DR서비스의 정상적인 작동 유무 검증 시연 ※ 장애상황에 따른 DR전환 시나리오 준비 및 시연	적합□ 부적합□
	- DR 관련 정책 및 지침	적합□ 부적합□
	- (DR관련) 인증평가 대상 자산 목록과 구성도	적합□ 부적합□
	- 고객용 (DR)서비스 설명 컨텐츠 및 이용 매뉴얼	적합□ 부적합□
	- DR서비스제공을 위한 상용솔루션 사용 여부 (DR서비스 제공을 위한 데이터백업, 서비스 전환 등을 위한 상용솔루션 등)	적합□ 부적합□
물리적 구축	• 공공클라우드 전용서버, 스토리지, 네트워크, 상면 등을 구비하고 있는가? ※ DR센터의 네트워크는 공공·민간 부문 공용으로 운영 가능 (단, 주센터는 공공·민간 부문 분리 필요함)	적합□ 부적합□
	• 공공클라우드시스템은 물리적으로 민간과 분리되어 있는가?	적합□ 부적합□
	• 접근통제가 적절하게 이루어지고 있는가? ※ 8.1. 물리적보호구역 및 8.2. 정보처리시설 및 장비보호에 대한 사항을 점검	적합□ 부적합□
공공 요구조건 충족 여부	• DR서비스제공과 관련하여 공공기관의 보안요구사항을 정의하고 있는가? - 보안요구사항 정의 및 계약 시 반영 - 공공기관에 보고 절차 수립	적합□ 부적합□

	• 국가정보원장이 안전성을 확인한 정보보호제품을 사용하고 있는가?	적합□ 부적합□
	• 암호화구간이 존재할 경우, 검증필암호화모듈을 사용하는가?	적합□ 부적합□
	• 내부관리망, 클라우드 플랫폼은 갖추고 있는가?	적합□ 부적합□
	• 중요자료 전송 및 저장시 암호화기술을 제공하고 있는가? - 고객이 VM등 서버에 원격 접속 시 - 공공기관 데이터 이관 시 - 법적요구사항을 고려하여 중요정보 저장 시 ※ 11.1.1. 네트워크 보안 정책 수립, 11.1.4. 네트워크 암호화, 12.3.1. 암호정책 수립, 12.3.2. 암호키 관리, 13.1.2. 인증 및 암호화 기능 통제항목 참조	적합□ 부적합□
	• 센터 절체 및 복구 관련 공공기관 담당자의 개입이 필요한 사항들에 대한 정의 및 협의서 양식은 준비되어 있는가?	적합□ 부적합□

7. 준거성

7.1 법 및 정책 준수

통제항목	7.1.1 법적요구사항 준수		
세부통제내용	정보보호 관련 법적 요구사항을 식별하고 준수하여야 한다.		
점검항목	1) 정보보호 관련 법적 요구사항을 식별하고 준수하고 있는가?		
신청기관 준비사항 (관련증적)	• 식별된 법적 요구사항 및 검토 결과	참고사항 (샘플자료)	• 정보보호 정책서
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ 점검항목 1)

■ 정보보호 관련 법적 요구사항을 식별하고 준수하여야 한다.

- 클라우드서비스 운영 시 준수해야 할 정보보호 관련 법적 요구사항 식별 (클라우드컴퓨팅법, 정보통신망법, 개인정보보호법, 전자금융거래법, 부정경쟁방지 및 영업비밀보호에 관한 법률 등 관련 법령 및 지침· 고시 해설서 참고

■ 정보보호 관련 법률의 제개정 등 클라우드의 중대한 환경 변화 시 기수립된 정보보호 정책의 타당성을 검토하고 제·개정을 통해 관련 문서에 반영해야 한다.

■ 클라우드컴퓨팅서비스 제공자는 법적 요구사항 준수 여부를 별도 점검하거나 법적 요구사항을 내부 정책, 지침 등에 반영한 후 해당 항목의 준수 여부에 대해서 점검 가능함

※ 관련 법규 파악·관리 예시

NO	분류	항목	준수 여부	현황	관련법률
1	침해사고	침해사고 발생 시 관계기관 및 이용자에게 통지 여부	Y	침해사고 발생 시 관계기관 신고절차 및 이용자 통보 절차를 수립·운영하고 있음	클라우드컴퓨팅 발전 및 이용자 보호에 관한법률 제25조
2	수집	서비스 제공을 위한 최소한의 정보만 수집하는가?	Y	서비스 제공을 위한 최소한의 정보만 수집하고 있음	개인정보보호법 제16조
3	동의	민감정보 수집 시 정보주체로부터 동의를 받거나 관련 법령을 근거로 수집하고 있는가?	Y	민감정보 수집 시 정보주체로부터 동의를 받아 수집하고 있음	개인정보보호법 제23조
4	이용	개인정보를 제공 받는 경우 제공받은 목적 외의 용도로 이용하지 않는가?	Y	개인정보를 제공 목적 외의 용도로 이용하고 있지 않음	개인정보보호법 제19조

- 클라우드컴퓨팅법 등 법률에서 요구하는 사항을 식별하고 현재 클라우드컴퓨팅서비스 제공자의 관련 정책에 반영하여야 함

통제항목	7.1.2 정보보호 정책 준수		
세부통제내용	정보보호 정책 및 서비스 수준 협약에 포함된 보안 요구사항을 식별하고 준수하며 이용자가 요구하는 경우 관련 증거를 제공하여야 한다.		
점검항목	1) 클라우드 정보보호 정책 및 서비스 수준 협약에 포함된 보안 요구사항을 식별하고 준수하고 있는가? 2) 이용자 요청시 보안 요구사항 준수여부에 대한 증거를 제공하고 있는가?		
신청기관 준비사항 (관련증적)	• 정보보호 정책서 • 계약서, 서비스 준수 협약서 • 식별된 보안요구사항 준수여부 검토 결과	참고사항 (샘플자료)	• 정보보호 정책서
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ 점검항목 1)

■ 클라우드 정보보호 정책 및 서비스 수준 협약에 포함된 보안요구사항을 식별하고 준수하여야 한다.

- 클라우드 보안 요구사항의 준수여부를 내부 보안감사 및 모니터링 등의 활동을 통해 검토하여야 한다.

■ 보안요구사항은 관련 법률, 정책, 계약서 및 SLA 등의 내용을 검토한 후 식별하고 Check List 형태로 작성하여 준수여부 및 개선방안을 검토한다.

No	법률명	관련조항그룹	No	법적고려사항	평가	수행현황	개선방안 및 보호대책	이행계획
1.1	개인정보보호법	관리적 조치	1.1.1	제3조(내부관리계획의 수립·시행) - 개인정보의 안전한 처리를 위하여 다음사항을 포함하는 내부관리계획을 수립·시행하고 있는가? 1. 개인정보 보호책임자의 지정에 관한 사항 2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항 3. 개인정보의 안전성 확보에 필요한 조치에 관한 사항 4. 개인정보취급자에 대한 교육에 관한 사항 5. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항 6. 그 밖에 개인정보 보호를 위하여 필요한 사항				
1.2			1.1.2	제4조(접근 권한의 관리) - 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하고 있는가? - 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하고 있는가? - 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우, 개인정보취급자 별로 사용자계정을 발급하며, 계정공유가 되지 않도록 하고 있는가? - 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하고 있는가?				

※ 주요 법적요구사항 미준수 사항

구분	내용
개인정보 수집	-개인정보 수집 시, 개인정보 목적 외 이용 시, 고유식별정보 처리 시, 민감정보 처리 시 등 정보주체 동의 시 각각 구분하여 동의 -개인정보 수집 시 필수항목 고지 -수집 및 제공하려는 개인정보 항목과 이용자 동의 시 고지하는 항목 간 일치
개인정보처리방침	-개인정보 수집 시 개인정보처리방침 고지 -개인정보 수집 및 보유 항목과 일치 -개인정보 위탁사 현황 업데이트 -개인정보 제3자 제공 현황 업데이트 -개인정보 보호책임자 및 개인정보 보호업무 및 고충사항 처리 부서 고지 -수립하거나 변경한 개인정보처리방침 지속 게재
안전성 확보조치 기준	-개인정보처리시스템 접속기록 1년 이상 보관 및 월 1회 이상 점검 -비밀번호 및 고유식별정보 등 암호화

⇨ 점검항목 2)

■ 이용자가 보안요구사항 준수여부에 대한 증거 요청 시 제공하여야 한다.

7.2 정보 시스템 감사

통제항목	7.2.1 독립적 보안감사		
세부통제내용	법적 요구사항 및 정보보호 정책 준수 여부를 보증하기 위해 독립적 보안감사 계획을 수립하여 시행하고 개선 조치를 취하여야 한다.		
점검항목	1) 클라우드 보안 요구사항의 준수여부를 보증하기 위해 독립적 감사 계획을 수립하여 시행하고 있는가? 2) 감사결과를 정보보호 최고책임자에게 보고하고 발견된 사항에 대해 개선조치를 취하고 있는가?		
신청기관 준비사항 (관련증적)	• 보안감사 계획서 • 보안감사 결과보고서 • 보안감사 이행조치결과서	참고사항 (샘플자료)	• 정보보호 정책서 • 보안감사 계획서 • 보안감사 결과보고서
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ 점검항목 1)

■ 다음의 항목을 포함한 독립적인 보안감사 계획을 수립하고 연1회 이상 수행하여야 한다.

- 보안감사 점검 인원
  - ·내부인력 활용 시 클라우드서비스 업무와 독립적인 업무를 담당하는 자 중 보안감사 역량을 보유한 자를 선임
- 보안감사 점검 인원의 자격요건 정의
  - ·점검의 객관성, 전문성 등을 확보할 수 있도록 자격요건을 정의
- 보안감사 일정 및 범위
  - ·클라우드컴퓨팅 및 정보보호 관련 법률
  - ·클라우드서비스 보안운영 명세서 내의 점검항목
  - ·규정 및 지침 등의 준수사항을 포함한 이행점검

■ ISMS 인증항목을 기준으로 감사를 수행할 경우 클라우드컴퓨팅서비스 정보보호에 관한 기준 등에서 요구하는 항목이 누락되지 않도록 적절한 감사항목을 생성하여야 한다.

⇨ 점검항목 2)

■ 보안감사 결과보고서를 작성하여 정보보호 최고책임자에게 보고하여야 한다.

- 보안감사 완료 후 결과보고서를 작성하여 정보보호 최고책임자 및 개인정보보호 책임자 등 경영진에게 보고

■ 보안감사 결과 보완이 필요한 사항이 발견된 경우에는 해당 사항에 대한 조치계획을 수립하여 이행하여야 한다.

- 조치 완료여부에 대하여도 확인 수행

통제항목	7.2.2 감사기록 및 모니터링		
세부통제내용	보안감사 증적(로그)은 식별할 수 있는 형태로 기록 및 모니터링 되어야 되고 비인가된 접근 및 변조로부터 보호되어야 한다.		
점검항목	1) 보안감사 증적(로그)을 식별하고 로그유형 및 보존기간의 법적요건을 고려하여 기록(보관), 검토하고 있는가? 2) 로그기록을 별도 저장장치를 통해 백업하고 비인가된 접근 및 변조로부터 보호하고 있는가?		
신청기관 준비사항 (관련증적)	• 보안감사 로그 유형, 보존기간 등 현황 • 로그 백업 대장 • 로그기록 백업매체 관리 증적 • 로그기록 검토/보고 증적	참고사항 (샘플자료)	• 정보보호 정책서
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 법적 요건을 고려하여 보관하여야 할 보안감사 증적(로그)을 식별하고 유형 및 기간을 정하여야 한다.

- 시스템 설계 시 보안감사 기록유형을 정의 (예: 사용자 접속 기록, 인증 성공/실패 로그, 권한 등록/변경/삭제 등)
- 시스템 설계 시 보안감사 증적으로 생성되어야 하는 로그항목을 선정 (예: 사용자 접속 기록의 경우 접속일시, ID, 접속지 IP, 처리한 정보주체 정보, 수행업무 등 (예: 이용자/사용자 식별 및 인증, 관리자의 관리행위, DB 접근 등)
- 생성된 보안감사 증적은 법률에 따라 보관 (최소 1년 이상)
- 시스템 설계 시 보안로그를 보호하기 위한 대책 마련

■ 응용프로그램 내의 보안감사(접근기록 등) 증적 외에도 윈도우시스템, 리눅스/유닉스시스템, 데이터베이스, WEB/WAS, 네트워크 장비 등에 대한 로그도 생성, 보관, 모니터링되어야 한다.

■ 보관되고 있는 보안감사 증적을 모니터링할 수 있는 수단을 제공해야 한다.

- 보안감사 증적을 이벤트별 조회, 사용자별 조회, 키워드를 적용한 조회, 날짜별 조회 등 다양한 조회 기능 적용
- 비정상적인 사건(연속된 인증실패, 저장 및 전송데이터 훼손, 대량의 데이터 다운로드 등)이 발생한 경우 알람 기능 적용

- 보안관제 시스템, 통합보안관리 시스템 등을 이용한 자동화된 모니터링 적용 등

■ 보안감사 증적 중 개인정보처리시스템의 접근기록 등은 월 1회 이상 점검하여야 하며, 기타 시스템의 감사로그는 공공기관의 요구사항 또는 클라우드컴퓨팅서비스 제공자의 정책 및 지침에 따라 정기적으로 검토되어야 한다.

■ 검토기준에 따라 검토 한 후 이상징후 여부 등 그 결과를 관련 책임자에게 보고하여야 한다.

■ 공공기관용 클라우드 서비스의 경우 공공기관이 감사 로그를 요청 시 제공하여야 한다.

※ 보안감사 로그 유형 예시

구분	설명
개인정보처리시스템 접근기록	- 사용자 및 관리자의 접속기록(사용자식별정보 : ID, 접속일시, 정보주체 정보, 접속지 : 단말기 IP, 수행업무 : 정보생성, 수정, 삭제, 검색 출력 등), - 인증 성공/실패 로그 - 파일 접근 - 계정 및 권한 등록/변경/삭제 - 정보시스템 시작 및 중지, 특수 권한으로의 접근 기록 - 주요업무관련 행위에 대한 로그 등
시스템 로그	- 주요 서버, 네트워크, 보안 장비 등의 로그(접근기록 및 이벤트 로그 등)

■ 시스템 로그는 각 시스템별로 생성되는 로그의 유형이 상이하므로 로그식별 및 보관정책 수립이 필요하다.

구분	설명
보안관련 감사로그	-사용자 접속기록(사용자식별정보 : ID, 접속일시, 접속지 : 단말기 IP, 처리한 정보주체 정보, 수행업무 : 정보생성, 수정, 삭제, 검색 출력 등) -인증 성공/실패 로그 -파일 접근 -계정 및 권한 등록/변경/삭제 등
시스템 이벤트 로그	-운영체제 구성요소에 의해 발생되는 로그(시스템 시작, 종료, 상태, 에러코드 등)
보안시스템 로그	-보안시스템 정책(룰셋 등) 등록/변경/삭제 로그 -이벤트 로그 등

⇨ 점검항목 2)

■ 보안감사 증적은 별도 저장장치에 백업하여야 하며, 비인가된 접근 및 변조로부터 보호되어야 한다.

- 시스템 설계 시 보안감사 증적에 대하여 비인가된 접근차단, 변조방지 기능 적용
- 보안감사 증적의 백업데이터(백업매체)에 대한 비인가된 접근 및 변조에 대한 관리적 보안대책 적용

8. 물리적 보안

8.1 물리적 보호구역

통제항목	8.1.1 물리적 보호구역 지정		
세부통제내용	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 한다.		
점검항목	1) 주요 설비 및 시스템을 보호하기 위하여 물리적 보호구역을 다음과 같이 정의하고 구역별 보호대책을 수립 • 이행하고 있는가? - 접견구역 : 외부인 접견 구역 - 제한구역 : 사무실 지역 등 - 통제구역 : 공공기관 클라우드 서비스 운용 설비 및 시스템 구역 등		
신청기관 준비사항 (관련증적)	• 보호구역 지정 현황 • 보호구역 물리적 보안대책 • 시스템 구성도 (물리적 구성 확인 가능)	**참고사항 (샘플자료)**	• 정보보호 정책서 • 물리적보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ **점검항목 1)**

■ 중요정보 저장시설, 서비스의 주요 장비가 운영되는 시설 등 서비스의 주요 물리적인 시설을 안전하게 보호하기 위해 중요도에 따라 분류하여 지정하고, 물리적인 접근통제 대책을 수립하여 적용하여야 한다.

예) 중요도에 따라 접견구역, 제한구역, 통제구역으로 분류

- 접견구역 : 외부인이 별다른 통제 없이 출입이 가능한 구역
- 제한구역 : 비인가된 접근을 방지하기 위하여 별도의 출입통제 장치 및 감시 시스템이 설치된 장소로 출입 시 직원카드와 같은 출입증이 필요한 장소
- 통제구역 : 제한구역의 통제항목을 모두 포함하고 출입자격이 최소인원으로 유지되며 출입을 위하여 추가적인 절차가 필요한 곳

접견구역	제한구역	통제구역
• 외부인이 통제없이 출입 가능	• 내부직원은 출입이 허용되나 외부인은 출입이 통제 • 출입통제 장치 등으로 인가된 인원만 출입 가능 • 사무실 복도 등에 CCTV 등 보안장치 설치 및 모니터링	• 외부인은 물론 내부직원이라도 필요한 최소한의 인원만 출입 가능 • 접견구역보다 더 엄격한 출입통제 적용 • CCTV 등 보안장치 설치 및 모니터링 • 출입을 위해 추가적인 신청, 검토, 승인 등의 절차 필요 • 비인가자 출입 시 인가자에 의한 인솔 등 필요
• 접견장소 등	• 각 부서별 사무실 등	• 전산실 • 통신장비실 • 관제실 • 운영실 • 공조실 • 발전실 등

■ 내부직원, 외부직원(유지보수 등), 제3자의 출입에 대한 출입절차를 수립하여 적용하여야 한다.

■ 통제구역은 반드시 인가된 인원만 출입을 허용하여야 하며, 인가자를 최소한으로 제한하여야 한다.

■ 통제구역임을 표시하고 비인가된 접근시도 여부를 주기적으로 검토하여야 한다.

■ 공공기관용 클라우드컴퓨팅시스템은 민간용과 물리적으로 분리운영되어야 한다. 별도 케이지 등을 설치하여 출입 및 출입기록을 관리하여야 한다.

■ 각 보호구역의 중요도 및 특성을 반영하여 작업 절차를 수립하고 필요 설비를 갖추어야 한다.

통제항목	8.1.2 물리적 출입통제		
세부통제내용	물리적 보안 구역에 인가된 자만이 접근할 수 있도록 출입을 통제하는 시설(예 : 경비원, 출입 통제 시스템 등)을 갖추어야 하고, 출입 및 접근 이력을 주기적으로 검토하여야 한다.		
점검항목	1) 물리적 보호 구역에 인가된 자만이 접근할 수 있도록 출입을 통제하는 시설(예 : 출입 통제 시스템 등)을 갖추고 있는가? 2) 주기적으로 통제구역의 출입명단 및 출입카드 발급 현황을 검토 및 승인하고 더 이상 출입하지 않는 직원은 출입명단에서 삭제하고 있는가?		
신청기관 준비사항 (관련증적)	• 보호구역 지정 현황 • 보호구역 물리적 보안대책 • 보호구역 인가자 목록 • 출입관리대장 • 출입카드 발급현황 • 출입자 이력 검토 증적	참고사항 (샘플자료)	• 정보보호 정책서 • 물리적보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 물리적 보호 구역에 인가된 자만이 접근할 수 있도록 출입을 통제하는 설비(예 : 출입 통제 시스템 등)을 갖추어야 한다.

- 출입 통제 시스템은 지식, 소유, 존재(생체), 행위 기반 중 자산의 중요도 및 통제 목적 등을 고려하여 선택 가능
- 비밀번호 방식의 지식 기반 출입 통제 시스템을 사용할 경우 출입 및 접근 이력관리를 위해 출입관리대장 등을 기록 작성 (CCTV 등을 통한 출입 유무에 대한 모니터링 수행 병행)

⇨ 점검항목 2)

■ 통제구역 인가자의 명단 및 출입카드 발급 현황을 주기적으로 검토하여야 한다.

■ 출입이 인가된 인력 중 퇴사, 역할의 변경, 전보 등으로 출입이 제한되는 경우 즉시 출입 권한을 회수하고 출입통제시스템에 반영하여야 한다.

■ 주기적으로 통제구역의 출입명단(장비 반출입 포함) 및 출입카드 발급 현황을 검토 및 승인하고 더 이상 출입하지 않는 직원은 출입명단에서 삭제하여야 한다.

■ 물리적 보안 구역에 출입 및 접근한 이력을 보관하고 주기적으로 검토하여야 한다.

<table>
<tr><th>통제항목</th><th colspan="3">8.1.3 물리적 보호구역 내 작업</th></tr>
<tr><td>세부통제내용</td><td colspan="3">유지보수 등 주요 정보처리 설비 및 시스템이 위치한 보호구역 내에서의 작업 절차를 수립하고 작업에 대한 기록을 주기적으로 검토하여야 한다.</td></tr>
<tr><td>점검항목</td><td colspan="3">1) 클라우드 시스템 도입, 유지보수 등으로 보호구역 내 작업이 필요한 경우 작업신청 및 수행 관련 절차를 수립하고 작업기록을 주기적으로 검토하고 있는가?
2) 클라우드 시스템이 위치한 통제구역 내 모바일기기(노트북, 스마트기기 등) 사용 방지 및 불법적인 활동을 모니터링(예: CCTV) 하기 위한 대책이 마련되어 있는가?</td></tr>
<tr><td>신청기관
준비사항
(관련증적)</td><td>• 보호구역 내 작업 절차
• 작업 신청서
• 출입관리대장(출입카드 발급현황 등)
• 작업 기록서
• 통제구역 CCTV 배치도
• 모바일기기 반출입관리대장 (백신 등)</td><td>참고사항
(샘플자료)</td><td>• 정보보호 정책서
• 물리적보안지침</td></tr>
<tr><td colspan="2">ISMS-P 인증 취득 시 심사 생략 가능 대상</td><td colspan="2">O</td></tr>
</table>

점검항목 해설

➪ **점검항목 1)**

■ 통제구역에서 정보시스템 도입 및 폐기, 유지보수(정기점검 포함) 등의 사유로 작업을 수행할 경우 작업 절차를 수립하고, 작업자가 작업 절차를 준수하는지 주기적으로 검토하여야 한다.

- 작업이 수행하기 전에 작업신청서를 통한 신청 및 신청에 대한 검토・승인
  ・작업신청서에는 작업자(내부인력 or 외부인력 등), 작업일시, 작업목적, 작업수행에 필요한 기기(노트북, USB, 네트워크, 모바일 기기 등)에 대한 안정성 확보 등이 포함되어야 함
- 작업기록에는 작업일자, 작업시간, 작업목적, 작업내용, 작업업체 및 담당자명, 검토자 승인자 등 포함
- 작업수행을 위한 보호구역 출입절차 마련
- 출입기록의 주기적 검토
- 작업 수행을 위한 모바일기기 반출입 및 안전성 확보 절차(백신 설치 등 필수 소프트웨어 설치) 마련

⇨ **점검항목 2)**

- 통제구역 내에서 작업을 수행하는 경우 작업수행에 필요한 모바일기기에 대한 사용은 원칙적으로 금지하여야 한다.

- 해당 작업에 불가피하게 모바일 기기를 사용해야 하는 경우 반드시 사전에 승인을 받고 사용하여야 하며, 모바일 기기의 보안성 검토를 수행한 후 사용하여야 한다.

통제항목	8.1.4 사무실 및 설비 공간 보호		
세부통제내용	사무실 및 설비 공간에 대한 물리적인 보호방안을 수립하고 적용하여야 한다.		
점검항목	1) 팩스, 복사기, 프린터, 공용 PC, 파일서버, 문서고 등 공용으로 사용하는 사무장비 및 시설에 대한 보호대책을 수립·이행하고 있는가? 2) 공용업무 환경 보안에 대한 관리자를 지정하고 준수여부를 주기적으로 검토하고 있는가?		
신청기관 준비사항 (관련증적)	• 공공 사무기기 현황 및 보호대책 • 공용업무환경 보안 관리자 지정 • 공용업무환경 점검 내역	참고사항 (샘플자료)	• 정보보호 정책서 • 물리적보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ **점검항목 1)**

■ 공용으로 사용하는 사무기기에 대한 보호대책을 수립하고 이행하여야 한다.

- 공용사무기기 : 팩스, 복사기, 프린터, 공용PC
  - ·공용사무기기 주변 및 공용사무실(회의실, 프로젝트룸 등)에는 주요문서 등이 방치되지 않도록 하여야 한다.
  - ·공용PC의 경우 화면보호기 설정, 재시작 시 암호설정, 고용패스워드의 주기적인 변경, 주요정보 저장 금지 등을 적용하여야 한다.
- 파일서버 : 공용으로 사용되는 파일서버의 경우 부서별, 업무별, 사용자별로 접근권한을 부여하여야 하며, 주요파일은 가급적 공용으로 사용하는 파일서버에 저장하지 않아야 한다.
- 문서고 : 문서고에 대한 접근권한을 부서별 혹은 업무별로 부여하여 출입가능 인원을 최소화하고 CCTV 혹은 출입통제시스템을 설치하여 출입이력을 관리하여야 한다.
- 기타 공용 업무환경에 대한 보안대책 수립

➪ **점검항목 2)**

■ 공용으로 사용하는 사무기기, 공용사무실 등에 대한 관리를 위해 관리담당자를 지정하고 수립된 보호대책이 준수되고 있는지 주기적으로 점검하여야 한다.

<table>
<tr><th>통제항목</th><th colspan="3">8.1.5 모바일 기기 반출・입</th></tr>
<tr><td>세부통제내용</td><td colspan="3">노트북 등 모바일 기기 미승인 반출・입을 통한 중요정보 유출, 내부망 악성코드 감염 등의 보안사고 예방을 위하여 보호구역 내 임직원 및 외부인력 모바일 기기 반출・입 통제절차를 수립하고 기록・관리하여야 한다.</td></tr>
<tr><td>점검항목</td><td colspan="3">1) 노트북, 패드 등 모바일 기기 반출・입 시 반출・입 통제 및 보안사고 예방 절차를 수립하고 있는가?
2) 모바일 기기 반출・입 절차에 따라 반출・입대장을 작성하고 관리자는 주기적으로 모바일 기기 반출・입 이력을 점검하고 있는가?</td></tr>
<tr><td>신청기관
준비사항
(관련증적)</td><td>• 모바일기기 반출・입 통제 절차 (백신 설치, 카메라 보안 씰 등 포함)
• 모바일기기 반출・입 신청서 및 승인 문서
• 모바일기기 반출・입 이력 검토 내역</td><td>참고사항
(샘플자료)</td><td>• 정보보호 정책서
• 물리적보안지침</td></tr>
<tr><td colspan="2">ISMS-P 인증 취득 시 심사 생략 가능 대상</td><td colspan="2">O</td></tr>
</table>

점검항목 해설

⇨ **점검항목 1)**

■ 보호구역별로 모바일기기(노트북, 탭, 패드 등)의 반출・입에 대한 통제절차를 수립하여 적용하여야 한다.

- 보호구역 출입통제 책임자의 사전승인 절차
- 반・출입 관리대장 등에 기록 및 출입 전 모바일 기기 보안 점검 절차 포함
- 모바일 기기 반출・입내역 주기적 점검 절차
- 보안사고 예방절차 등 포함 (백신 설치 감사, 모바일 기기의 카메라 차단 등)
- 외부의 모바일 기기는 원칙적으로 반입을 금지하고 필요한 경우 내부에서 관리되고 있는 모바일 기기를 사용하도록 절차 수립
- USB 사용이 필요한 경우 보안USB 사용
- 개인 모바일기기 반입 금지 등 예방 절차 포함

⇨ **점검항목 2)**

■ 보호구역 내로 모바일기기를 반・출입하는 경우 반출・입에 대한 이력을 기록으로 보관 유지하여야 하며, 담당자는 주기적으로 기록을 검토하여야 한다.

■ 기록(반출・입 관리대장 등)에는 반출・입 일시, 사용자, 기기식별정보(모델, MAC, 시리얼 번호 등), 사유, 반출・입 구역, 보안점검 결과, 관리자 확인 서명 등

8.2 정보처리 시설 및 장비보호

통제항목	8.2.1 정보처리시설의 배치		
세부통제내용	물리적 및 환경적 위험으로부터 잠재적 손상을 최소화하고 비인가된 접근 가능성을 최소화하기 위하여, 정보처리시설 내 장비의 위치를 파악하고 배치하여야 한다.		
점검항목	1) 클라우드시스템의 특성을 고려하여 배치 장소를 분리하고 있는가? 2) 클라우드시스템의 실제 물리적 위치를 손쉽게 확인할 수 있는 방안(배치도, 자산목록 등)을 마련하고 있는가?		
신청기관 준비사항 (관련증적)	• 정보자산 배치도 • 정보자산 목록	**참고사항 (샘플자료)**	• 정보보호 정책서 • 물리적보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ **점검항목 1)**

■ 서버, 네트워크 장비, 정보보호시스템, 백업장치 등 정보시스템 특성에 따라 분리하여 배치하고, 전산랙(Rack) 등을 이용하여 시스템을 외부로부터 보호하여야 한다.
- 침수, 외부의 물리적 공격을 최소화할 수 있는 곳에 주요한 시스템 배치
- 정보시스템의 수량이 많지 않을 경우 하나의 전산랙에 배치하되 특성별 분리 배치 가능

■ 개인정보 또는 사내 기밀정보 등 중요정보를 저장하고 있는 서버나 중요 네트워크 장비(백본 등)의 경우 전산랙에 잠금장치를 설치하는 등 인가된 자에 한해 접근이 가능하도록 관리하여야 한다.

⇨ **점검항목 2)**

■ 정보시스템은 관리자가 즉시 위치를 확인할 수 있도록 물리적 배치도(시설 단면도, 배치도 등) 또는 목록을 마련하여 최신본으로 관리하여야 한다.
- 시스템 정보자산목록에 물리적 위치를 표시
- 목록에서 물리적 배치를 확인 가능하도록 최신현황 유지

<table>
<tr><th>통제항목</th><th colspan="3">8.2.2 보호설비</th></tr>
<tr><td>세부통제내용</td><td colspan="3">각 보안 구역의 중요도 및 특성에 따라 화재, 누수, 전력 이상 등 자연재해나 인재에 대비하여 화재 감지기, 소화 설비, 누수 감지기, 항온항습기, 무정전 전원 장치(UPS), 이중 전원선 등의 설비를 갖추어야 한다.</td></tr>
<tr><td>점검항목</td><td colspan="3">1) 각 보호구역의 중요도 및 특성에 따라 화재, 전력 이상 등 인재 및 자연재해 등에 대비하여 필요한 설비를 갖추고 운영절차를 수립·관리하고 있는가?
2) 보호구역 내 주요 시스템 및 인력을 화재로부터 보호하기 위하여 필요한 설비를 설치하고 지속적으로 운영·관리하고 있는가?
3) 보호구역 내 주요 시스템을 수해로부터 보호할 수 있도록 누수를 탐지할 수 있는 설비를 설치하고 지속적으로 운영·관리하고 있는가?
4) 보호구역 내 주요 정보시스템이 안정적인 환경에서 동작할 수 있도록 적절한 온도와 습도를 유지시키는 항온항습 또는 에어컨을 설치하여 운영·관리하고 있는가?
5) 보호구역 내 주요 시스템이 전력을 안정적으로 공급받을 수 있도록 시설을 설치하고 지속적으로 운영·관리하고 있는가?
6) 화재 등의 재해 발생 시 임직원이 대피절차에 따라 안전하게 대피할 수 있도록 비상벨, 비상등, 비상통로 안내표지 등을 설치하고 있는가?
7) 주요 정보시스템을 외부 집적정보통신시설(IDC)에 위탁운영하는 경우, 물리적보호에 필요한 요구사항을 계약서에 반영하고 운영상태를 주기적으로 검토하고 있는가?</td></tr>
<tr><td>신청기관
준비사항
(관련증적)</td><td>• 보호설비 운영 절차 및 기준
• 보호구역 내 설비 현황
• 정보자산 목록
• 위탁운영업체의 물리적 보호설비에 대한 정기운영점검결과
• 물리적 보호설비 주기적 검토 내역</td><td>참고사항
(샘플자료)</td><td>• 정보보호 정책서
• 물리적보안지침</td></tr>
<tr><td colspan="2">ISMS-P 인증 취득 시 심사 생략 가능 대상</td><td colspan="2">O</td></tr>
</table>

점검항목 해설

⇨ **점검항목 1)**

■ 보호구역의 중요도와 특성에 따라 인재 및 자연재해를 대비한 운영절차를 마련하여야 한다.

➪ **점검항목 2)**

■ 화재 감지기를 적절한 간격으로 설치하고 충분한 소화시설을 확보하여야 한다.
- 보호구역 면적에 대비하여 화재 감지기 및 소화설비 설치
- 소화설비 장치 사용법 안내서 배치
- 소화설비에 대한 주기적인 점검 수행

➪ **점검항목 3)**

■ 수해로부터 보호구역을 보호하기 위한 보호대책을 이행하여야 한다.
- 누수감지기 설치
- 누수감지 설비에 대한 주기적인 점검

➪ **점검항목 4)**

■ 보호구역의 온도 및 습도를 적절하게 유지하여야 한다.
- 항온항습에 대한 기준 수립
- 항온항습기 또는 에어컨 등 온습도 유지를 위한 시설 설치
- 항온항습 설비에 대한 주기적인 점검 수행

➪ **점검항목 5)**

■ 보호구역 내 정보시스템을 위한 안전한 전원공급 설비를 구비하여야 한다.
- 무정전전원장치(UPS), 비상발전기, 전원선 이중화, 전압유지기, 접지시설 등 보호구역의 특성에 따라 적절한 전원공급 설비 구축
- 전원공급 설비에 대한 주기적인 점검 수행

➪ **점검항목 6)**

■ 화재 등의 재해 발생 시 임직원이 대피할 수 있도록 대피절차를 별도로 마련하고 절차에 따라 신속하게 대피할 수 있도록 비상벨, 비상등, 비상통로 안내표지 등을 설치하여야 한다.

➪ **점검항목 7)**

■ 주요 정보시스템을 외부 집적정보통신시설(IDC)에 위탁운영하는 경우 화재, 수재, 전력이상, 온도, 습도, 환기 등의 환경적 위협 및 파손, 도난 등 물리적 위협으로부터 보호되도록 보안요구사항을 계약서에 반영하고 운영상태를 주기적으로 검토하여야 한다

통제항목	8.2.3 케이블 보호		
세부통제내용	데이터를 송수신하는 통신케이블이나 전력을 공급하는 전력 케이블은 손상이나 도청으로부터 보호하여야 한다.		
점검항목	1) 전력 및 통신케이블이 외부로부터의 물리적 손상이나 전기적 영향 (예 : 간섭)으로부터 보호되고 있는가?		
신청기관 준비사항 (관련증적)	• 전력 및 통신케이블 보호 대책	참고사항 (샘플자료)	• 정보보호 정책서 • 물리적보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ 점검항목 1)

■ 전력 및 통신케이블 등이 외부의 영향 없이 안정적으로 전력 및 데이터 전송이 이루어질 수 있도록 보호대책을 적용해야 한다.

- 전력케이블과 통신케이블은 물리적으로 구분하여 배선
- 전력케이블과 통신케이블에 대한 식별
- 전력케이블과 통신케이블 사이의 상호간섭을 방지하기 위한 거리 유지
- 케이블을 지지하고 보호할 수 있는 설비 설치 (예 : 케이블 트레이)
- 도청이나 손상이 일어나지 않도록 케이블을 보이지 않게 매설할 것
- 약전실, 강전실, 배전반 등에 대한 접근통제 등

통제항목	8.2.4 시설 및 장비 유지보수		
세부통제내용	정보처리시설은 가용성과 무결성을 지속적으로 보장할 수 있도록 유지보수 하여야 한다.		
점검항목	1) 시설 및 장비의 가용성 및 무결성 보장하기 위해 지속적으로 유지보수를 하고 있는가?		
신청기관 준비사항 (관련증적)	• 보호구역 내 시설 및 장비 정기점검 내역	참고사항 (샘플자료)	• 정보보호 정책서 • 물리적보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ **점검항목 1)**

■ 주요 시설 및 장비에 대해서는 정기점검 계획을 수립하고 시행하여야 한다.

- 유지보수 전문기관과 유지보수 계약을 맺고, 유지보수 인력의 출입에 대한 보안대책을 수립하여 적용하여야 한다.
- 정보처리시설에 대하여 정기적인 점검을 수행하여야 한다.(월 1회 이상 권고)

통제항목	8.2.5 장비 반출・입		
세부통제내용	장비의 미승인 반출・입을 통한 중요 정보 유출, 악성코드 감염 등의 침해사고 예방을 위하여, 보안 구역 내 직원 및 외부 업무 관련자에 의한 장비 반출・입 절차를 수립하고, 기록 및 관리하여야 한다.		
점검항목	1) 보호구역 내 중요한 장비, 문서, 매체 등에 대한 반출입 관련 정책 및 절차를 수립・이행하고 있는가?		
신청기관 준비사항 (관련증적)	• 보호구역 내 장비 등 반출입 절차 • 반출입 신청서 • 반출입 관리 대장	참고사항 (샘플자료)	• 정보보호 정책서 • 물리적보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ 점검항목 1)

■ 보호구역 내 장비, 설비, 저장매체 등의 반・출입 통제 정책 및 절차를 수립하고 이행하여야 한다.

- 서버, 네트워크 장비와 같은 전산정비 반・출입 절차 포함
- 항온항습기, UPS 등과 같은 설비의 반・출입 절차 포함
- 조직의 기밀문서, 대외비 문서 등 문서에 대한 반・출입 절차 포함
- 외장형 HDD, CD, USB 메모리 등 저장매체 및 카메라 등의 촬영기기 등에 대한 반・출입 절차 포함

■ 관리대장을 구비하거나 전산화를 통하여 장비의 반・출입 내역을 기록으로 보관하고 유지하여야 한다.

- 기록에는 일시, 품명 및 수량, 반・출입 담당자, 반・출입 장소, 반・출입 사유, 관리부서 확인 및 서명 등과 내용을 포함

통제항목	8.2.6 장비 폐기 및 재사용		
세부통제내용	정보처리시설 내의 저장 매체를 포함하여 모든 장비를 파악하고, 민감한 데이터가 저장된 장비를 폐기하는 경우 복구 불가능하도록 하여야 한다. 또한 재사용하는 경우에도 복구 불가능 상태에서 재사용하여야 한다.		
점검항목	1) 저장매체의 장비폐기에 대한 절차를 수립·이행해야 하며 저장매체 폐기 및 재사용 시 정보가 복구되지 않도록 처리하고 있는가? 2) 자체적으로 저장매체를 폐기할 경우 관리대장을 통해 폐기이력을 남기고 폐기확인증적을 함께 보관하고 있는가? 3) 외부업체를 통해 저장매체를 폐기할 경우 폐기 절차를 계약서에 명시하고 완전한 폐기에 대한 확인을 하고 있는가?		
신청기관 준비사항 (관련증적)	• 저장매체 폐기 절차 • 저장매체 데이터 삭제 관련 증적 • 공공용 저장매체 재사용 시 보관 관련 증적 • 저장매체 폐기 관리대장 • 폐기 확인 증적	참고사항 (샘플자료)	• 정보보호 정책서 • 물리적보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 저장매체에 대한 폐기절차를 수립하고 이행하여야 한다.
- 폐기 기준 수립
- 폐기 방법(물리적, 전자적으로 완전 파괴)
- 폐기 담당자 명시 등

■ 공공용 클라우드컴퓨팅 시스템에서 사용된 저장매체를 재사용 또는 폐기하기 위하여 보관할 경우 민간용과 별도 분리·보관하여야 한다.

■ 공공용 클라우드컴퓨팅 시스템에서 사용된 저장매체를 재사용할 경우 공공용 클라우드컴퓨팅 시스템 내에서만 사용하여야 한다.

■ 저장매체 재사용시에는 오버라이팅, 로우레벨 포맷 등을 통하여 복구 불가능한 상태에서 재사용하여야 한다.

⇨ 점검항목 2)

■ 자체적으로 폐기하는 경우 폐기이력을 기록으로 유지하여야 하며, 폐기에 대한 책임자의 확인을 득해야 한다.

- 폐기일자
- 폐기 담당자, 확인자(책임자) 서명
- 폐기방법
- 폐기확인증적(동영상, 사진 등) 등

⇨ 점검항목 3)

■ 외부업체를 통해 저장매체를 폐기할 경우 내부 폐기절차와 상응하는 내용을 계약서에 반영하여야 한다.

■ 외부업체가 폐기절차를 준수하는지 감독하여야 하며, 폐기에 대한 증적(예: 사진, 동영상 등)을 보관・유지하여야 한다.

9. 가상화 보안

9.1 가상화 인프라

통제항목	9.1.1 가상자원 관리		
세부통제내용	가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리방안을 수립하여야 한다.		
점검항목	1) 가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리방안을 수립 및 이행하고 있는가? 2) 가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 승인, 책임추적성 확보 방안 및 주기적 점검을 이행하고 있는가?		
신청기관 준비사항 (관련증적)	• 가상자원 관리 절차 및 방법 • 가상자원 점검내역 • 이용자 가상자원 완전 삭제 관련 증적	**참고사항 (샘플자료)**	• 정보보호 정책서 • 가상화보안관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ **점검항목 1)**

■ 가상자원의 생성, 변경, 회수 등에 대한 관리방안을 수립하고 운영하여야 한다.

- 가상자원 생성/변경/회수 등에 대한 절차 및 방법

구분	고려사항
가상자원 생성	가상자원 접근통제 가상 소프트웨어 이미지 등록 절차 가상 소프트웨어 이미지 등록, 배포 담당자 가상 소프트웨어 이미지, 스냅샷 저장 장소 가상 소프트웨어 이미지, 스냅샷의 공유 금지 가상 소프트웨어 이미지, 스냅샷의 안전성 (바이러스 검사, 보안 업데이트, 패치 등)
가상자원 변경	다른 가상자원에 대한 영향 등 고려
가상자원 회수	가상자원 회수 절차 및 방법 비정상적인 회수 대책 가상자원 회수 기록 관리 등

➪ **점검항목 2)**

■ 가상자원을 생성/변경/회수할 때 승인절차가 마련되어야 한다.

■ 가상자원의 생성/변경/회수에 대하여 주기적으로 점검을 수행하고 점검 이력을

남겨야 한다.

- 예) 점검사항으로는 가상자원의 생성/변경/회수에 대한 책임자의 승인 여부, 담당자의 실행 여부, 업무 수행 이슈가 발생한 경우 사후조치를 수행하였는지 여부, 승인된 범위를 벗어난 생성/변경/회수 등이 발생했는지 등 점검

통제항목	9.1.2 가상자원 회수		
세부통제내용	이용자와의 계약 종료 시 가상자원 회수 절차에 따라 백업을 포함한 모든 클라우드 시스템에서 삭제하여야 한다.		
점검항목	1) 이용자의 가상자원의 처분에 대한 내용을 클라우드 서비스 수준 협약(SLA) 및 계약서에 반영하고 있는가? 2) 이용자의 가상자원 회수 시 모든 가상자원은 클라우드 환경에서 완전 삭제 되는가?		
신청기관 준비사항 (관련증적)	• 계약서 및 SLA • 이용자 가상자원 회수 절차 • 이용자 가상자원 완전 삭제 기법 설명 증적	참고사항 (샘플자료)	• 정보보호 정책서 • 가상화보안관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ **점검항목 1)**

■ 클라우드 서비스 계약서 및 수준협약(SLA)에 서비스 이용 계약 종료에 따른 모든 가상자원(백업된 가상자원 포함)의 완전삭제의 내용이 포함되어 있어야 한다.

➪ **점검항목 2)**

■ 계약 종료에 따른 가상자원 회수절차를 수립하여야 한다. 해당 절차에는 이용자의 모든 가상자원(백업된 가상자원 포함) 및 이용자의 데이터(백업 데이터 포함)가 삭제될 수 있도록 절차를 마련하고 절차에 따라 수행하여야 한다.

통제항목	9.1.3 가상자원 모니터링		
세부통제내용	가상자원에 대한 무결성 보장하기 위한 보호조치 및 가상자원의 변경(수정, 이동, 삭제, 복사)에 대해 모니터링 하여야 한다. 또한, 가상자원에 손상이 발생한 경우 이를 이용자에게 알려주어야 한다.		
점검항목	1) 가상자원에 대한 무결성을 보장하기 위한 보호조치 및 모니터링을 수행하고 가상자원 손상 시 이용자에게 통지하기 위한 절차가 마련되어 있는가?		
신청기관 준비사항 (관련증적)	• 가상자원 무결성 보장 방안 (보호조치 및 모니터링) • 가상자원 모니터링 결과 • 손상 발견 시 이용자 통지 절차	**참고사항 (샘플자료)**	• 정보보호 정책서 • 가상화보안관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 가상자원의 무결성을 보장하기 위한 보호대책을 수립하고 이행하여야 한다.
- 가상자원(스냅샷이나 이미지 등)의 비인가된 변경을 방지하고, 무단변경을 탐지하기 위해 해시, 체크섬 등을 이용한 무결성 변경 방지
- 동일 하이퍼바이저에서 동작하는 각각의 가상머신이 사용하는 메모리 공유 금지

■ 가상자원의 생성, 이동, 삭제, 복사 등 변경에 대하여 모니터링 체계를 갖추고 이행하여야 한다.
- 가상자원의 생성, 이동, 삭제, 복사 등은 책임자의 승인하에 이루어져야 하며, 인가된 관리자가 작업을 수행해야 한다.
- 가상자원의 생성, 이동, 삭제, 복사 등의 작업에 대하여 승인된 작업만 이루어지는지 모니터링을 수행하여야 한다.

■ 가상서버의 생성, 변경, 삭제, 상태(동작여부) 등의 현황을 전자적 방법(예: 포털) 등을 통해 이용자에게 알려주어야 한다.

■ 가상자원에 손상이 발생하는 경우 이용자에게 통지하기 위한 절차를 수립하고 이행하여야 한다.
- 가상자원에 손상이 발생하는 경우 지체없이 해당 이용자에게 손상에 대한 통지를 수행해야 한다.
- 손상에 대한 책임이 있는 책임자의 연락처, 손상의 범위, 손상으로 인한 피해 등의 내용을 통보해야 한다.

통제항목	9.1.4 하이퍼바이저 보안		
세부통제내용	가상자원을 관리하는 하이퍼바이저의 기능 및 인터페이스에 대한 접근 통제 방안을 마련하여야 한다. 또한 하이퍼바이저에 대한 소프트웨어 업데이트 및 보안패치를 최신으로 유지하여야 한다.		
점검항목	1) 하이퍼바이저를 보호하기 위한 보호조치 및 시스템 관리 인터페이스에 대한 접근을 통제하고 있는가? 2) 하이퍼바이저 운영자의 권한 오남용을 방지하기 위해 지속적으로 탐지하고 통제하기 위한 방안을 마련하고 있는가? 3) 바이러스, 웜, 트로이목마 등의 악성코드로부터 하이퍼바이저를 보호하기 위한 방안을 마련하고 있는가?		
신청기관 준비사항 (관련증적)	• 하이퍼바이저 접근통제 및 보호대책 방안 • 하이퍼바이저 접근 기록 검토 증적	참고사항 (샘플자료)	• 정보보호 정책서 • 가상화보안관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ **점검항목 1)**

■ 가상자원 관리를 위하여 하이퍼바이저에 대한 보호조치를 수립하여 적용하여야 한다.

- 하이퍼바이저에 대한 최신 업데이트 적용
- 하이퍼바이저 관리기능에 대한 접근통제
  - 2-Fact 인증 적용, 원격관리의 경우 접근 IP 제한, 전용 관리단말 지정 등
  - 원격관리의 경우 통신 구간에 대한 보호대책 적용(암호통신 등)
  - 접속 및 작업 로그 생성 및 보관
- 비인가된 소프트웨어 설치 금지
- 주기적인 하이퍼바이저 로그 분석

■ 클라우드시스템 관리 인터페이스에 대한 접근을 제한하여야 한다.

- 방화벽을 사용한 제한된 콘솔 접근
- 다중요소인증, IP 주소 필터링 등을 통한 접근제어
- 하이퍼바이저 접근을 위한 관리망을 별도로 구성
- 하이퍼바이저 원격 접속 관리 비활성화 또는 원격 접근이 필요 시에는 암호화된 통신 수단을 사용

➪ **점검항목 2)**

■ 관리자(운영자)에게 관리권한을 제공하는 경우 최소한의 관리기능만 사용할 수

있도록 하여야 한다.

■ 관리행위에 대한 로그를 남기고 로그에 대한 주기적인 검토를 통해 위반 사항을 탐지할 수 있는 방안을 수립하여 적용하여야 한다.

⇨ 점검항목 3)

■ 하이퍼바이저가 설치된 시스템에는 악성코드 탐지를 위한 백신 프로그램을 설치하여야 하며, 백신 프로그램은 최신의 버전을 유지할 수 있도록 하여야 한다.

■ 악성코드 감염 시에 대한 대응방안(격리 등)을 수립하여야 한다.

통제항목	9.1.5 공개서버 보안		
세부통제내용	가상자원을 제공하기 위한 웹사이트와 가상소프트웨어(앱, 응용프로그램)를 배포하기 위한 공개서버에 대한 물리적, 기술적 보호대책을 수립하여야 한다.		
점검항목	1) 웹서버 등 공개 서버를 운영하는 경우 이에 대한 보호대책을 마련하고 있는가? 2) 공개서버는 내부 네트워크와 분리된 DMZ(Demilitarized Zone) 영역에 설치하고 침입차단시스템 등 보안시스템을 통해 보호하고 있는가? 3) 공개서버의 취약점 점검을 주기적으로 수행하고 발견된 취약점을 조치하고 있는가?		
신청기관 준비사항 (관련증적)	• 네트워크 및 시스템 구성도 • 보안시스템 운영 현황 • 취약점 점검 및 조치 현황	참고사항 (샘플자료)	• 정보보호 정책서 • 가상화보안관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ **점검항목 1)**

■ 공개 서버(웹서버, 배포 서버 등)를 운영하는 경우 아래 보호 대책을 참고하여 적용하여야 한다.

- 공개 서버의 경우 서비스별 전용으로 서버를 운영
- 웹서버를 통한 개인정보 송·수신 시 TLS V1.2 이상 적용
- IPTABLES, PodSecurityPolicy, Container Network Interface 등을 이용한 접근통제 및 식별 및 인증을 통한 권한 설정
- 백신 설치 및 OS 최신 패치
- 불필요한 서비스 제거 및 포트 차단
- 불필요한 소프트웨어·스크립트·실행파일 등 설치 금지 등
- 불필요한 페이지(테스트 페이지) 및 에러처리 미흡에 따른 시스템 정보 노출 방지

⇨ **점검항목 2)**

■ 공개 서버(웹서버, 배포 서버 등)는 DMZ 영역에 설치하고 공개 서버가 침해당하더라도 공개 서버를 통한 내부 네트워크 침입이 불가능하도록 접근통제 정책을 적용하여야 한다.

- DMZ의 공개 서버가 내부 네트워크에 위치한 DB, WAS(Web Application Server) 등의 정보시스템과 접속이 필요한 경우, 엄격한 접근통제 정책 적용
- 침입차단시스템의 정책은 서비스를 위한 최소 서비스만 허용하도록 설정 관리

⇨ 점검항목 3)

■ 공개서버의 취약점 점검은 인증기준 “3.3.2. 취약점 점검” 통제항목의 취약점 점검절차에 따라 수행하여야 한다.

- OS, 어플리케이션, 웹서비스 등에 대한 취약점 점검 수행
- 웹서버의 경우 OWASP TOP 10등 웹 응용프로그램 취약점 점검
- 발견된 취약점은 신속하게 조치

통제항목	9.1.6 상호 운용성 및 이식성		
세부통제내용	클라우드컴퓨팅서비스 제공자는 표준화된 가상화 포멧, 이식성이 높은 가상화 플랫폼, 공개 API 등을 이용하여 클라우드컴퓨팅서비스 간의 상호 운용성 및 이식성을 높여야 한다.		
점검항목	1) 상용 운용성 및 이식성을 높이기 위한 조치(표준화된 가상화 포멧, 이식성이 높은 가상화 플랫폼, 공개 API) 들을 취하고 있는가?		
신청기관 준비사항 (관련증적)	• 가상화보안관리지침 • 클라우드 상호 운영/이식성 제공 방안(가상화 포맷, 플랫폼, API 등)	참고사항 (샘플자료)	• 정보보호 정책서 • 가상화보안관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ 점검항목 1)

■ 클라우드서비스 제공자는 표준화된 가상화 플랫폼, API 등을 지원하여 클라우드서비스 간의 이식성 및 상호 운용성을 지원해야 한다.

- 가상화 플랫폼은 표준화된 플랫폼 적용
  - ・OVF(Open Virtualization Format)
  - ・OVA(Open Virtualization Application/Appliance) 등
- 공개된 API 사용 및 마이그레이션 응용프로그램 도입
  - ・공개된 API는 공격의 정보로 사용될 수 있으므로 이에 대한 클라우드 서비스를 설계하는 단계에서부터 보안대책을 수립한 후 적용

9.2 가상 환경

통제항목	9.2.1 악성코드 통제		
세부통제내용	바이러스, 웜, 트로이목마 등의 악성코드로부터 이용자의 가상 환경(가상 PC, 가상서버, 가상 소프트웨어 등)을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술을 지원하여야 한다. 또한 이상징후 발견 시 이용자 통지하고 사용 중지 및 격리 조치를 수행하여야 한다.		
점검항목	1) 바이러스, 웜, 트로이목마 등의 악성코드로부터 가상 환경을 보호하기 위한 기술을 도입 또는 지원하고 있는가? 2) 이상 징후 발견 시 이용자에게 통지하고 사용 중지 및 격리 조치를 수행하고 있는가?		
신청기관 준비사항 (관련증적)	• 정보자산 목록 (백신, 웹쉘탐지, 웹방화벽 등 설치된 악성코드 통제 보안시스템 목록) • 이상 징후 발견 시 통지 및 조치 절차	참고사항 (샘플자료)	• 정보보호 정책서 • 가상화보안관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 바이러스, 웜, 트로이목마 등의 악성코드로부터 이용자의 가상 환경을 보호하기 위한 보안기술을 지원하여야 한다.

- 보안시스템(백신, 이메일 보안, 웹쉘탐지, 웹방화벽 등) 설치 및 최신업데이트
- 운영체제의 보안업데이트
- 서비스되는 SW(WAS, DB 등) 최신 보안패치 등

⇨ **점검항목 2)**

■ 이용자의 가상 환경에서 이상 징후가 발견되는 경우 이용자에게 통지하고 사용 중지 및 격리 조치를 수행하여야 한다.

- 바이러스, 웜, 트로이목마 등 악성코드가 발견된 시스템은 즉시 사용을 중단하고, 타 시스템과 격리(네트워크 분리)
- 다른 시스템에 악성코드가 전파되었는지 점검 수행
- 가능한 경우 감염경로를 파악하고 보안대책을 수립하여 조치
- 서비스에 영향을 미치는 경우 이용자에게 통지

통제항목	9.2.2 인터페이스 및 API 보안		
세부통제내용	가상 환경(가상 PC, 가상서버, 가상 소프트웨어 등) 접근을 위한 인터페이스 및 API에 대한 보안취약점을 주기적으로 분석하고, 이에 대한 보호 방안을 마련하여야 한다.		
점검항목	1) 가상 환경(가상 PC, 가상서버, 가상 소프트웨어 등) 접근을 위한 인터페이스 및 API에 대한 보호 방안을 마련하고 있는가?		
신청기관 준비사항 (관련증적)	• 가상 환경 인터페이스(API) 취약점 점검 및 조치 현황	참고사항 (샘플자료)	• 정보보호 정책서 • 가상화보안관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 전송, 권한 및 인증, 소프트웨어 개발, 메시지 보호 측면에서의 인터페이스 및 API 취약점 분석, API 간 연관성 분석을 주기적으로 수행하고 보완하여야 한다.

통제항목	9.2.3 데이터 이전		
세부통제내용	이용자가 기존 정보시스템 환경에서 클라우드컴퓨팅서비스의 가상 환경으로 전환 시 안전하게 데이터를 이전하도록 암호화 등의 기술적인 조치방안을 제공하여야 한다.		
점검항목	1) 기존 정보시스템 환경에서 가상 환경으로 데이터 이전 시, 안전하게 이전하고 있는가?		
신청기관 준비사항 (관련증적)	• 전송구간 암호화 솔루션 운영 현황(예: VPN 등) • 데이터 이전 시 보안대책	참고사항 (샘플자료)	• 정보보호 정책서 • 가상화보안관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 가상 환경으로 이용자의 데이터를 이전하는 경우 다음과 같은 기술적 방안을 마련하여야 한다.

- 안전한 암호화 통신채널(예: 전용회선, VPN 등) 적용

■ 수동으로 이용자 데이터를 이전하는 경우 이동매체의 안전한 전달, 이동매체에 데이터 저장 시 암호화, 이동 간의 데이터 무결성 확보 등의 보안대책을 수립하여야 한다.

통제항목	9.2.4 가상 소프트웨어 보안		
세부통제내용	클라우드컴퓨팅서비스 제공자는 출처, 유통경로 및 제작자가 명확한 소프트웨어로 구성된 가상 환경을 제공하여야 한다.		
점검항목	1) 가상 환경 내에 출처, 유통경로 및 제작자가 명확하지 않은 가상 소프트웨어의 설치를 방지하고 있는가? 2) 허가 받지 않은 소프트웨어 설치가 탐지된 경우 이용자에 알리기 위한 연락체계가 수립하고 있는가?		
신청기관 준비사항 (관련증적)	• 정보자산목록 (가상 환경 관련 소프트웨어) • 소프트웨어 패치관리대장 • 공공기관 제공 필수 SW 현황	참고사항 (샘플자료)	• 정보보호 정책서 • 가상화보안관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ 점검항목 1)

■ 출처, 유통경로 및 제작자가 명확한 소프트웨어를 이용하여 가상 환경을 제공해야 한다.

- 최초 이미지 배포 시 승인된 소프트웨어만 설치 및 배포
- 출처가 불명확한 소프트웨어, 검증되지 않은 프리웨어 소프트웨어, 오픈소스 소프트웨어 등은 설치 금지
- 라이선스가 없거나 EOL 소프트웨어 등은 설치 금지

■ 설치된 소프트웨어는 소프트웨어 제작사가 제공하는 보안패치 및 업데이트를 적용하여야 한다.

⇨ 점검항목 2)

■ 클라우드컴퓨팅서비스 제공자가 제공한 이미지 내에 허가받지 않은 소프트웨어 설치가 탐지된 경우 이용자에게 신속하게 알려야 한다.

10. 접근통제

10.1 접근통제 정책

통제항목	10.1.1 접근통제 정책 수립		
세부통제내용	비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다.		
점검항목	1) 접근 통제영역을 정의하고 접근 통제영역별로 접근통제 정책을 수립하고 있는가? (접근통제 영역별 통제 규칙, 방법, 절차, 예외사항에 대한 안전한 관리절차 등)		
신청기관 준비사항 (관련증적)	• 접근통제 정책 및 방안 • 관리자 단말기 현황	참고사항 (샘플자료)	• 정보보호 정책서 • 접근통제관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ **점검항목 1)**

■ 클라우드서비스 운영 서버, 개발 서버, 정보보호시스템, 이용자 또는 사용자 데이터 등에 대한 접근통제 정책을 수립하여야 한다.
- 접근통제 대상에 따라 접근에 대한 권한과 책임을 명시
- 주요 서버 또는 중요 데이터에 접근하는 경우 two-fact 인증 고려
- 시스템별 계정을 명확히 식별하고 안전한 접근수단 적용
- 원격 접속 구간에 대한 통신 암호화 또는 VPN 적용
- 클라우드서비스 보안 설정 기준(인증, 암호화, 세션 관리, 접근통제, 장기미사용 잠금 등)
- 서비스의 중요도에 따른 영역 간 접근통제 적용

■ 관리서버의 경우 보다 강력한 인증을 고려하여야 한다.

■ 업무상 불가피하게 접근통제 정책을 벗어난 접근이 필요한 경우 접근시간, 접근위치 제한 등 추가적인 보완대책을 마련한 후 접근을 허용하여야 한다.
- 접근통제 정책 예외 시 책임자 승인 필요
- 접근통제 정책 예외 시 책임자 승인, 허가기간 등의 이력 보관

■ 클라우드서비스 운영 서버에 접근 가능한 관리용 단말을 지정하고 무선을 통한 접근은 차단하여야 한다.
- 관리시스템 접근 가능한 단말을 관리용 단말로 지정하고 목록 관리
- 접속 가능한 단말의 IP주소, MAC 주소 등으로 제한

통제항목	10.1.2 접근기록 관리		
세부통제내용	접근기록 대상을 정의하고 서비스 통제, 관리, 사고 발생 책임추적성 등을 보장할 수 있는 형태로 기록되고 유지하여야 한다.		
점검항목	1) 클라우드 시스템의 사용자/관리자 접속 내역을 기록하고, 접근의 타당성을 정기적으로 검토하고 있는가?		
신청기관 준비사항 (관련증적)	• 접근기록 생성 대상 목록 • 접근기록 검토 내역 (보안로그)	참고사항 (샘플자료)	• 정보보호 정책서 • 접근통제관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ 점검항목 1)

■ 접근기록을 생성하여 보관해야 하는 대상시스템을 정의하고 목록화하여 관리하여야 한다. 대상시스템은 서비스 및 업무 중요도를 고려하여 접근기록의 보존이 필요한 대상을 정의한다.

■ 보안사고의 사후 조사 지원 등 책임추적성 확보를 위해 클라우드시스템의 접근기록은 도입 공공기관의 정책에 따라 일정기간 동안 보관하여야 한다.

■ 최소 대상시스템에서 생성된 접근기록(보안로그)는 최소 1년 이상 유지• 관리하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관・관리하여야 한다. 접근권한 부여 기록은 최소 3년 보관하여야 한다.

■ 접근권한 부여, 수정, 삭제 등과 관련된 기록은 법률 및 도입 공공기관의 정책을 준수하여야 한다.

※ 접근권한 부여 기록 보관 기한 예시

법률	보관 기간
개인정보보호법에 따른 개인정보처리자	최소 3년간 보관
정보통신망법에 따른 정보통신서비스 제공자 등	최소 5년간 보관

■ 접근기록은 사고 발생 시 책임추적성을 보장할 수 있도록 다음의 사항을 포함하여 생성되고 보존되어야 한다.

- 접근 주체 정보(계정 등)
- 접근시간
- 접근 IP 또는 MAC 정보
- 수행업무(접근데이터 정보, 접근 후 활동 정보 등)
- 처리한 정보주체 정보

■ 기록된 접근기록은 통제항목 ‘7.2.2. 감사기록 및 모니터링’의 점검항목과 함께 검토되어야 하며 개인정보처리시스템의 접근기록 등은 월 1회 이상 점검되어야 한다. 기타 접근기록은 도입 공공기관의 정책 또는 클라우드컴퓨팅서비스 제공자의 정책, 지침에 따라 정기적으로 검토하여야 한다.

10.2 접근권한 관리

통제항목	10.2.1 사용자 등록 및 권한 부여		
세부통제내용	클라우드 시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다.		
점검항목	1) 클라우드 시스템 내 사용자 계정에 대한 등록•변경•삭제에 관한 공식적인 검토•승인 절차가 있는가? 2) 클라우드 시스템의 사용자 계정 생성 및 변경 시 직무별, 역할별 접근권한 분류 체계를 수립하고 있으며, 업무상 필요한 최소한의 권한만을 부여하고 있는가?		
신청기관 준비사항 (관련증적)	• 사용자 계정 등록, 변경, 삭제 승인 절차 및 승인 내역 • 접근권한 분류체계 • 접근권한 부여 기록	**참고사항 (샘플자료)**	• 정보보호 정책서 • 접근통제관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ **점검항목 1)**

■ 사용자 계정을 등록•변경•삭제(비활성화)하는 경우 공식적으로 검토•승인하는 절차를 수립하여야 한다.

- 계정 발급 시 해당 계정 발급의 적정성 검토 절차
- 관리자 또는 특수권한 사용자(개인정보취급자 등)에 대한 계정 발급 및 변경에 대한 적정성 검토 절차
- 발급된 계정의 접근범위 및 권한 등에 대한 사항 검토 절차
- 전보, 퇴직 등 인사이동 발생 시 계정 삭제 등의 절차
- 책임자의 승인 절차
- 임시 계정 발급 (접근위치, 사용기간 등 관리) 절차
- 접근권한 부여 기록에 대한 보관

※ 접근권한 부여 기록 보관 기한 예시

법률	보관 기간
개인정보보호법에 따른 개인정보처리자	최소 3년간 보관
정보통신망법에 따른 정보통신서비스 제공자 등	최소 5년간 보관

➪ **점검항목 2)**

■ 직무별, 역할별, 서비스 유형별 등 클라우드 시스템 접근권한을 정의한 분류 체계를 수립하고 관리하여야 한다.

- 불필요하거나 과도하게 중요 정보 또는 개인정보에 접근하지 못하도록 권한 세분화

※ 접근권한 분류 체계 예시

구분	서비스 그룹	담당	조회	수정	삭제	다운로드	권한부여
최고 관리자	A 서비스	홍OO	○	○	○	○	○
	B 서비스	홍OO	○	○	○	○	○
서브 관리자	A 서비스	이OO	○	○	○	○	○
	B 서비스	강OO	○	○	○	○	○
사용자	A 서비스	유OO	○	○	○	○	
	A 서비스	김OO	○				
	B 서비스	박OO	○	○	○	○	
	B 서비스	정OO	○				

■ 접근권한은 업무 수행에 필요한 최소한으로 할당하여야 하며, 담당자 직무에 따라 차등 부여하여야 한다.

- 정보 시스템 운영직무와 개발 직무 간 접근계정 분리, 민간 및 공공기관 클라우드컴퓨팅 시스템 간 접근계정 분리 등

※ 권한 최소 부여 및 현황 관리 예시

- 업무상 불필요한 직무자(계정)에게 권한 부여 여부 (업무 변경, 부서 변경, 퇴직자 등)
- 수행 직무, 역할별 권한 차등 부여
- 마지막 접속 후 장기간(예, 3개월 이상) 미접속된 계정
- 시스템 슈퍼 어드민 권한 등을 팀내 전체 인원에게 부여하는 경우 적절한 사유 등을 주기적으로 검토, 현황 관리 (업무 수행을 위한 필요성과 업무 수행을 위한 최소한의 권한만 부여하도록 관리)

통제항목	10.2.2 관리자 및 특수 권한 관리		
세부통제내용	클라우드 시스템 및 중요정보 관리, 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.		
점검항목	1) 관리자 및 특수 권한은 최소한의 인원에게만 부여하고, 권한 부여 시 책임자 승인 절차를 수립하고 있는가? 2) 관리자 권한 및 특수 권한을 식별하여 별도 목록으로 관리하고 있는가? 3) 외부자에게 부여하는 계정은 한시적으로 부여하고, 사용이 끝난 후에는 즉시 삭제 또는 정지하고 있는가?		
신청기관 준비사항 (관련증적)	• 사용자 계정 등록, 변경, 삭제 승인 내역 • 접근권한 부여 기록 • 특수권한자 목록 • 외부자에게 부여된 계정 목록	참고사항 (샘플자료)	• 정보보호 정책서 • 접근통제관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

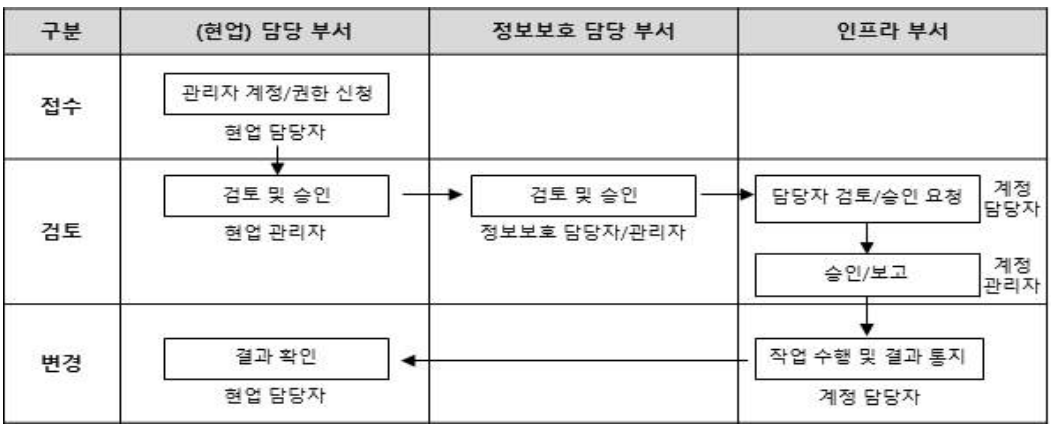
점검항목 해설

⇨ 점검항목 1)

■ 클라우드 시스템의 관리자(root, administrator 등) 및 특수권한(계정 및 접근 설정 권한 등)을 갖는 계정을 할당하는 경우 책임자로부터 승인을 받은 후 계정을 할당하여야 한다.

- 관리자 및 특수권한을 부여하는 경우 공식적인 절차에 따라 신청 및 승인이 이루어질 수 있도록 절차를 수립하여 이행
- 관리자 및 특수권한을 부여하는 경우 일반적인 사용자 계정•권한 발급 절차보다 엄격한 기준 적용(임원 또는 정보보호 최고책임자 승인 등)

※ 관리자 계정/권한 절차 예시



➪ **점검항목 2)**

■ 할당된 관리자 권한 및 특수권한을 목록화하여 관리하여야 한다.

- 특수권한은 반드시 필요한 경우에만 할당
- 특수권한의 최소화 및 모니터링을 위해 특수권한을 부여받은 계정 식별 및 현황 관리

※ 관리자 및 특수권한 예시

- 시스템(서버, 데이터베이스, 네트워크 등)의 관리자
- 정보보호시스템의 관리자
- 응용프로그램 배치 및 구동을 위한 사용되는 계정
- 응용프로그램의 관리자 (권한 부여, 수정, 삭제 등 권한 보유)
- 응용프로그램의 이용자 (수정, 삭제, 다운로드 등 가능한 자와 조회만 가능한 자 분류)

※ 관리자 계정 목록 예시

No	시스템 명	아이디	사용자	부서	용도	비고
1	A 서버(hostname1)	sample1	홍길동	A팀	운영	
2	B 서버(hostname2)	sample2	김철수	B팀	개발	
이하 생략						

➪ **점검항목 3)**

■ 정보 시스템 유지보수 등을 위해 외부자에게 계정 및 접근권한을 부여하는 경우 사용기간, 접근위치 등을 제한하여 발급하고, 관련 업무 활동이 종료된 이후 해당 계정을 즉시 삭제하거나 사용을 정지시켜야 한다.

- 내•외부자의 권한을 구분하여 별도 그룹으로 관리

통제항목	10.2.3 접근권한 검토		
세부통제내용	클라우드 시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 점검하여야 한다.		
점검항목	1) 클라우드 시스템에 대한 접근권한 검토 기준, 검토주체, 검토방법, 주기 등을 정하여 정기적 검토를 이행하고 있는가? 2) 접근권한의 검토 결과 접근권한 오남용 등의 이상 징후가 발견된 경우 그에 따른 조치절차를 수립•이행하고 있는가?		
신청기관 준비사항 (관련증적)	• 접근권한 검토 이력 (접근권한 점검대장) • 이상 징후 발견 시 조치 절차	참고사항 (샘플자료)	• 정보보호 정책서 • 접근통제관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 할당된 계정 및 접근권한이 적절한지 주기적으로 검토를 수행하여야 한다.

- 클라우드서비스의 환경변화 또는 관련 직원의 인사변경(퇴직, 휴직, 전보 등) 등 반영 여부
- 장기간 미사용(3개월 권고) 계정의 존재 여부
- 외부자에게 할당된 계정의 관리 상태
- 계정 및 권한 할당 시 승인 등의 절차 준수 여부
- 직무의 변경 등이 발생한 경우 계정 또는 접근권한의 회수 및 재할당
- 계정 등록대장과 실 시스템 계정 일치 여부
- 직무 변경 등에 따른 접근권한 승인 내역
- 임시 계정 권한 회수 여부

■ 검토 기준별로 검토주체, 방법, 주기(최소 분기 1회 이상 권고) 등을 정하여 이행하여야 한다.

⇨ 점검항목 2)

■ 접근권한 검토 결과 의심스러운 상황이 발견된 경우 원인분석, 보완대책 마련, 보고 등 절차를 수립, 이해하여야 한다.

- 과다한 권한부여, 오남용, 계정 및 권한 할당 시 승인절차 미준수 등 의심스러운 상황
- 검토 후 변경 적용된 권한에 대해서는 사용자 및 관련자에게 통지
- 이상 징후 발생 시 그 성격에 따라 선 조치 후 보고 실시
- 권한변경관리대장(직무변경, 입퇴사자)을 기준으로 이상 징후 확인

10.3 사용자 식별 및 인증

<table>
<tr><th>통제항목</th><th colspan="3">10.3.1 사용자 식별</th></tr>
<tr><td>세부통제내용</td><td colspan="3">클라우드 시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다. 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.</td></tr>
<tr><td>점검항목</td><td colspan="3">1) 클라우드 시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고, 추측 가능한 식별자의 사용을 제한하고 있는가?
2) 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받고 있는가?</td></tr>
<tr><td>신청기관
준비사항
(관련증적)</td><td>• 시스템 관리자 계정 관리 대장
• 공용 계정 관리대장
• 공용 계정 발급 승인 내역</td><td>참고사항
(샘플자료)</td><td>• 정보보호 정책서
• 접근통제관리지침</td></tr>
<tr><td colspan="2">ISMS-P 인증 취득 시 심사 생략 가능 대상</td><td colspan="2">O</td></tr>
</table>

점검항목 해설

➪ **점검항목 1)**

■ 클라우드 시스템은 사용자를 유일하게 구분할 수 있는 식별자(아이디)를 할당하여 모든 사용자의 책임추적성을 보장하여야 한다.

- 시스템 설계 시에 유일한 식별자 발급에 대한 부분을 고려
- 관리자 및 특수권한 계정은 추측 가능한 식별자(root, administrator 등) 사용은 제한
- 시스템 설치 후 제조사 또는 판매사의 기본계정 및 시험계정 등은 제거 또는 추측이 어려운 계정으로 변경하여 사용
- 기본 계정 사용 시 별도의 통제방안 마련

➪ **점검항목 2)**

■ 클라우드 시스템 관련 업무상 불가피하게 계정을 공유하여 사용할 경우, 사유와 타당성을 검토하여 책임자의 승인을 받아야 하며 책임추적성을 보장할 추가적인 통제방안을 적용하여야 한다.

- 공유 계정 사용 시 사용자의 식별을 위한 추가 접근 통제방안 마련

통제항목	10.3.2 사용자 인증		
세부통제내용	클라우드 시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증절차에 의해 통제하여야 한다.		
점검항목	1) 클라우드 시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증절차에 의해 통제하고 있는가? 2) 싱글사인온 등의 인증 방법을 사용하는 경우, 이에 대한 별도의 보호대책을 수립하고 있는가?		
신청기관 준비사항 (관련증적)	• 사용자 인증 화면 • 로그인 횟수 제한 설정 또는 제한된 화면 • 불법 로그인 시도 경고 화면 • 강화된 인증 수단 제공 화면	참고사항 (샘플자료)	• 정보보호 정책서 • 접근통제관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 클라우드 시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증절차에 의해 통제하여야 한다.

- 시스템 설계 시에 사용자 인증 시 통제방안 고려
- 공개 인터넷망을 통해 접속하는 포탈의 경우 아이디, 패스워드 기반 이외에 강화된 인증수단(OTP, 공인인증서 등) 적용 고려
- 법적 요구사항에 따른 강화된 인증방식 사용이 필요한 경우 준수

⇨ 점검항목 2)

■ 싱글사인온 등 다양한 정보 시스템에 대한 사용자 인증을 용이하게 하는 시스템을 운영하는 경우 병목 및 침투(인증 도용 등) 시 피해 확대 가능성이 있으므로 별도의 보안대책(주요 정보 시스템 재인증, 강화된 인증 적용 등)을 마련하여야 한다.

통제항목	10.3.3 강화된 인증 수단 제공		
세부통제내용	이용자가 클라우드컴퓨팅서비스에 대해 다중 요소 인증 등 강화된 인증 수단을 요청하는 경우 이를 제공하기 위한 방안을 마련하여야 한다.		
점검항목	1) 이용자 요구 시 인증(PKI)기반, OTP, 지문 등 다중 인증 수단을 제공할 수 있는가?		
신청기관 준비사항 (관련증적)	• 추가 인증수단 적용 화면 (OTP, 전자 우편 인증 등)	참고사항 (샘플자료)	• 정보보호 정책서 • 접근통제관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ 점검항목 1)

■ 이용자 요구 시 인증(PKI)기반, OTP, 지문 등 다중 인증 수단을 제공할 수 있도록 방안을 마련하여야 한다.

■ 정보통신망을 통해 외부에서 클라우드컴퓨팅서비스 시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

■ 이용자/사용자가 접근하는 모든 외부 인터페이스에 패스워드 복잡도와 상관 없이 강화된 인증수단이 기본 적용되어야 합니다.

- 공공서비스 제공자(공공기관의 클라우드서비스 관리자 및 임직원, 공공기관에 용역서비스를 제공하는 업체 임직원(인증범위의 클라우드서비스를 이용하는 경우)): 다중 요소인증 기본 사용
- 클라우드컴퓨팅 서비스를 통해 제공되는 대민 서비스를 이용하는 자: 다중 요소인증 의무 적용 대상자는 아님

※ 인증수단 예시

- 추가 인증수단: OTP, 휴대폰 SMS 인증, 공인인증서, 전자 우편 인증코드
- 추가 통제방안: IP(국가)제한, MAC제한, 브라우저 제한

통제항목	10.3.4 패스워드 관리		
세부통제내용	법적 요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경 주기 등 사용자 및 이용자 패스워드 관리 절차를 수립·이행하고 패스워드 관리 책임이 사용자 및 이용자에게 있음을 주지시켜야 한다. 특히 관리자 패스워드는 별도 보호대책을 수립하여 관리하고, 이용자 패스워드 관리절차는 공지하여야 한다.		
점검항목	1) 클라우드 시스템 또는 서비스에 대해 보안성 기준을 만족하는 안전한 사용자 및 이용자 패스워드 관리 절차를 수립•이행하고 있는가? 2) 클라우드 시스템 관리자 패스워드는 별도 목록(문서 또는 파일)으로 유지•관리하고, 비밀등급에 준하는 보호대책을 적용하고 있는가? 3) 이용자 계정 및 패스워드 관리절차 관련 내용을 홈페이지 또는 메일 등을 통하여 이용자가 쉽게 확인하고 이해할 수 있도록 공지하고 있는가?		
신청기관 준비사항 (관련증적)	• 패스워드 관리 절차 • 패스워드 복잡도 설정, 변경 주기 등 설정 화면 • 시스템 관리자 패스워드 관리대장 • 이용자 계정 및 패스워드 관리 방법 및 절차 공지	참고사항 (샘플자료)	• 정보보호 정책서 • 접근통제관리지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ 점검항목 1)

■ 사용자 및 이용자 패스워드 관리를 위한 관리절차를 수립하여 적용하여야 한다.

- 시스템 설계 시 패스워드 관리절차의 요구사항 적용
- 패스워드를 별도 문서 또는 파일로 보관하는 경우 비밀등급으로 분류하여 비인가자의 접근통제 방안 수립

※ 패스워드 관리절차 예시

- 문자(영문 대소문자), 숫자, 특수문자를 조합하는 패스워드 생성규칙 수립
- 패스워드의 주기적으로 변경 (분기 1회 이상 권고, 동일 패스워드 재사용 금지)
- 연속 숫자, 생일, 전화번호 등 추측하기 쉬운 개인 신상정보를 활용한 패스워드 사용 제한
- 정보 시스템 최초 접근 시 패스워드 강제 변경
- 패스워드 처리(입력, 변경) 시 마스킹 처리
- 종이, 파일, 포켓용 소형기기 등에 패스워드 기록•저장을 제한하고 부득이하게 기록•저장해야 하는 경우 암호화 등의 보호대책 적용
- 정보 시스템 침해사고가 발생 또는 패스워드의 노출 징후가 의심될 경우 즉시 패스워드 변경
- 자동 로그인 금지
- 패스워드 분실, 도난 시 본인확인 등을 통한 안전한 재발급 절차 마련
- 개인정보취급자의 경우, 패스워드 작성 규칙에 대해 법적 요구사항 반영 등

■ 패스워드는 영문 대문자, 영문 소문자, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성하여야 한다.

※ 클라우드서비스사업자의 관리자가 관리시스템에 로그인 시 강화된 인증수단 적용 필수

※ 클라우드컴퓨팅서비스를 이용하는 국가・공공기관의 이용자가 관리시스템에 로그인 시 강화된 인증수단 적용 필수 (국가・공공기관의 서비스를 이용하는 민간인의 경우, 강화된 인증수단 적용 필수 대상에서 제외)

※ 참고

법률	내용
개인정보의 기술적•관리적 보호조치 기준(고시)' 제4조	영문 대문자, 영문 소문자, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성
'개인정보 안전성 확보조치 기준 제5조(비밀번호관리)'에 대한 해설서	영문 대문자, 영문 소문자, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성

⇨ 점검항목 2)

■ 관리자 패스워드는 일반 사용자 패스워드와 별도 관리하여야 한다.

예) 서버 시스템에 접속 가능한 일반 사용자 계정과 root 계정이 있는 경우 root 계정의 패스워드를 별도 안전하게 관리 (관리자 부재 또는 패스워드를 잊어버린 경우 확인 목적 등)

- 관리자 패스워드를 기록한 문서 또는 저장매체는 비밀에 준하여 관리
- 내화금고 등 잠금장치로 비인가자의 접근 통제

⇨ 점검항목 3)

■ 이용자에게 이용자 패스워드 관리에 대한 절차를 공지하여야 한다.

- 안전한 패스워드 생성규칙 수립 (패스워드 복잡도, 길이 등)
- 연속 숫자, 생일, 전화번호 등 추측하기 쉬운 개인 신상정보를 이용한 패스워드 생성 제한
- 초기/임시 패스워드를 발급할 경우 최초 로그인 시 변경
- 주기적인 패스워드 변경 유도
- 이용자 패스워드 분실•도난 시 안전한 재발급 절차(본인인증 등)
- 패스워드 관리에 대한 책임 등
- 연속적인 로그인 실패 시에 대한 안내
- 장기 미사용, 이용만료 등에 대한 안내

■ 공지 방법은 홈페이지 공지사항, 알림 메시지, 전자 우편 등을 이용하여 공지할 수 있다.

11. 네트워크 보안

11.1 네트워크 보안

통제항목	11.1.1 네트워크 보안정책 수립		
세부통제내용	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크에 대해 보안정책과 절차를 수립하여야 한다.		
점검항목	1) 내•외부 네트워크를 통한 클라우드 시스템의 접근을 통제하는 보안 정책이 수립되어 있는가?		
신청기관 준비사항 (관련증적)	• 정보자산목록 (IP정보 포함) • 네트워크 구성도 (IP정보 포함) • 단말기 접근 통제 방안 • 클라우드 접속 단말기 지정 현황 • 시스템 원격 접속 현황 및 방법	참고사항 (샘플자료)	• 정보보호 정책서 • 네트워크 보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ **점검항목 1)**

■ 내부망을 통해 클라우드 시스템에 접속하는 경우 지정된 단말을 통해서만 접근할 수 있도록 통제하여야 한다.

- 스마트패드, 스마트폰 등 스마트기기를 통한 클라우드 시스템 원격운영 금지
- 무선 네트워크 사용에 대한 제한 사항
- 네트워크 관리용 단말의 접근통제 절차(IP나 MAC 통제 방법, 단말의 수 등)
- 네트워크 관리용 단말의 운영절차(백신 설치, 최신 보안패치, 불필요한 프로그램 제거, 식별 및 인증 수행 등)
- IP 할당 절차 등
- 계정별 사용현황 현행화 및 정기 검토
- 네트워크 사용 단말기 목록 관리

■ 외부 네트워크를 통한 시스템 원격운영은 원칙적으로 금지하여야 한다.

- 단 긴급 장애대응 등과 같이 부득이한 경우 보안대책 마련
  - 최고책임자의 승인
  - 접속 단말 및 사용자 인증 (IP/MAC인증, Two fact 인증 등)
  - 한시적 접근권한 부여
  - 원격으로 접근하는 채널에 대한 보호 대책(VPN 사용, SSH 사용 등)

- 접속 단말 보안
- 원격 운영 현황 모니터링
- 원격 접속에 대한 로깅 및 주기적 분석
- 원격운영 관련 보안인식 교육 등
- 접속 위치 제한 : 접근가능 위치 제한, 접속자 특정 IP주소 할당
- 외부에서 시스템 접속 시 관리자 전용 페이지 접근 제한

통제항목	11.1.2 네트워크 모니터링 및 통제		
세부통제내용	DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요정보 유출 등을 막기 위해 네트워크를 모니터링하고 통제하여야 한다.		
점검항목	1) 접근통제 정책에 따라 인가된 사용자만이 내부 네트워크(서비스망, 관리망)에 접근할 수 있도록 네트워크 식별자(IP) 할당 등을 통제하고 있는가? 2) 내부 네트워크를 구성하는 주요자산 목록, 구성도, IP 현황을 최신으로 유지하고 안전하게 관리하고 있는가? 3) 내부 네트워크 IP 주소는 사설 IP로 할당하고 국제권고표준을 따르고 있는가? 4) DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요 정보 유출 등을 예방하기 위해 네트워크를 모니터링하고 있는가?		
신청기관 준비사항 (관련증적)	• 정보자산목록 (IP정보 포함) • 네트워크 구성도 • 네트워크 모니터링 시스템 • 네트워크 모니터링 위탁 시 계약서, SLA 등	참고사항 (샘플자료)	• 정보보호 정책서 • 네트워크 보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 클라우드서비스 운영에 포함된 자산에 IP를 부여하는 경우 승인절차에 따라 IP를 할당하여야 하며, 승인되지 않은 IP의 경우 접속을 차단하여야 한다.

- 인가된 사용자만 네트워크에 접근할 수 있도록 허용
- 네트워크 장치에 불필요한 서비스 및 포트 등 제거 또는 차단

⇨ 점검항목 2)

■ 내부 네트워크를 구성하는 주요 자산목록, 구성도, IP 현황 등을 최신으로 유지하고, 외부에 유출되지 않도록 대외비 이상으로 안전하게 관리하여야 한다.

- 최소한의 인력만 문서에 접근 가능하도록 통제
- 전자문서 형태로 관리할 경우 암호 설정 등
- 정기적인 접근권한 타당성 검토
- 네트워크 접근이 가능한 모든 IP 식별

➪ **점검항목 3)**

■ 관리망의 주소체계는 사설 IP주소 체계를 사용하고, 내부 주소체계가 외부에 유출되지 않도록 하여야 한다.

- 네트워크별 IP주소 부여 기준 마련

※ 사설 IP주소

- 10.0.0.0 ~ 10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0 ~ 192.168.255.255

➪ **점검항목 3)**

■ DDoS, 비인가 접속 등의 서비스 중단 및 중요정보 유출 등을 예방하기 위해 네트워크 모니터링 방안을 수립하고 이행하여야 한다.

※ 네트워크 관리 및 모니터링 등은 외부 위탁 가능하며, 외부 위탁되는 경우 계약서 또는 SLA를 확인하여야 한다.

- 접속기록 및 이벤트 로그 정기 모니터링

통제항목	11.1.3 네트워크 정보보호시스템 운영		
세부통제내용	클라우드컴퓨팅서비스와 관련된 내•외부 네트워크를 보호하기 위하여 정보보호시스템(방화벽, IPS, IDS, VPN 등)을 운영하여야 한다.		
점검항목	1) 내•외부 네트워크를 보호하기 위하여 정보보호시스템(방화벽, IPS, IDS, VPN 등)가 운영되고 있는가? 2) 정보보호시스템 관리자 등 접근이 허용된 인원을 최소화하고 비인가자 접근을 엄격하게 통제하고 있는가? (직접운영 시) 3) 정보보호시스템별 정책(룰셋 등) 신규 등록, 변경, 삭제 등 절차를 수립하고 정책의 타당성 검토를 주기적으로 수행하고 있는가? (직접운영 시)		
신청기관 준비사항 (관련증적)	• 정보자산목록 (정보보호시스템) • 네트워크 구성도 • 정보보호시스템 관리자 및 관리자 PC 현황 • 정보보호시스템 로그 • 정보보호시스템 정책 관리 절차 • 정보보호시스템 정책 타당성 검토 현황	참고사항 (샘플자료)	• 정보보호 정책서 • 네트워크 보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 내•외부 네트워크 보호를 위한 정보보호시스템을 운영하여야 한다.

- 정보보호시스템 도입 시 국내외 CC인증을 획득한 제품을 도입
- 정보보호시스템 운영절차 수립
- 정보보호시스템의 운영 및 관리 등은 외부 위탁 가능하며, 외부 위탁되는 경우 계약서 또는 SLA에 정보보호시스템 운영 및 관리 등의 내용을 포함
- 단 클라우드컴퓨팅서비스 제공자의 사용자가 원격 접속 등을 위해 VPN을 운영하는 경우 반드시 CC인증 제품을 사용하지 않아도 가능 (대고객 서비스(공공기관 이용자 등)를 위한 VPN의 경우 CC인증 제품 필수 사용)

⇨ 점검항목 2)

■ 정보보호시스템 관리자 등 접근이 허용된 인원 이외의 비인가자 접근을 통제하여야 한다.

- 정보보호시스템 관리자는 최소 인원으로 운영

- 사용자 인증
- 관리자 단말 IP 또는 MAC 지정
- 주기적인 접속 로그 분석 등

⇨ 점검항목 3)

■ 정보보호시스템의 정책을 관리(등록, 변경, 삭제 등)하는 절차를 수립하고 이행하여야 한다.

- 정보보호시스템별 적절한 보안정책(룰셋) 적용
- 정보보호시스템의 보안정책(룰셋)에 대한 주기적인 검토 수행
- 정보보호시스템의 정상동작 여부 점검(월 1회 이상) 수행
- 정보보호시스템의 패턴 등 보안패치 적용
- 미승인 정책 유무
- 장기간 미사용 정책
- 중복 또는 사용 기간 만료 정책
- 퇴직자 또는 직무 변경자 관련 정책 등

통제항목	11.1.4 네트워크 암호화		
세부통제내용	클라우드 시스템에서 중요정보가 이동하는 구간에 대해서는 암호화된 통신 채널을 사용하여야 한다.		
점검항목	1) 클라우드 시스템에서 중요정보를 송•수신하는 경우 암호화 통신 채널을 사용하고 있는가?		
신청기관 준비사항 (관련증적)	• 클라우드 서비스 내에 암호화 통신 채널 사용 현황 (대상, 방법, 알고리즘 등)	참고사항 (샘플자료)	• 정보보호 정책서 • 네트워크 보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 클라우드 시스템에서 중요정보가 이동하는 구간에 대해서는 암호화된 통신 채널을 사용하여야 한다.

※ 암호화된 통신 채널 예시
- 서버 원격 접근 시 암호화된 통신수단(VPN, SSH 등)을 사용
- 공공기관 데이터이관 시 VPN을 통해 이관
- 기타 관리를 위한 접근 시 OpenSSH 및 OpenSSL(TLS V1.2) 사용

■ 암호화된 통신 채널을 사용하는 경우 지원되는 암호의 보안 강도가 요구되는 수준을 만족하여야 한다.
- 요구되는 보안 강도 : 2^{112}
- 만족하는 알고리즘의 예
  - 블록 암호 알고리즘 : SEED, ARIA, AES 등 키 길이 128bits 이상 지원
  - 공개키 암호 알고리즘 : RSA 등 키 길이 2048bits 이상 지원
  - 해쉬 알고리즘 : SHA2 이상 등

※ 암호이용 안내서(KISA 발간) 참고

통제항목	11.1.5 네트워크 분리		
세부통제내용	클라우드컴퓨팅서비스 제공자의 관리 영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리하여야 한다.		
점검항목	1) 클라우드 서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항 등에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 있는가?		
신청기관 준비사항 (관련증적)	• 네트워크 구성도 (네트워크 분리 및 연계 방법)	참고사항 (샘플자료)	• 정보보호 정책서 • 네트워크 보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 클라우드 서비스 핵심 업무와 관련된 내부 네트워크는 물리적 또는 논리적으로 분리하고 영역 간 접근통제를 하여야 한다.

- DMZ영역은 공개서버를 경유하여 내부망으로 접근이 이뤄지지 않도록 접근통제 수행
- 이용자의 중요정보 등이 저장된 DB는 네트워크 별도 분리
- 클라우드 시스템을 운영하는 인력이 사용하는 네트워크 별도 분리
- 개발에 사용되는 네트워크는 별도 구성
- 이용자 간 서비스 영역은 물리적 또는 논리적으로 분리
- 기타 업무 특성 및 중요도에 따라 네트워크 분리 기준 수립 후 적용
- 내부 서버에서 외부 인터넷 접근 제한
- 망간 자료전송 통제 방안 마련
- 우회 경로 차단 및 조치

※ 영역별 네트워크 분리 예시

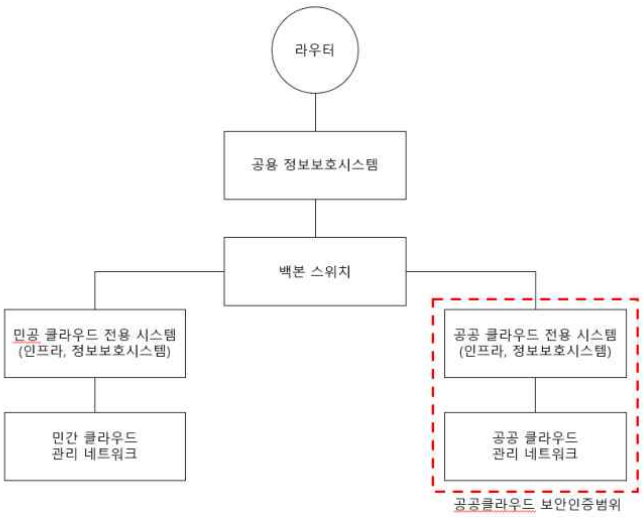
구분	설명
DMZ망	외부로부터의 접근이 불가피한 영역 공개서버를 경유하여 내부망으로의 접근이 이루어지지 않도록 접근통제 수행
DB망	이용자의 중요정보 등 DB가 위치한 영역 다른 네트워크 영역과 분리
관리망	서버, 보안장비, 네트워크장비 등 중요 클라우드시스템을 운영하는 인력이 사용하는 영역 다른 네트워크 영역과 분리
개발망	개발업무(개발자PC, 개발서버, 테스트서버 등)에 사용되는 영역 운영 네트워크 영역과 분리
이용자망	이용자 간 서비스 영역 물리적 또는 논리적으로 분리
기타	업무망의 경우 업무의 특성, 중요도에 따라 네트워크 대역 분리 기준 수립 후 운영

- 민간 서비스 네트워크와 공공 서비스 네트워크의 분리 (서비스 관리망도 분리)
  (단, DR 센터의 네트워크는 공공·민간 부문 공용으로 운영 가능)

■ 외부 네트워크에서 접근할 필요가 없는 클라우드컴퓨팅서비스 제공자의 사용자 포탈은 이용자 포탈과 별도 분리하여 내부망에 설치 운영하여야 한다.

■ 분리된 네트워크 간에는 방화벽과 같은 정보보호시스템 또는 네트워크 접근제어 목록(Network ACL), 보안그룹(Security Group), 접근제어그룹(Access Control Group) 등과 같은 접근통제 기능을 제공하는 수단을 이용하여 접근통제를 적용하여야 한다.

[네트워크 구성도 예시]



통제항목	11.1.6 무선 접근통제		
세부통제내용	클라우드 시스템은 무선망과 분리하고, 무선접속에 대한 접근을 통제하여야 한다. 무선접속을 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.		
점검항목	1) 무선 네트워크 환경을 구축(AP 설치)할 경우 허가(승인), 보안성 검토 등 절차를 마련하고 구축에 따른 보호대책을 적용하고 있는가? 2) 외부인에게 제공하는 무선 네트워크를 내부 네트워크(업무망)와 분리하고 있는가?		
신청기관 준비사항 (관련증적)	• 네트워크 구성도 • 무선 네트워크 현황 • 무선 네트워크 보호대책 • 무선 네트워크 사용 절차 • 주요 단말기 지정 현황 (IP 정보 포함)	**참고사항 (샘플자료)**	• 정보보호 정책서 • 네트워크 보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		**O**	

점검항목 해설

➪ **점검항목 1)**

■ 공공기관용 클라우드 시스템의 경우 무선을 통한 접근이 불가능하도록 통제되어야 한다.

■ 내부 네트워크에 연결이 가능한 무선 네트워크 환경을 구축하는 경우 내부 승인 절차를 마련하고 비인가된 사설 무선 네트워크가 운영되지 않도록 관리하여야 한다.

- 무선 네트워크 접속 단말 인증 방안(IP, MAC 인증 등)

■ 사전 보안성 검토 및 무선 네트워크 운영 시 다음과 같은 사항이 적용되어야 한다.

- 무선 네트워크 장비 접속 단말기 인증 및 보안
- 무선 네트워크 장비 (예 : AP, Access Point) 보안 및 허용 장비 리스트
- 무선 네트워크를 통하여 접근할 수 있는 정보 시스템 범위 정의
- 무선 네트워크 사용권한 신청/변경/삭제 절차
- 사용자 식별 및 인증
- 무선 네트워크 서비스 거리 제한 (주파수 세기 조정)
- 정보송수신 시 무선망 암호화 기준 (예 : WPA2)
- 전산실 등 통제구역 내 무선 네트워크 사용 제한
- SSID(Service Set IDentification) 브로드캐스팅 중지 및 추측 어려운 SSID 사용 등

➪ **점검항목 2)**

■ 회의실, 교육장, 기자실, 민원실 등 외부인의 접근이 빈번한 장소인 경우 외부인에게 무선 네트워크 사용을 허용할 수 있으나 내부 네트워크(업무망)과 분리하여 무선 네트워크를 통한 내부 네트워크 침투 및 내부 정보유출을 방지하여야 한다.

- 임직원과 외부인에게 제공하는 무선 네트워크 대역 분리

12. 데이터 보호 및 암호화

12.1 데이터 보호

통제항목	12.1.1 데이터 분류		
세부통제내용	데이터 유형, 법적 요구사항, 민감도 및 중요도에 따라 데이터를 분류하고 관리하여야 한다.		
점검항목	1) 클라우드 시스템 상에서 기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 데이터의 중요도를 평가하기 위한 기준을 수립하고 있는가?		
신청기관 준비사항 (관련증적)	• 데이터 분류표 • 데이터 중요도 평가기준 • 데이터 흐름도/흐름표 • 데이터 현황/목록	참고사항 (샘플자료)	• 정보보호 정책서 • 데이터보호 및 암호화 지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ **점검항목 1)**

■ 데이터의 유출, 장애 및 침해 발생 시 클라우드 시스템 및 이용자에게 미치는 영향을 고려하여 식별된 데이터의 중요도를 평가할 수 있도록 기준을 수립하여야 한다.

- 기밀성, 무결성, 가용성, 법적요구사항 등을 고려
- 그 외에 서비스 영향, 이익손실, 고객 상실, 대외 이미지 등 추가 고려 가능
- 클라우드 시스템 상의 데이터 식별 및 중요도 평가
- 중요도 등급별 적절한 보안 정책 적용

■ 데이터에 미치는 위험은 데이터의 중요도가 높을수록 증가하며, 비용효과적인 방법으로 정보보호대책을 선정할 수 있다.

- 데이터의 중요도가 높을수록 이를 처리하는 시스템의 중요도 또한 영향을 미침 (3.3.3. 위험분석 및 평가와 연계)

※ 클라우드컴퓨팅서비스 이용자 데이터 목록 및 중요도 평가 예시

방법	데이터 유형	보관 장소	암호화 여부	담당	C	I	A	법적 요구사항	중요도
회원 가입 시	성명, 전화번호, 이메일, 비밀번호	이용자 DB	비밀번호 (해쉬)	홍길동	2	2	2	2	2
본인 인증 시	이름, 생년월일, 전화번호, CI, DI	이용자 DB		홍길동	2	2	2	1	2
서비스 이용 시	쿠키, 접속 로그(IP)	이용자 DB		홍길동	1	1	1	1	3
서비스 제공	클라우드서비스 데이터 (메일)	클라우드 서비스 DB		홍길동	3	3	3	1	1
서비스 제공	클라우드서비스 데이터 (게시판)	클라우드 서비스 DB		홍길동	3	3	3	1	1

- 매체(스토리지, 백업 드라이브 등)
- 가상머신 이미지
- 스냅샷

통제항목	12.1.2 데이터 소유권		
세부통제내용	이용자와 서비스 수준 협약 단계에서 데이터의 소유권을 명확하게 확립하여야 한다.		
점검항목	1) 이용자와의 클라우드컴퓨팅서비스 수준 협약 시 협약서 내에 생성되는 데이터에 대한 소유권(정의, 분류, 책임 등)을 명시하고 있는가?		
신청기관 준비사항 (관련증적)	• 클라우드서비스 제공 계약서, 약관, SLA 등	참고사항 (샘플자료)	• 정보보호 정책서 • 데이터보호 및 암호화 지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ 점검항목 1)

■ 클라우드컴퓨팅서비스 제공자는 서비스 제공 시 발생하는 데이터의 소유권을 명확하게 정의하여야 하며, 데이터 소유권은 클라우드 사업자와 이용자 사이의 계약에 의해 정의하여야 한다.

- 모든 데이터의 소유권(정의, 할당, 전달된 책임 등)을 지정

※ 데이터 소유권 및 보안서비스 제공 관련 계약서 예시

- 클라우드서비스를 이용하면서 발생하는 데이터의 소유는 이용자에게 있으며 클라우드서비스 제공자는 법령이 정하는 바에 따라 데이터를 보호하여야 한다.
- 클라우드서비스 제공자는 적절한 수준의 보안서비스를 제공하고 사고를 방지할 의무가 있으며 이용자는 이용자의 주의의무 위반으로 인한 이용자 정보의 도용 및 유출 등에 대해서 책임을 진다.

통제항목	12.1.3 데이터 무결성		
세부통제내용	입·출력, 전송 또는 데이터 교환 및 저장소의 데이터에 대해 항상 데이터 무결성을 확인하여야 한다.		
점검항목	1) 클라우드 시스템 내 이용자 데이터의 입력, 출력, 전송, 저장 시 데이터의 무결성을 보장하기 위해 기술적인 방안을 마련하고 있는가?		
신청기관 준비사항 (관련증적)	• 데이터 무결성 조치 기술 * 시스템 설계서 등 • 데이터 흐름도/흐름표 상의 무결성 보장 방안	참고사항 (샘플자료)	• 정보보호 정책서 • 데이터보호 및 암호화 지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 클라우드 시스템 내 이용자 데이터가 입력, 출력, 전송, 저장되는 경우 이용자 데이터에 대한 무결성을 보장하기 위한 기술적인 방안을 수립하여야 한다.

- 시스템 설계 시 이용자 데이터 처리 시 무결성 보장 방안을 고려
- 무결성 보장이 필요한 이용자 데이터에 대한 분류 및 정의 수행

※ 데이터 처리 유형별 무결성 보장 예시

구분	설명
데이터 입력, 출력 시 (클라우드서비스 이용 시)	* 서비스 이용자 또는 서비스 관리자 App에서 데이터 입력, 출력 시 무결성 보장
데이터 전송 시	* 데이터 전송 시 암호화 및 체크섬(해시) 적용
데이터 저장 시	* 중요 데이터 저장 시 체크섬(해시) 적용 또는 암호화 * 다수 이용자에게 서비스를 제공할 경우 데이터 개별 분리 (테넌트 분리, 테이블 분리, 물리적 분리 등)

통제항목	12.1.4 데이터 보호		
세부통제내용	데이터에 대한 접근제어, 위•변조 방지 등 데이터 처리에 대한 보호 기능을 이용자에게 제공하여야 한다.		
점검항목	1) 데이터에 대한 접근제어 및 위•변조 방지 등의 데이터 보호 기능 방안을 마련하고 있는가?		
신청기관 준비사항 (관련증적)	• 데이터 분류표 • 데이터 중요도 평가기준 • 데이터 현황 • 데이터 보호조치 기술 • 시스템 설계서	참고사항 (샘플자료)	• 정보보호 정책서 • 데이터보호 및 암호화 지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ 점검항목 1)

■ 모든 매체(스토리지, 백업 드라이브 등), 가상화된 이미지, 스냅샷에 대해 엄격한 접근 통제가 이루어져야 된다.

- 데이터에 대한 논리적 접근제어(가상화 이미지 및 스냅샷 등)
  ・가상화 이미지 및 스냅샷에 대한 무단 변경을 탐지하기 위한 암호 체크섬
- 시스템 자원, 데이터 자산, 백업 매체에 대한 물리적 접근제어
- 데이터 입력, 처리, 통신, 전송, 출력, 저장 및 검색과 관련된 처리 및 전송 통제
- 접근 가능한 인원을 최소화하고 접근권한 부여 등을 통해 접근통제 수행
- 데이터에 접근할 수 있는 모든 경로 식별하여 접근통제 정책 적용

■ 다음의 경우 데이터의 분실 방지 대책이 마련되어 있는지 확인하여야 한다.

- 저장 데이터 : 클라우드 시스템 내 스토리지에 저장된 데이터
- 이동 중인 데이터 : 클라우드서비스 중 내•외부 네트워크에서 이동 중인 이용자 데이터

■ 다수 이용자에게 서비스를 제공할 경우 데이터 개별 분리 (테넌트 분리, 테이블 분리, 물리적 분리 등)가 적용되어야 한다.

예시)

- NAS의 디렉토리 접근 권한 방식 적용 불가
- Object Storage를 통한 이용자별 접근통제 적용 가능
- Block Storage를 통한 이용자별 스토리지 테넌트 분리

통제항목	12.1.5 데이터 추적성		
세부통제내용	이용자에게 데이터를 추적하기 위한 방안을 제공하고, 이용자가 요구하는 경우 구체적인 제공정보(이용자의 정보가 저장되는 국가의 명칭 등)를 공개하여야 한다.		
점검항목	1) 클라우드 이용자의 데이터가 어디에 저장·관리되고 있는지 확인할 수 있는 방안을 마련하고 있는가?		
신청기관 준비사항 (관련증적)	• 클라우드서비스 제공 계약서, SLA 등 • 클라우드서비스 이용 홈페이지 화면 (시스템으로 메커니즘 구현 시)	**참고사항 (샘플자료)**	• 정보보호 정책서 • 데이터보호 및 암호화 지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 서비스 제공 전에 이용자와 합의하여 데이터가 저장 및 처리되는 위치를 계약서 또는 SLA에 명확히 포함하여야 한다.

- 클라우드컴퓨팅서비스 제공자와 이용자가 서비스 제공에 관한 계약 체결 시 계약서 또는 SLA에 저장 및 처리 위치를 명시

■ 클라우드 서비스 이용자에게 데이터의 물리적 위치를 확인할 수 있는 메커니즘을 제공하여야 한다.

- 데이터의 물리적 위치정보는 데이터센터의 위치 등을 포함
- 공공기관 클라우드 서비스의 물리적 위치는 국내로 한정

※ 계약서 내 이용자의 데이터 저장 및 처리 위치 포함 예시

> 제OO조(목적) 이 계약은 OOOO (이하 “사업자”라 한다)이 제공하는 클라우드컴퓨팅서비스 (데이터 저장 및 처리 위치 : OOO사 공공클라우드 IaaS 서비스) 이용과 관련하여 사업자와 클라우드컴퓨팅서비스를 이용하고자 하는 이용기관(이하 “이용기관”이라 한다)간의 권리와 의무 및 책임범위, 그밖에 필요한 기본적인 사항을 규정함을 목적으로 한다.

통제항목	12.1.6 데이터 폐기		
세부통제내용	클라우드컴퓨팅서비스 종료, 이전 등에 따른 데이터 폐기 조치 시 이용자와 관련된 모든 데이터를 폐기하여야 하며, 폐기된 데이터를 복구할 수 없도록 삭제 방안을 마련하여야 한다.		
점검항목	1) 클라우드컴퓨팅서비스 이용 종료 또는 이전 시 이용자가 생산한 데이터의 폐기 시 정보가 복구되지 않는 방법으로 처리하고 있는가?		
신청기관 준비사항 (관련증적)	• 클라우드서비스 제공 계약서, SLA 등 • 데이터 폐기 관련 기법/기술 * 시스템 설계서 등	참고사항 (샘플자료)	• 정보보호 정책서 • 데이터보호 및 암호화 지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ **점검항목 1)**

■ 이용자와의 계약 종료 또는 이전 시, 이용자의 데이터를 재사용할 수 없도록 정보를 완전히 삭제하여야 한다.

- 시스템 설계 시 이용자 데이터 삭제 시 데이터 완전삭제 기능 적용
- 데이터 완전삭제
  - 표준화된 방법 적용(DoD 5220.22-M-ECE, DoD 5220.22-M, HMG IAS No.5 Higher Overwrite, Russian GOST, Canadian RCMP OPS, German VSITR, NIST 800-88 등)
  - 새로운(무의미한) 데이터를 여러 차례 덮어쓰기 적용
- 이용자의 데이터를 백업해 놓은 경우, 백업데이터도 일정 기간 이내(이용자와 협의하여 기한을 정함)에 삭제
- 데이터 폐기 이후 폐기 사실에 대하여 이용자에게 통보

※ 계약서 내 이용자의 데이터 반환 및 파기 예시

> 제OO조(이용자 정보의 처리 등) ① 계약이 해제, 해지 또는 종료되면 이용자 정보를 이용기관에게 반환하여야 하고, 이용기관이 반환을 받지 아니하거나 반환을 원하지 아니하는 등의 이유로 사실상 반환이 불가능한 경우에는 이용기관과 협의하여 이용자 정보를 파기한다.
> ② 이용기관의 이용자 정보를 폐기할 때 사업자는 복구가 불가능한 방법으로 완전히 폐기해야 하며, 이용기관은 완전히 폐기 되었는지를 확인하여야 한다.

12.2 매체 보안

통제항목	12.2.1 저장매체 관리		
세부통제내용	중요정보를 담고 있는 하드디스크, 스토리지 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제하여야 한다.		
점검항목	1) 클라우드시스템 폐기 또는 재사용 발생 시 중요정보를 담고 있는 저장매체 처리(폐기, 재사용) 절차를 수립•이행하고 있는가? 2) 저장 또는 이동 매체 폐기 또는 재사용 시 정보가 복구되지 않는 방법으로 처리하고 있는가? 3) 자체적으로 저장매체를 폐기할 경우, 관리대장을 통해 폐기 이력을 남기고 폐기확인 증적을 함께 보관하고 있는가? 4) 외부업체를 통해 저장매체를 폐기할 경우, 폐기 절차를 계약서에 명시하고 완전한 폐기에 대한 확인을 하고 있는가?		
신청기관 준비사항 (관련증적)	• 저장매체 처리 절차 및 방법 • 저장매체 폐기관리대장 • 저장매체 용역 계약서 및 확인서 • 저장매체 폐기 확인 증적	**참고사항 (샘플자료)**	• 정보보호 정책서 • 데이터보호 및 암호화 지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ **점검항목 1)**

■ 사용기한 경과, 고장 등의 사유로 정보 시스템을 폐기 또는 재사용(양도, 내부 판매, 재활용 등)할 경우 저장매체 처리에 관한 절차를 수립하여 저장매체에 저장된 중요정보 유출을 방지하여야 한다.

- 저장매체 확인 및 승인
- 저장매체 폐기, 재사용에 따른 처리방법 정의 (예: 폐기 시에는 물리적 폐기 또는 디가우징 등, 재사용 시에는 완전 포맷 등)
- 저장매체 처리 확인 및 기록 유지

■ 회수된 공공기관 클라우드 하드웨어 자원은 공공기관 클라우드 컴퓨팅 제공을 위한 시스템에서만 사용하여야 한다.

⇨ **점검항목 2)**

■ 저장매체의 폐기 시 물리적, 전자적으로 완전 파괴하고, 재사용 시에는 완전포맷 방식으로 정보를 삭제하여야 한다.

- “완전포맷“은 저장매체 전체의 자료저장 위치에 새로운 자료를 중복하여 저장하는 것을 의미하여, 완전포맷 횟수는 조직이 스스로 정하여 적용할 수 있다.
- 저장매체 재사용 시 로우레벨 포맷으로 저장매체 초기화하여 사용

⇨ 점검항목 3)

■ 자체적으로 저장매체 폐기할 경우 폐기이력에 대한 감사증적을 확보할 수 있도록 다음 항목이 포함된 관리대장을 작성하고 관련 책임자가 확인하여야 한다.
- 폐기일자, 담당자, 확인자, 방법, 폐기확인 증적 등

⇨ 점검항목 4)

■ 아웃소싱 등 외부업체를 통해 저장매체를 폐기할 경우, 내부 폐기정책과 절차 내용을 계약서에 명시하여야 한다.
- 폐기 시 가능하면 외부업체와 함께 현장에서 함께 폐기현장을 실사
- 폐기증적을 사진, 동영상 등으로 받아 확인
- 완전한 폐기 여부 점검

통제항목	12.2.2 이동매체 관리		
세부통제내용	중요정보 유출을 예방하기 위해 외장하드, USB, CD 등 이동매체 취급, 보관, 폐기, 재사용에 대한 절차를 수립하여야 한다. 또한 매체를 통한 악성코드 감염 방지 대책을 마련하여야 한다.		
점검항목	1) 외장하드, USB, CD 등 이동매체 취급(사용), 보관, 폐기, 재사용에 대한 정책 및 절차를 수립•이행하고 있는가? 2) 클라우드 시스템 중 중요 시스템이 위치한 통제구역, 중요 제한구역 등에서 이동매체 사용을 제한하고 있는가? 3) 이동매체를 통한 악성코드 감염 및 중요정보 유출 방지를 위한 대책을 마련하고 있는가? 4) 이동매체 보유현황 및 관리 실태를 주기적으로 점검하고 있는가?		
신청기관 준비사항 (관련증적)	• 이동저장매체 관리절차서 • 이동저장매체 관리대장 • 이동저장매체 사용 신청서 • 이동저장매체 실태점검 이력	**참고사항 (샘플자료)**	• 정보보호 정책서 • 데이터보호 및 암호화 지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		**O**	

점검항목 해설

⇨ **점검항목 1)**

■ 업무용으로 개인 휴대용 저장매체를 사용하는 것은 원칙적으로 금지하여야 하며, 업무 목적상 외장하드, USB 메모리, CD 등 휴대용 저장매체를 사용하여야 하는 경우 허가된 저장매체만 사용할 수 있도록 다음과 같은 정책 및 절차를 수립하고 이행하여야 한다.

- “이동매체“란 디스켓, 외장형 하드디스크, USB 메모리, CD, DVD 등 자료를 저장할 수 있는 일체의 것으로, PC 등의 정보통신시스템과 분리할 수 있는 기억장치를 말한다.
- 외부업체가 이동매체를 사용할 경우, 관련절차를 수립하고 이행하여야 한다.
  - ·이동매체 취급(사용)범위 : 통제구역, 제한구역 등 보호구역 별 저장매체 사용 가능 여부
  - ·이동매체 사용허가 및 등록
  - ·이동매체 반출, 반입
  - ·이동매체 폐기, 재사용
  - ·이동매체 보호대책 등
  - ·이동매체 보유현황 관리대장
  - ·이동매체 사용기록 컴퓨터 레지스트리 확인

⇨ 점검항목 2)

■ 클라우드 시스템 중 중요 시스템이 위치한 통제구역(전산실 등), 조직 내 중요정보에 접근이 가능한 제한구역(운영실, 관제실 등)에서는 이동매체의 사용 및 반입을 엄격하게 제한하여야 한다.

- 불가피하게 사용할 경우 책임자의 허가절차를 거친 후 적법한 절차에 따른 사용여부 확인을 위하여 지속적인 점검 수행
- 중요 제한구역 내 이동매체 사용현황을 불시 점검

⇨ 점검항목 3)

■ 이동매체를 통해 바이러스, 악성코드가 유포되지 않도록, 이동매체가 연결되는 PC 등 단말기에 보호대책을 적용하고 주기적으로 점검하여야 한다.

- 이동매체 자동실행 기능 해지
- 이동매체 이용 시 바이러스 및 악성코드 사전(자동) 검사
- 이동매체 내 숨김 파일 및 폴더 등이 표시되도록 PC 등 단말기 옵션 변경 등
- 보안USB 등 안전한 이동매체 사용
- 이동매체 사용통제 솔루션 사용 등

■ 클라우드 사업자 조직 및 시스템의 중요정보(개인정보, 기밀정보 등)의 경우 이동매체 저장을 제한하여야 한다.

- 업무상 저장이 필요한 경우에는 암호화 등의 보호대책을 마련하여 매체 분실, 도난 등에 따른 중요정보 유출을 방지

⇨ 점검항목 4)

■ 업무 목적으로 사용이 허용된 이동매체의 경우, 식별번호, 유형, 사용목적, 관리자, 책임자 등이 명시된 보유목록을 작성하고, 주기적인 자산실사를 통해 목록을 현행화하여야 한다.

- 수기 관리대장을 통해 기록하는 경우 최소 3개월 동안 유지
- 관리대장 및 이동매체는 안전한 장소(잠금장치 등)에 보관

12.3 암호화

통제항목	12.3.1 암호 정책 수립		
세부통제내용	클라우드컴퓨팅서비스에 저장 또는 전송 중인 데이터를 보호하기 위해 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 마련하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.		
점검항목	1) 클라우드 시스템에서 중요정보의 전송 및 저장 시 안전한 보호를 위한 암호 정책을 수립•이행하고 있는가? 2) 이용자(고객 등) 및 사용자(임직원 등)의 비밀번호 저장 시 암호 정책을 수립•이행하고 있는가?		
신청기관 준비사항 (관련증적)	• 암호화 정책 • 암호화 대상 및 방법	참고사항 (샘플자료)	• 정보보호 정책서 • 데이터보호 및 암호화 지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ **점검항목 1)**

■ 클라우드 시스템에서 개인정보 및 시스템 정보 등 중요 정보를 전송하거나 저장하는 경우 다음과 같은 내용이 포함된 암호정책을 수립하여야 한다.

- 암호대상 : 취급하는 정보의 민감도 및 중요도와 법적 요구사항 유무에 따라 정의

구분	대상
중요 정보	* 클라우드 시스템 운영과 관련된 정보 (정보자산목록, 네트워크 구성도, 취약점점검결과, 위험분석평가결과보고 등) * 클라우드서비스와 관련하여 이용자와 협의된 정보 * 기타 IaaS 사업자가 중요도를 판단한 정보
법적 요구사항에 따른 암호화 대상	* 개인정보, 인증정보, 금융정보, 고유식별정보

- 암호화 방식과 암호 알고리즘 정의

암호화 방식	알고리즘 강도 (공공기관)	암호키 길이
대칭키 암호화 방식	SEED, ARIA, AES	128 bits 이상
비대칭키 암호화 방식	RSA	2048 bits 이상
일방향 암호화 방식	SHA-224/256/384/512	-

- 중요 정보 전송 및 저장 시 암호화 방안

구분	암호화 방안
서버와 클라이언트 간 전송	* SSL 방식 * 응용프로그램 방식
개인정보처리시스템 간 전송	* IPSec 방식, SSL 방식, SSH 방식
개인정보처리시스템 암호화 방식	* 응용프로그램 자체 암호화 * DB 서버 암호화 * DBMS 자체 암호화 * DMBS 암호화 기능 호출 * 운영체제 암호화
업무용 컴퓨터, 보조저장매체 암호화 방식	* 문서 도구 자체 암호화 * 암호 유틸리티 이용 암호화 * DRM * 디스크 암호화

- 암호키 관리를 위한 관리지침 (암호화 대상 및 대상별 적절한 암호화 방식의 구현 여부) 점검

※ 개인정보의 암호화 조치 안내서 (KISA 발간) 참고
※ 암호 알고리즘 및 키 길이 이용 안내서 (KISA 발간) 참고

⇨ 점검항목 2)

■ 관련 법률에 따라 이용자 및 사용자의 비밀번호는 안전한 알고리즘(예 : 128비트 이상. SHA 256, SHA384 등)을 통해 일방향 암호화하여야 한다.
- 법률에 따른 대상 이외의 서비스 및 시스템 비밀번호도 일방향 암호 알고리즘 적용

통제항목	12.3.2 암호키 관리		
세부통제내용	암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고, 암호키는 별도의 안전한 장소에 보관하여야 한다.		
점검항목	1) 암호키 생성, 이용, 보관, 배포, 복구, 파기 등에 관한 절차를 수립 • 이행하고 있는가? 2) 암호키 생성 후 암호키는 별도의 안전한 장소에 소산 보관하고, 암호키 사용에 관한 접근권한 부여를 최소화하고 있는가? 3) 암호키 변경에 관한 정책을 수립•이행하고 있는가?		
신청기관 준비사항 (관련증적)	• 암호화키 관리 절차 • 암호화키 관리대장 • 암호화키 소산 백업	참고사항 (샘플자료)	• 정보보호 정책서 • 데이터보호 및 암호화 지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 암호키 생성, 이용, 보관, 배포, 파기에 대해 다음과 같은 항목이 포함된 정책 및 절차를 수립하고 이행하여야 한다.

구분	방법
암호키 관리 담당 지정	* 암호키 생성, 배포, 백업, 복구, 폐기를 수행하는 담당자
암호키 생성 방법	* 대칭키 또는 비대칭키 알고리즘의 암호키 생성 * 난수발생기를 이용하거나 미리 공유된 키를 이용하여 암호키 유도
암호키 보관 방법	* 유효기간 만료 전까지 장비 모듈 또는 저장매체에 보관 * 무결성 및 접근통제 적용 (물리적으로 분리된 서버에 저장, 소산백업, 암호화 키 접근 권한 최소화 등)
암호키 배포 방법	* 수동 키 분배 (수동적으로 키를 분배하고 적용) * 자동 키 분배 (인터넷 등을 통해 자동 키 분배)
암호키 사용 유효기간	* 암호화 방식별 암호키 유효기관 관리 * 최대 2년 이내 (개인정보의 암호화 조치 안내서 내의 ‘키 유형에 따라 권장하는 키 유효기간’ 참조)
암호키 복구 방법	* 보관된 암호키 반출 및 적용 또는 암호키 재생성
암호키 폐기 방법	* 키와 관련된 자료 완전삭제

※ 암호 키 관리 안내서(KISA 발간) 참고
※ 암호 알고리즘 및 키 길이 이용 안내서 (KISA 발간) 참고

⇨ 점검항목 2)

■ 생성된 암호키는 암호키 손상 시 시스템 또는 암호화된 정보의 복구를 위하여 별도의 매체에 저장 후 안전한 장소에 보관(소산백업 포함)하여야 한다.
- 소산 보관 : 천재지변 등 비상사태를 대비하여 일정거리 이상 떨어진 장소에 보관하는 방법
- 암호키는 하드코딩 방식으로 구현 지양
- 암호키 접근권한 최소화
- 암호키를 서버 또는 하드웨어 토큰에 저장 시 물리적으로 떨어진 서버 사용

⇨ 점검항목 3)

■ 암호키 변경과 관련한 지침은 암호화 정책에 포함하여 수립하여야 한다.

■ 암호키의 사용 기간은 최대 2년 유효기간은 최대 5년을 권고하고 있으나, 암호키 변경 시 비용과 기업의 정보자산 및 업무 중요도를 고려하여 자체적으로 정하여 적용할 수 있다.

■ 암호키의 유효기간 만료가 가까워지는 경우, 암호키가 유출되거나 유출이 의심되는 경우, 즉시 암호키를 변경하여야 한다.

■ 암호키 유효기간 설정 시 키 노출이 발생 가능한 위험요소와 키 노출에 따른 비용 등을 고려해야 한다.

■ 담당자는 암호키 복구 및 폐기절차를 숙지하여야 한다.

13. 시스템 개발 및 도입 보안

13.1 시스템 분석 및 설계

통제항목	13.1.1 보안요구사항 정의		
세부통제내용	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.		
점검항목	1) 신규 시스템 개발 및 기존 시스템 변경 시 최신 보안취약점 대응, 인증, 로깅, 권한, 암호화, 접근제어 등 정보보호 기본요소, 법적 요구사항 등을 포함한 보안 요구사항을 정의하고 설계 단계에서부터 반영하고 있는가?		
신청기관 준비사항 (관련증적)	• 시스템 설계서 • 시스템 변경 내역서 • 보안요구사항 정의/반영 절차	참고사항 (샘플자료)	• 정보보호 정책서 • 시스템개발보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ **점검항목 1)**

■ 클라우드컴퓨팅서비스를 개발하기 위하여 정보보호 관련 법적 요구사항, 최신 보안 취약점, 정보보호 기본요소(기밀성, 무결성, 가용성) 등을 고려한 보안 요구사항을 정의하여 적용하여야 한다.

- 기밀성/무결성이 요구되는 데이터 분류
- 데이터의 상태에 따른 기밀성/무결성 적용 여부(저장, 전송 등)
- 기밀성/무결성 적용 시 적용되는 암호 알고리즘의 적정성 여부

■ 정의된 보안 요구사항을 반영하여 설계하고 개발하여야 한다.

■ 신규 클라우드 시스템 개발 및 기존 시스템 변경 시 아래의 정보를 참고하여 요구사항 정의부터 운영까지 일관성 있게 적용할 수 있도록 하여야 한다.

- 개인정보처리에 관련된 법적 요구사항 (예 : 개인정보 취급자 권한 부여 기록, 접속기록, 암호화 대상 정보 등)
- 이용자 및 기관의 정보보호 요구사항 (예 : 접근권한 정의 및 통제 원칙, 암호화 대상 선정, 외주 위탁 시 보안요구사항 등)
- 정보보호 관련 기술적인 요구사항 등 (예 : 개발보안, 인증, 암호화 등)

통제항목	13.1.2 인증 및 암호화 기능		
세부통제내용	클라우드 시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입·출력 및 송·수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다.		
점검항목	1) 클라우드 서비스 설계 시 사용자 인증에 대한 보안 요구사항을 정의하여 반영하고 있는가? 2) 중요정보의 입·출력(저장 및 조회) 시 암호화가 요구되는 경우 법적 요구사항을 고려한 적절한 암호화 방법을 사용하고 있는가? 3) 개인정보 및 인증정보 등의 중요한 정보 전송 시 SSL보안서버 구축 등을 통하여 암호화하고 있는가?		
신청기관 준비사항 (관련증적)	• 시스템 설계서 • 시스템 변경 내역서 • 보안요구사항 정의/반영 절차 • 사용자 인증 기능 • 중요 데이터 전송 및 보관 시 적용 기술/기법	참고사항 (샘플자료)	• 정보보호 정책서 • 시스템개발보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ 점검항목 1)

■ 클라우드 시스템 설계 시 사용자 인증에 대한 보안요구사항을 정의하여야 한다.
- 인증 시기 : 클라우드 시스템이 사용자를 인증해야 하는 시점
- 패스워드 관련 : 패스워드 잠김 임계치 설정, 패스워드 암호화, 패스워드 길이 및 조합규칙, 패스워드 변경 주기 등
- 접근 권한 : 동일사용자 동시접근 제한, 동일권한 동시접근 제한, 접근 IP 또는 MAC 제한 등
- 세션 관리 : 관리자 등 접근 후 관리 활동을 수행하지 않는 경우 타임아웃 설정 등
- 추가적인 사용자 인증 : 중요한 시스템(예 : 개인정보처리시스템 등)의 경우 추가적인 인증(예 : OTP, 바이오, 공인인증서 등) 요구

■ 사용자 인증 시 고려대상은 다음을 포함해야 된다.
- 서비스 이용자를 위한 웹 포털 및 어플리케이션 인증
- 하이퍼바이저 및 관리 스택 인증
- 관리서버 사용자 인증
- 개인정보 수집서버 및 과금관련 서버 등

⇨ 점검항목 2)

■ 중요 정보로 분류된 데이터에 대하여 저장 시에 암호화 및 복호화를 적용하도록 설계하여야 한다.

- 이때 사용되는 암호 알고리즘은 안전성이 입증된 알고리즘과 키 길이를 사용 (클라우드 정보보호 기준 12.3.1 암호정책 수립 참고)

⇨ 점검항목 3)

■ 클라우드 시스템을 통해 중요 정보를 송·수신하는 경우 기밀성 및 무결성을 지원하는 안전한 채널을 통하여 중요 정보를 송·수신하여야 한다.

- 기밀성 및 무결성이 보장되는 통신은 일반적으로 VPN 사용, TLS V1.2 이상이 적용된 SSL 통신 및 SSH 통신 등이 있다.

통제항목	13.1.3 보안로그 기능		
세부통제내용	클라우드 시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 하여야 한다.		
점검항목	1) 클라우드서비스 설계 시 보안관련 로그, 감사증적 등을 확보할 수 있는 기능을 반영하고 있는가? 2) 클라우드서비스 설계 시 보안로그를 보호하기 위한 대책을 마련하고 있는가?		
신청기관 준비사항 (관련증적)	• 시스템 설계서 • 시스템 변경 내역서 • 보안요구사항 정의/반영 절차 • 시스템 감사 증적 생성 및 보호 기능	참고사항 (샘플자료)	• 정보보호 정책서 • 시스템개발보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ **점검항목 1)**

■ 보안사고 발생 시, 책임 추적을 위하여 클라우드 시스템은 다음과 같은 감사증적(로그)을 확보할 수 있도록 설계하여야 한다.
- 사용자, 관리자의 접속기록 (로그인 및 로그아웃)
- 사용자 권한 부여, 변경, 말소 기록
- 중요 정보에 대한 접근 및 다운로드 기록
- 특수권한으로의 접근기록
- 감사증적은 발생일시, 발생 주체(ID, IP 등), 주체의 활동 내역이 포함되어야 함

⇨ **점검항목 2)**

■ 클라우드 시스템 설계 시 감사증적의 변조 및 비인가된 삭제를 방지하기 위한 대응이 가능하도록 설계하여야 한다.
- 감사증적에 대한 접근통제
- 감사증적에 대한 무단변경 방지
- 이용자 또는 관리자라 하더라도 감사증적에 대한 변경이나 삭제 불가

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

통제항목	13.1.4 접근권한 기능		
세부통제내용	클라우드 시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다.		
점검항목	1) 클라우드 서비스 설계 시 시스템 사용자의 업무 목적, 기능, 중요도에 따라 접근권한이 부여될 수 있도록 접근권한 부여 기능을 보안 요구사항 및 설계에 반영하고 있는가?		
신청기관 준비사항 (관련증적)	• 시스템 설계서 • 시스템 변경 내역서 • 보안요구사항 정의/반영 절차 • 시스템 접근권한 부여 기능	참고사항 (샘플자료)	• 정보보호 정책서 • 시스템개발보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

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

- 사용자별
- 사용자 업무 역할별(일반 사용자, 관리자, 개인정보취급자 등)
- 기능별(보안 기능, 서비스 기능, 관리기능 등)
- 메뉴별 등(설정 메뉴, 조회 메뉴 등)

통제항목	13.1.5 시각 동기화		
세부통제내용	로그기록의 정확성을 보장하고 법적인 자료로서 효력을 지니기 위해 클라우드 시스템 시각을 공식 표준시각으로 정확하게 동기화하여야 한다. 또한 서비스 이용자에게 시각 정보 동기화 기능을 제공하여야 한다.		
점검항목	1) 각 클라우드시스템의 시각을 표준시각으로 동기화하고 있는가?		
신청기관 준비사항 (관련증적)	• 시스템 설계서 • 시스템 변경 내역서 • 보안요구사항 정의/반영 절차 • 시스템 표준 시각 동기화 설정	참고사항 (샘플자료)	• 정보보호 정책서 • 시스템개발보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ 점검항목 1)

■ 클라우드서비스 설계 시 감사증적(로그)의 생성일시를 동기화하기 위하여 표준시각을 동기화하는 기능을 제공하여야 한다.

- 운영체제에서 제공하는 NTP 서버 동기화 기능 활용
- 클라우드 시스템이 직접 NTP 서버와 동기화를 위해 NTP 서버를 설정하는 기능 제공
- 서비스 이용자에게 시각 정보 동기화 기능 제공

13.2 구현 및 시험

통제항목	13.2.1 구현 및 시험		
세부통제내용	안전한 코딩방법에 따라 클라우드컴퓨팅서비스를 구현하고, 분석 및 설계 과정에서 도출한 보안 요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다.		
점검항목	1) 클라우드서비스의 안전한 구현을 위한 코딩표준이 마련되어야 하며 이에 따라 구현하고 있는가? 2) 구현된 기능이 사전 정의된 보안 요구사항을 충족하는지 시험을 수행하고 있는가?		
신청기관 준비사항 (관련증적)	• 시큐어 코딩 기준 • 보안 요구사항 충족 시험 증적	참고사항 (샘플자료)	• 정보보호 정책서 • 시스템개발보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ **점검항목 1)**

■ 클라우드 시스템을 안전하게 개발하기 위하여 안전한 코딩표준 및 규약에 따라 구현하여야 한다.

- 외부 환경 분석(법, 제도, 규정 등)을 통한 항목 식별 및 적용
- 기능에 대한 보안항목 식별
  . 사용자가 입력한 데이터의 유효성 확인 및 안전한 오류 처리
  . SQL 삽입 방지
  . 검증되지 않은 URL 리다이렉션 방지
  . 안전한 세션 관리 등

※ 소프트웨어 개발 보안 가이드 (KISA, 참고)

➪ **점검항목 2)**

■ 클라우드 시스템 구현 완료 후 사전 정의된 보안요구사항이 설계된 대로 구현되었는지 확인하기 위하여, 시험 시나리오, 체크리스트 등을 작성하여 시험을 수행하여야 한다.

- 모든 보안요구사항이 구현되었는지 확인

■ 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.

통제항목	13.2.2 개발과 운영환경 분리		
세부통제내용	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다. 단 분리하여 운영하기 어려운 경우 그 사유와 타당성을 검토하고 안전성 확보 방안을 마련하여야 한다.		
점검항목	1) 클라우드서비스의 개발 및 시험 시스템을 운영시스템과 분리하고 있는가? 2) 운영환경으로의 이관 절차를 수립하고, 이에 따라 이행하고 있는가?		
신청기관 준비사항 (관련증적)	• 개발/시험 및 운영 네트워크 구성도 • 운영환경 이관 절차	참고사항 (샘플자료)	• 정보보호 정책서 • 시스템개발보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 클라우드서비스는 원칙적으로 개발/시험 환경과 운영환경이 분리되어야 한다.

- 개발 및 시험 시스템과 운영 시스템의 분리

■ 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

⇨ **점검항목 2)**

■ 개발/시험이 완료된 결과를 운영환경으로 이관하기 위한 절차를 수립하여야 한다.

- 개발환경에서 운영환경으로의 이관방법
- 이관 중 발생 가능한 문제 예상 및 대응방안
- 이관에 대한 책임자 승인절차

통제항목	13.2.3 시험 데이터 보안		
세부통제내용	시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다.		
점검항목	1) 시험데이터는 임의의 데이터를 생성하거나 운영데이터를 가공하여 사용하고 있는가? 2) 운영데이터를 시험 환경에서 불가피하게 사용할 경우 책임자 승인 등의 인가 후 제한된 환경에서 사용하고 있는가? 3) 시스템 및 어플리케이션이 활성화되기 전에 시험데이터와 계정을 제거하고 있는가?		
신청기관 준비사항 (관련증적)	• 시험데이터 관리 절차 • 운영데이터의 시험 환경 사용 여부 • 운영 전 시험데이터 및 시험 계정 삭제 여부	참고사항 (샘플자료)	• 정보보호 정책서 • 시스템개발보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 시험에 사용되는 데이터의 생성, 이용 및 관리, 파기에 관한 절차를 수립하여 적용하여야 한다.

■ 시험에 사용되는 데이터는 가급적 임의로 생성한 데이터를 이용하여야 하며, 필요한 경우 가공된 운영데이터를 이용할 수 있다.

⇨ 점검항목 2)

■ 부득이하게 운영데이터를 시험데이터로 사용하는 경우 책임자의 승인을 받아야 하며, 제한된 시험환경에서 사용되어야 한다.

■ 운영데이터의 사용에 대한 기록(사용된 시험항목, 사용자, 폐기 여부 등)을 남겨야 하며, 사용이 완료된 운영데이터는 즉시 폐기하여야 한다.

⇨ 점검항목 3)

■ 시험이 완료된 시스템 및 어플리케이션은 운영 전 시험에 사용된 시험데이터 및 계정은 모두 삭제하여야 한다.

- 시험 데이터, 테스트 계정
- 테스트 및 디버깅 툴, 소스프로그램 등

통제항목	13.2.4 소스 프로그램 보안		
세부통제내용	소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행하여야 한다. 또한 소스 프로그램은 운영환경에 보관하지 않는 것을 원칙으로 한다.		
점검항목	1) 클라우드 서비스 구현과 관련된 소스 프로그램(소스코드)에 대해 변경관리를 수행하고 있는가? 2) 클라우드 서비스의 소스 프로그램(소스코드)은 인가된 사용자만이 소스 프로그램(소스코드)에 접근할 수 있도록 통제를 구현하고 있는가?		
신청기관 준비사항 (관련증적)	• 소스코드 관리 절차 • 소스코드 관리 방법 * 소스코드 권한 관리 및 접근 통제	참고사항 (샘플자료)	• 정보보호 정책서 • 시스템개발보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ **점검항목 1)**

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

- 소스 코드에 대한 변경관리를 위하여 형상관리 베이스라인을 정의
  - ・베이스라인 : 각 형상항목의 기술적 통제 시점으로 개발과정의 각 단계별 산출물을 검토, 평가, 조정, 처리 등의 변화를 통제하는 시점의 기준
  - ・예를 들면, OOO 소프트웨어 V1.0을 릴리즈한 시점을 베이스라인으로 설정하였다면 V1.0 이후 변경에 대한 관리를 수행하여야 한다는 의미
  - ・변경에는 소스 코드의 수정, 추가, 삭제 등이 포함되며, 이러한 작업을 수행하는 경우 정해진 절차에 따라 수행 필요
- 소스 코드는 정해진 인력만 접근할 수 있도록 접근통제 수행(식별 및 인증)
- 소스 코드 관리는 형상관리 도구(Git, SVN, SourceSafe 등)를 이용하고 도구가 지원하는 식별 및 인증 기능을 활용

⇨ **점검항목 2)**

■ 소스 코드는 별도의 서버(형상관리 서버)에 보관하고 서버는 안전한 위치에 설치하여 운영하여야 하며, 소스코드 관리담당자만 접근할 수 있도록 서버에 대한 접근통제를 수행하여야 한다.

13.3 외주 개발 보안

통제항목	13.3.1 외주 개발 보안		
세부통제내용	클라우드 시스템 개발을 외주 위탁하는 경우 분석 및 설계단계에서 구현 및 이관까지의 준수해야 할 보안요구사항을 계약서에 명시하고 이행여부를 관리·감독하여야 한다.		
점검항목	1) 클라우드 시스템 개발을 외주 위탁하는 경우, 개발 시 준수해야할 보안 요구사항을 제안요청서에 기재하고 계약시에 반영하고 있는가? 2) 외주 위탁업체가 계약서에 명시된 보안요구사항을 준수하는지 여부를 관리·감독하고 있는가? 3) 클라우드 시스템 개발 완료 후, SW 보안취약점 제거여부 진단 등을 확인 후 검수·인수하고 있는가?		
신청기관 준비사항 (관련증적)	• 외주 개발 제안요청서/계약서 • 보안요구사항 점검 증적 • 검수(인수) 확인서	**참고사항 (샘플자료)**	• 정보보호 정책서 • 시스템개발보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ **점검항목 1)**

■ 시스템 개발에 적용되어야 할 보안요구사항을 계약서에 명시하여야 한다.
- 설계, 구현, 시험에 대한 요구사항
- 개발환경에 대한 요구사항
- 소스 코드 관리에 대한 요구사항
- 코딩 표준 및 규약에 대한 요구사항
- 개발 완료 후 수탁사로의 이관에 대한 요구사항

⇨ **점검항목 2)**

■ 수탁사가 계약서에 명시된 요구사항을 준수하고 있는지에 대한 관리·감독을 수행하여야 한다.
- 계약서 상에 명시된 요구사항을 준수하는지 주기적으로 점검 수행

⇨ **점검항목 3)**

■ 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.

13.4 시스템 도입 보안

통제항목	13.4.1 시스템 도입 계획		
세부통제내용	클라우드 시스템의 처리 속도와 용량에 대하여 주기적인 모니터링을 수행하고 안정성의 확보에 필요한 시스템 도입 계획을 수립하여야 한다.		
점검항목	1) 신규 클라우드 시스템 또는 보안시스템의 도입 계획을 수립하고 있는가?		
신청기관 준비사항 (관련증적)	• 시스템 도입 계획서	**참고사항 (샘플자료)**	• 정보보호 정책서 • 시스템개발보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

➪ **점검항목 1)**

■ 운영 중인 클라우드시스템 및 정보보호시스템에 대한 주기적인 모니터링을 수행하여 시스템의 안전성을 점검하여야 한다.

- 시스템의 점검결과를 분석하고 신규 시스템 도입을 위한 계획을 수립

■ 시스템 (신규) 도입 계획 수립 시 호환성, 운영환경, 제공되는 성능 수준 등을 분석하고 추가 도입의 필요성, 도입 시기 등을 결정할 수 있도록 계획을 수립하여야 한다.

- 성능, 안전성, 호환성, 신뢰성, 보안성, 법적 요구사항 등을 고려한 기능적, 운영적 요구사항을 정의하고 제품 선정 시 요구되는 규격의 만족 여부 등을 검토

■ 정보보호시스템을 도입하는 경우 국가/공공기관의 정보보호시스템 도입 기준(보안적합성 검증 등) 준수 등 법적 요구사항을 만족하는지 검토하여야 한다.

통제항목	13.4.2 시스템 인수		
세부통제내용	새로 도입되는 시스템에 대한 인수 기준이 수립되어야 하며, 인수 전에 테스트가 수행되어야 한다.		
점검항목	1) 신규 클라우드 시스템의 인수 여부를 판단하기 위하여 기본 보안설정 등이 반영된 인수 승인 기준을 수립하고 있는가? 2) 신규 클라우드 시스템의 인수 전 수립된 인수 승인 기준에 따른 적합성 테스트를 수행하고 있는가?		
신청기관 준비사항 (관련증적)	• 시스템 인수 기준 • 검수(인수) 확인서	참고사항 (샘플자료)	• 정보보호 정책서 • 시스템개발보안지침
ISMS-P 인증 취득 시 심사 생략 가능 대상		O	

점검항목 해설

⇨ 점검항목 1)

■ 신규 클라우드시스템 및 정보보호시스템을 구축 후 인수 전 13.4.1. 시스템 도입 계획 단계에서 식별되었던 요구사항의 만족 여부를 확인하기 위한 인수 기준을 수립하여야 한다.

- 도입 시스템(클라우드시스템 및 정보보호시스템 등)에 대한 인수 기준을 수립 (CC인증 확인서 및 보안기능 확인서 등 확인 포함)

■ 초기 설정 등 삭제 여부, 보안업데이트 적용 여부, 불필요한 계정(디폴트 계정, 임시 계정, 시험용 계정 등) 삭제 여부, 불필요한 서비스 및 포트 등의 차단 조치 여부, 이중화, 취약점 점검 후 이행조치 등 클라우드시스템 운영에 적합한 기준을 수립하여야 한다.

⇨ 점검항목 2)

■ 수립된 기준에 따라 인수과정에서 점검(필요한 경우 인수 테스트 등)을 수행하고 그 결과를 기록 보존하여야 한다.

14. 국가기관등의 보안요구사항

■ “14. 국가기관등의 보안요구사항” 내의 세부 보안 요구사항은 국가정보보안 기본지침 및 국가 클라우드 컴퓨팅 보안 가이드라인을 준수하여야 함

14.1 관리적 보호조치

통제항목	14.1.1 보안서비스 수준 협약		
세부통제내용	국가기관등의 보안 요구사항이 반영된 보안서비스 수준 협약을 체결하고, 클라우드컴퓨팅서비스 관련 정보보호 정보를 국가기관등에게 제공하여야 한다.		
점검항목	1) 국가기관등에 클라우드 서비스 제공 시, 국가기관등의 보안요구사항을 정의하여 계약(보안서비스 수준 협약 등) 시 반영하고 있는가? 2) 정보보호 대책 내 국가기관등의 보안요구사항의 정확한 구현 여부, 보안운영 및 모니터링 결과산출 여부 등에 대해 국가기관등에 주기적으로 보고하고 있는가?		
신청기관 준비사항 (관련증적)	• 표준계약서, 서비스수준협약서(SLA), 서비스 약관 등 • 국가기관등 보안요구사항 보고 증적	참고사항 (샘플자료)	-
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 국가기관등에 클라우드 서비스 제공을 위한 계약 시, 국가기관등의 보안요구사항을 정의하고 계약서(보안서비스 수준 협약 등)에 반영하여야 한다.

■ 국가기관등에 클라우드서비스를 제공하는 경우, 계약 또는 보안서비스 수준 협약 과정에서 다음 사항들을 고려하여야 한다.
- 클라우드컴퓨팅서비스 제공 범위
- 국가기관등과 IaaS 사업자의 책임 명시
- 이용자 데이터 소유권, 저장 위치, 이관 및 보호 방법 (국가기관등 클라우드컴퓨팅서비스의 물리적 위치는 국내로 한정)
- 계약의 만료 또는 종료 시 데이터의 처리
- 고객에게 영향을 미치는 제3자 또는 하도급 업체 관계에 대한 정보
- 서비스 수준 미달성시의 대응 절차 및 보상 방법

- 사고 또는 장애발생 시 대내·외 관련 기관 및 전문가와 협조체계를 구성하여 대응하고, 국가정보원 및 이용기관의 대응에 협조
- 사전인증이 필요한 제품군은 CC인증, 보안기능확인서 등을 받은 제품 도입
- 사고 또는 장애발생 시 대내·외 관련 기관 및 전문가와 협조체계를 구성하여 대응하고, 국가정보원 및 이용기관의 사고·장애 대응 및 예방보안 활동 등에 협조
- 클라우드 보안관제 수행 및 정부보안관제체계와 연계하기 위한 제반환경 지원 대한 사항 명기
- 클라우드 컴퓨팅 서비스 망 운용 관리에 따른 보안 취약점 개선·발굴, 사이버공격 위협에 대한 예방, 대응, 실태평가, 안전성 및 보안대책의 적합성과 이행여부 확인 등의 목적으로 클라우드 사업자 시설에 대한 현장실사 방문, 안전성 보안 측정 실시, 보안진단·점검 등 수행 협조 사항 명기
- 현장실사, 안전성 보안측정 실시, 보안점검 등 수행 목적으로 기술적 지원을 요청할 시에 모니터링 도구, 로그 수집 기술 등의 제반 환경을 제공 사항 명기
- 기타 국가기관등 보안 요구사항 (기관의 특성에 따라 달라질 수 있음)

⇨ 점검항목 2)

■ 클라우드컴퓨팅서비스 제공자는 클라우드 서비스를 구축하면서 적용한 정보보호대책이 국가기관등의 보안요구사항을 정확하게 반영하고 있는지 지속적으로 모니터링하고 서비스를 이용하는 국가기관등의 정보보호대책이 유지되는지 검토해야 한다.

- 서비스 제공자는 자신이 수립한 정보보호대책이 도입 국가기관등의 정보보호대책과 일관성을 유지하고 있는지 확인
- 서비스를 이용하는 국가기관등의 정보보호대책이 의도한 대로 운영되는지 확인

  (자산목록, 가상머신 내 운영체제, 가상 소프트웨어, 보안정책 등의 변경여부에 대한 모니터링 결과, 형상변경시의 보안영향분석결과 등)
- 서비스 제공자가 산출된 결과물을 서비스를 이용하는 국가기관등에게 보고하는 절차의 수립 및 이행 여부

■ 국가기관등의 보안요구사항 구현 여부 등에 대해서 주기적으로 국가기관등에 보고하여야 한다.

통제항목	14.1.2 도입 전산장비 안전성		
세부통제내용	클라우드컴퓨팅서비스 구축을 위해 도입되는 보안기능을 가진 정보통신제품 중에서 전자정부법 제56조에 규정된 전자문서의 위조·변조·훼손 또는 유출을 방지하기 위한 목적으로 도입하는 제품은 국가정보원장이 안전성을 확인한 제품을 사용하여야 한다.		
점검항목	1) 클라우드 시스템을 보호하기 위해 도입하는 정보통신 제품이 국가정보원장이 공지한 바에 따른 인증 요건을 만족하는가?		
신청기관 준비사항 (관련증적)	• 정보자산목록 • 정보보호제품 CC인증서 • 보안기능확인서 • 성능평가서	참고사항 (샘플자료)	-
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ **점검항목 1)**

■ 클라우드 서비스를 제공하기 위해 구축되는 정보보호시스템과 네트워크 장비 중에 CC 인증 또는 보안기능 확인서 등 사전 인증이 필수적인 제품군은 국가정보원장이 안정성을 확인한 제품을 도입하여야 한다.

※ 사전 인증이 필요한 국내·외 제품 유형은 국가정보보안기본지침 또는 국가정보원 홈페이지에서 확인 가능

- IT보안인증사무국(https://www.itscc.kr)
- 국가정보원(https://www.nis.go.kr)
- CC Portal(https://commoncriteriaportal.org)

※ 기타 세부사항은 국가정보원이 공지한 보안적합성 검증 정책을 따름

통제항목	14.1.3 보안관리 수준		
세부통제내용	클라우드컴퓨팅서비스 운영 장소 및 망은 국가기관등 내부 정보시스템 운영 보안수준에 준하여 보안 관리하여야 한다.		
점검항목	1) 국가기관등의 공통적인 보안 요구사항을 반영하여 그에 준하는 보안 대책을 수립하고 있는가?		
신청기관 준비사항 (관련증적)	• 물리적 위치 및 물리적 접근통제 정책 현황 • 관련 시설에 대한 주기적인 점검 이력	참고사항 (샘플자료)	-
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ 점검항목 1)

■ 서비스 제공자는 국가기관등에서 요구되는 시설 및 물리적 통제에 대한 보안요구 사항을 만족할 수 있도록 서비스를 제공하여야 한다.

- 국가기관 클라우드 서비스 제공을 위한 시스템의 물리적 위치 식별
- 식별된 물리적 공간에 대한 접근통제 정책 수립하고, 물리적 출입통제에 대한 산출물(작업내용 기록, 장비 반출입 기록, 출입 로그 등)을 유지·관리 및 이상 유무를 주기적 검토하여야 함
- 화재, 전력 이상 등 인재 및 자연재해 등에 대비하여 필요한 설비를 갖추고 이에 대한 보호 방안을 수립 적용하여야 함

※ 화재감지 및 소화설비, 누수감지기, CCTV, 외부침입감지 및 경보, 출입통제 시스템, UPS, 항온항습기, 비상발전기, 전압유지기, 전력선 이중화 등

통제항목	14.1.4 사고 및 장애 대응		
세부통제내용	클라우드컴퓨팅서비스를 제공하는 민간 사업자는 사고 또는 장애 발생 시 관계 법령이 정하는 바에 따라 해당 국가기관, 대내·외 관련 기관 및 전문가와 협조체계를 구성하여 대응하여야 하며, 피해확산 및 재발 방지와 복구 등에 필요한 조치를 위해 국가정보원 및 이용기관의 보안 관제 및 사고조사, 예방보안활동 등에 적극 협조하여야 한다.		
점검항목	1) 국가기관등 클라우드 서비스의 사고 및 장애 대응절차는 국가기관등의 사고 및 장애 대응절차를 반영하였는가? 2) 국가기관등 클라우드 서비스의 사고 및 장애 대응절차에는 해당 국가기관등, 대내외 관련기관과의 협조체계가 반영되어 있는가?		
신청기관 준비사항 (관련증적)	• 침해사고/장애 대응 절차 • 침해사고/장애 대응조직도 및 비상연락망 • 침해사고/장애 발생 보고서 • 침해사고/장애 신고/통지 절차 • 침해사고/장애 조치 보고서	참고사항 (샘플자료)	-
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ 점검항목 1)

■ 국가기관등 클라우드 서비스의 사고 및 장애 대응절차는 국가기관등의 사고 및 장애 대응절차를 반영하여 수립, 운영되어야 한다.

- 발생내용, 원인, 조치현황 등을 신속 파악
- 국가기관(이용기관) 등의 정보보안담당관에게 신고 절차 포함

■ 사고 및 장애 발생 시 국가기관등의 클라우드 보안사고 및 장애 대응 절차에 따라 진행되도록 사업자의 침해사고 대응 절차를 점검하고, 아래의 내용을 포함한 사고 발생 보고서를 해당 국가기관등에 제공할 수 있어야 한다.

- 사고 발생일시
- 보고자와 보고일시
- 사고내용 (원인, 발견사항, 피해내용 등)
- 사고대응 경과 내용
- 사고대응까지의 소요시간
- 사고자 및 관계자의 인적 사항
- 조치 내용 등

■ 클라우드컴퓨팅서비스 제공자는 다음의 하나에 해당하는 경우 지체없이 이용자에게 알려야 한다.

구분	신고	통지
침해사고 발생 시	관계법령에 따른 신고	이용자에게 통지 [통지 내용] 1. 발생 내용 2. 발생 원인 3. 클라우드컴퓨팅서비스 제공자의 피해 확산 방지 조치 현황 4. 클라우드컴퓨팅서비스 이용자(이하 "이용자"라 한다)의 피해 예방 또는 확산 방지 방법 5. 담당부서 및 연락처 [통지방법] 전화, 휴대전화, 우편, 전자우편, 문자메시지, 클라우드컴퓨팅서비스 접속화면 등
이용자 정보 유출 시	개인정보 유출 시 개인정보보호법에 따른 신고 그 외의 경우 클라우드컴퓨팅법에 에 다른 신고	
사전 예고 없이 일정한 기간 이상 서비스 중단 시 -중단기간이 연속 10분이상의 경우 -중단 사고가 발생한 때로부터 24시간 이내 2회 이상 중단된 경우 (중단된 기간이 15분 이상인 경우)	관계법령에 따른 통지	

⇨ 점검항목 2)

■ 클라우드컴퓨팅서비스 제공자는 신속한 사고 및 장애대응을 위하여 대내외 관련 기관 및 전문가와 협조 및 연락체계를 구축하여야 한다.

■ 클라우드컴퓨팅서비스 제공자는 아래와 같이 사이버공격과 관련한 정보를 확인한 경우에는 전화·팩스·이메일 등 통신수단을 활용하여 지체없이 그 사실을 국가기관등의 정보보안담당관에게 통보하고 국가정보원 및 국가기관등 에서 사고조사・예방활동 등에 협조하여야 한다.

- 대규모 사이버공격 발생시
- 사이버공격으로 인하여 피해가 발생하거나 피해 발생이 예상되는 경우
- 사이버공격이 확산될 우려가 있는 경우
- 그 밖에 사이버공격 계획 등 사이버안전에 위협을 초래할 수 있는 정보를 입수한 경우

14.2 물리적 보호조치

통제항목	14.2.1 물리적 위치 및 영역분리		
세부통제내용	클라우드 시스템, 백업 시스템 및 데이터와 이를 위한 관리·운영 인력의 물리적 위치는 국내로 한정하여야 한다. 또한, 국가기관용 클라우드컴퓨팅서비스의 물리자원(서버, 네트워크, 보안장비 등), 출입통제, 운영인력 등은 데이터 및 프로세스 등의 간섭없이 국가기관등의 보안관제, 사고조사, 예방보안활동 유지를 위한 제반 환경을 만족시킬 수 있도록 일반 이용자용 클라우드컴퓨팅서비스 영역과 물리적으로 분리하여 운영하여야 한다.		
점검항목	1) 국가기관용 클라우드 시스템, 데이터, 관리·운영 인력이 물리적으로 국내에 위치하고 있는가? 2) 국가기관용 클라우드 시스템과 민간용 클라우드 시스템 간 물리적 또는 논리적으로 분리(출입통제 및 기록, 네트워크 분리 등)하는 방안이 마련되어 있는가?		
신청기관 준비사항 (관련증적)	• 자산목록 • 네트워크 구성도 • 시설구성도	참고사항 (샘플자료)	-
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 국기기관등에 클라우드 서비스 제공과 관련된 시스템, 데이터, 관리·운영 인력은 물리적으로 국내에 위치하여야 한다.

- 국가기관등의 클라우드서비스를 운영하기 위한 모든 구성요소(데이터서버, 관리·운영서버, 인증서버, 로그 및 백업서버 등)는 국내에 위치하여야 함

※ 대한민국의 배타적 법적관할하에 있는 시설에 위치해야 함

- 클라우드 서비스 운영·관리(사고 및 장애대응, 이용자 계정 권한 부여/변경/삭제 등) 인력은 국내에 거주하여야 함

⇨ **점검항목 2)**

■ 국가기관등에 클라우드 서비스를 제공하는 시스템과 민간기관에 클라우드 서비스를 제공하는 시스템은 물리적 또는 논리적으로 영역을 분리하여야 한다.

- 국가기관등의 클라우드서비스를 위한 물리적 장치(IDC 내 클라우드 관련 인프라 등)가 설치된 시설에 대한 물리적인 출입통제 수행
- 물리적인 출입통제에 대한 출입기록 등 유지

통제항목	14.2.2 중요장비 이중화 및 백업체계 구축		
세부통제내용	클라우드컴퓨팅서비스를 제공하는 사업자는 네트워크 스위치, 스토리지 등 중요장비를 이중화하고 서비스의 가용성을 보장하기 위해 백업체계를 구축하여야 한다.		
점검항목	1) 국가기관등 클라우드 시스템에 대해 네트워크 스위치, 스토리지 등 중요장비가 이중화로 구축되어 있는가? 2) 국가기관등 클라우드 시스템에 대한 백업에 대한 전반적인 표준운영절차(SOP)를 수립하였는가?		
신청기관 준비사항 (관련증적)	• 정보자산목록 • 네트워크 구성도 • 백업지침(표준운영절차) • 백업 관리대장	참고사항 (샘플자료)	-
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ 점검항목 1)

■ IaaS의 장애 및 사고 발생에 대비하여 네트워크 장비, 스토리지 등 IaaS 서비스 제공에 중요한 역할을 담당하는 물리적인 자원에 대하여 이중화를 구축하여 운영하여야 한다.

⇨ 점검항목 2)

■ 서비스를 이용하는 국가기관등의 업무 관련 정보를 안전하게 유지하기 위하여 백업 및 복원 체계를 구축하고 유지하여야 한다.

■ 백업 및 복원을 위한 백업사이트 구축 및 운영 지침(표준운영절차)를 수립하여 적용하여야 한다.

■ 사고 발생 시 즉시 복원이 가능한지 지속적으로 모니터링을 수행하여야 하며, 백업사이트 구축 및 운영 지침 등에 복원을 위한 절차를 포함하여야 한다.

14.3 기술적 보호조치

통제항목	14.3.1 검증필 암호화 기술 제공		
세부통제내용	클라우드컴퓨팅서비스를 통해 생성된 중요자료를 암호화하는 수단을 제공하는 경우에는 검증필 국가표준암호화 기술을 제공하여야 한다.		
점검항목	1) 보안적합성검증 제품 유형 중 가상사설망, 보안 USB, 호스트 자료유출 방지제품(암호화 저장가능 존재시) 등 중요자료 전송 및 저장을 위해 사용하는 제품들에 대해서 검증필 암호모듈을 탑재하고 있는가?		
신청기관 준비사항 (관련증적)	• 정보보호제품 목록 • 적용된 검증필 암호모듈 목록(정책서 포함) • CC인증, 보안기능 확인서 등 사본 • 보안기능시험결과서	참고사항 (샘플자료)	-
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

➪ **점검항목 1)**

■ IaaS 서비스를 운영하는데 사용되는 VPN, 보안USB, 자료유출방지 등의 제품이 운영되는 경우 검증필 암호모듈이 적용된 제품을 사용하여야 한다. 또한, 해당 제품은 CC 인증 또는 보안기능 확인서 등을 획득한 제품을 사용하여야 한다.

※ 기타 세부사항은 국가정보원의 보안적합성 검증 정책, 암호모듈검증 정책에 따름

■ 검증필 암호모듈과 CC인증의 유효기간은 별도이므로 둘 중 하나의 유효기간이 만료되면 해당 제품은 유효하지 않은 것으로 판단하여야 한다.

※ 검증필 암호모듈 탑재 필수 제품 유형은 국가정보보안기본지침 또는 국가정보원 홈페이지에서 확인 가능

- IT보안인증사무국(https://www.itscc.kr)
- 국가정보원(https://www.nis.go.kr)

통제항목	14.3.2 보안관제 제반환경 지원		
세부통제내용	클라우드컴퓨팅서비스를 국가기관등에 제공하는 민간사업자는 민간 영역을 제외한 공공 영역 대상 사이버공격 및 위협을 탐지하기 위한 국가기관등의 클라우드컴퓨팅서비스 보안관제 수행 및 정부보안관제체계와 연계하기 위해 필요한 제반환경을 지원하여야 한다.		
점검항목	1) 국가기관등에 클라우드 서비스 보안관제 수행에 필요한 제반환경을 지원하고 있는가?		
신청기관 준비사항 (관련증적)	• 보안관제 월간보고자료 • 보안관제 수행을 위해 제공되는 환경	참고사항 (샘플자료)	-
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

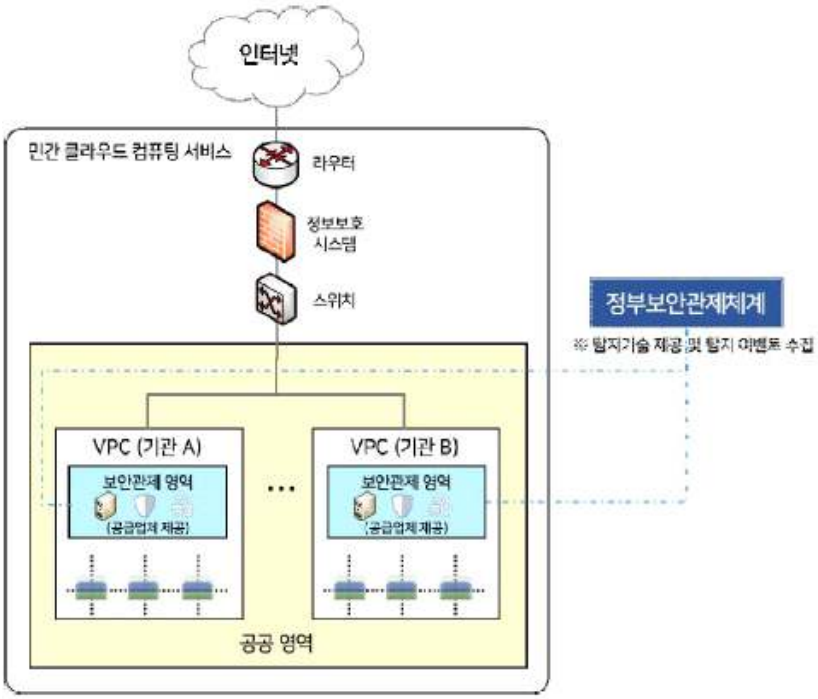
■ 민간 사업자는 국가기관 등에 클라우드 컴퓨팅 서비스 보안관제 수행 및 정부보안관제체계와 연결하기 위해 필요한 제반환경을 지원하여야 한다.

- 이용기관은 보안관제 시스템을 구축하고 직접 보안관제를 수행하거나 다른 국가·공공기관이 운영하는 보안관제시스템을 활용하는 것이 효율적인 경우 다른 기관의 보안관제센터에 위탁가능
- 민간 사업자는 이용기관이 민간 클라우드 컴퓨팅 서비스에 대한 보안관제 수행에 필요한 제반환경을 지원

■ 클라우드에 구축된 보안관제 시스템은 정부보안관제체계와 연계되어야 하며, 세부사항은 국가 클라우드 컴퓨팅 보안 가이드라인 참조

- 서비스 공급업체는 기관 VPC 영역에서 보안관제를 수행할 수 있는 기반 제공
- 서비스 공급업체는 기관의 보안관제 영역과 정부보안관제체계를 연계할 수 있는 기반 제공
- 이용기관은 보안관제 영역에서 탐지기술을 적용하여 보안관제를 수행하며, 탐지정보를 정부보안관제체계와 연계

<국가 클라우드 컴퓨팅 보안 가이드라인>



통제항목	14.3.4 시스템 격리		
세부통제내용	클라우드컴퓨팅서비스는 보안관제가 이뤄지는 서비스 네트워크 이외의 비정상 통신경로가 발생하지 않도록 주기적으로 검토하고 점검하는 체계 마련 등 기술적 대책을 수립하여야 한다.		
점검항목	1) 국가기관등 클라우드 서비스에서 비정상 통신경로가 발생하지 않도록 주기적 검토를 수행하고 있는가?		
신청기관 준비사항 (관련증적)	• 비정상 통신경로 점검 결과 및 검토 결과	참고사항 (샘플자료)	-
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 클라우드컴퓨팅서비스는 보안관제가 이루어지는 서비스 네트워크 외에 비정상 통신경로가 발생하지 않도록 주기적으로 검토하여야 한다.

- 민간 클라우드컴퓨팅 서비스 관리자가 이용기관에 할당된 자원(메모리・HDD 등), 데이터에 임의 접근하지 못하도록 접근제어 및 격리 등을 통한 기술적 접근통제 수단을 마련하여 제시
- 이용자가 본인에게 할당된 자원 이외의 자원에 접근하지 못하도록 기술적 통제 수단 마련하여 제시
- 클라우드 시스템은 무선망과 분리하고 무선접속에 대한 접근을 통제
- 가상머신 탈출, 은닉 채널 생성 등 비정상 통신경로를 발생 시킬 수 있는 최신 보안 취약점을 주기적으로 점검・확인 하고 보안패치 적용
- 외장하드, USB 등 이동매체를 통한 악성코드 감염방지 대책 마련 필요
- 비정상 통신경로 등을 확인할 수 있는 기술적 대책(스캔, 모니터링 등) 수립

통제항목	14.3.5 영역분리		
세부통제내용	국가기관용 클라우드컴퓨팅서비스와 일반 이용자용 클라우드컴퓨팅서비스는 영역분리를 통해 데이터 및 프로세스 등의 간섭없이 국가기관 등의 보안관제, 사고조사, 예방 보안활동 유지를 위한 제반환경을 만족시킬 수 있도록 기술적 보호조치를 취해야 하며, 영역 분리를 훼손하여 데이터에 접근할 수 있는 취약점을 방지/완화/제거 하고, 비인가 접근을 모니터링 해야 한다.		
점검항목	1) 클라우드 서비스는 물리적·논리적 분리를 통해 영역간 분리가 수행되고 있는가? 2) 일반 이용자용 클라우드컴퓨팅서비스와 영역분리되어 데이터 및 프로세스 등의 간섭없이 국가정보원 및 이용기관의 보안관제, 사고조사, 예방활동 유지를 위한 제반 환경을 만족시킬 수 있는 보호조치를 취할 수 있는가?		
신청기관 준비사항 (관련증적)	• 민간 공공영역 영역 분리증적 • 비인가 접근 모니터링 결과 • 보안관제 및 예방 활동 결과보고서	참고사항 (샘플자료)	-
ISMS-P 인증 취득 시 심사 생략 가능 대상		X	

점검항목 해설

⇨ **점검항목 1)**

■ 일반이용자용 클라우드와 국가·공공기관용 클라우드 서비스는 물리적·논리적 분리를 통해 상호 데이터 등에 접근할 수 없도록 기술적 보호조치를 취해야 한다.

- 국내 민간 사업자 클라우드센터에 위치
- 국가·공공기관용 클라우드 컴퓨팅 서비스 영역과 민간 이용자용 클라우드 컴퓨팅 서비스 영역 간 물리적·논리적 영역 분리 수행
- 논리적으로 영역 분리를 하는 경우, 영역 분리를 훼손하여 데이터에 접근할 수 있는 취약점을 방지/완화/제거하고 비인가 접근 모니터링 수행 등
- 클라우드 서비스를 이용하는 이용자가 영역 분리(물리적 또는 논리적) 및 영역 분리를 위한 보호조치 등에 대한 증적 자료 등을 요청할 경우, 이를 위한 자료를 제출하여야 함

⇨ **점검항목 2)**

■ 국가정보원 및 국가기관에서 사고조사 및 예방활동을 요청하는 경우 활동을 위한 제반환경을 제공하여야 한다.

- 이용기관별로 일반이용자용 클라우드와 영역분리되어 각 영역 마다 사고조사, 예방보안활동 등 국가정보원 및 이용기관의 사이버위협 대응활동 유지를 위한 제반환경 만족하도록 구성

클라우드서비스(IaaS)
보안인증기준 해설서

발행일 : 2023년 3월

발행처 : 과학기술정보통신부, 한국인터넷진흥원

< 비매품 >