정보보호 관리체계(ISMS) 운영지침

ICT전략실 정보보호부

제정 2021.04.12. 지침 제330호

개정 2023.12.18. 지침 제412호

(상임이사·지원·지원장 명칭 변경 등에 따른 계약사무처리지침 등 26개 지침의 일부개정에 관한 지침)

제1장 총칙

제1조(목적) 이 지침은「정보통신망법」제47조(정보보호 관리체계 인증)에 따라 건강보험심사평가원의 정보보호 관리체계 인증 업무의 효율적 운영을 기하기 위하여 필요한 세부사항을 규정함을 목적으로 한다.

제2조(정의) 이 지침에서 사용하는 용어의 정의는 다음의 각 호와 같다.

1. “정보보안최고책임자(CISO)”라 함은「정보보안지침」제5조에 따른 정보보안최고책임자(CISO)를 말한다.
2. “분임보안담당관”이라 함은「보안업무 운영세칙」제5조에 따른 분임보안담당관을 말한다.
3. “보안심사위원회”라 함은「보안업무 운영세칙」제2장에 따른 보안심사위원회를 말한다.
4. “정보보안조직구성원”이라 함은「직제규정」에 따라 정보보안업무를 총괄하는 부서의 소속직원을 말한다.
5. “정보시스템관련부서”라 함은 심사평가원의 ICT 자산을 도입·운영·관리하는 부서를 말한다.
6. “시스템담당자”라 함은 “정보시스템관련부서” 소속의 ICT 자산을 담당하여 운

영・관리하는 해당 직원을 말한다.

7. “시스템관리자”라 함은 “시스템담당자” 가 소속된 부에서 해당시스템의 관리를 책임지는 상급자를 말한다.
8. “개발담당자”라 함은 심사평가원의 ICT 자산을 활용하여 업무용 응용프로그램을 개발・운영하는 업무를 담당하는 직원을 말한다.
9. “네트워크담당자”라 함은 심사평가원의 ICT 자산 중 네트워크 분야에 해당하는 자산을 담당하여 운영・관리하는 해당 직원을 말한다.

제3조(다른 법령과의 관계) 건강보험심사평가원(이하 “심사평가원”이라 한다)의 정보보호 관리체계 인증 유지에 관하여는 다른 법령 또는 제규정에 특별히 정하고 있는 경우를 제외하고는 이 지침에서 정하는 바에 따른다.

제2장 정보보호 정책 및 조직

제4조(정책의 수립 및 운영) ① 이 지침은 이해관계자의 협의 또는 심사평가원「보안업무 운영세칙」제2장에 따른 보안심사위원회의 심의를 거쳐 건강보험심사평가원장(이하 "원장"이라 한다)의 최종 승인 후 시행한다.

② 이 지침의 시행을 위해 하위 가이드 등을 제·개정하는 경우에는 분임보안담당관이 작성하여 원장의 승인을 받은 후 시행하여야 한다.

③ 제2항에서 정한 바에 따라 수립되는 체계를 제외하고 이 정책의 원활한 시행을 위하여 부서 또는 본부 등 별도의 가이드 등을 수립할 수 있으며, 이 경우 이 지침과의 일관성 유지를 위하여 그 시행 전에「직제규정 시행세칙」에 따라 정보보호업무를 담당하는 부에서 검토를 받고 시행한다. <개정 2023.12.18.>

④ 이 지침은 임직원 및 관련자가 이해하기 쉽도록 작성 및 관리되어야 한다.

제5조(정책의 검토) ① 정보보안최고책임자(CISO)는 다음 각 호의 상황을 고려하여 정보보호 관리체계(ISMS) 운영지침에 대해 연 1회 이상 변경 여부를 검토하고 필요시에 변경하여야 한다.

1. 정보보호 목표 및 전략의 변경

2. 정보보호 관련 조직 구조 및 인력의 중대한 변경

3. 중대한 보안사고 및 새로운 위협·취약점이 발생한 경우

4. 관련 상위법의 제·개정 확인 여부

5. 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 기준 재검토

6. 그 밖에 정보보안최고책임자(CISO)가 필요하다고 판단하는 경우

② 이 지침의 이력관리를 위하여 제·개정 이력목록을 기록하여야 하며, 제·개정 시 관련 정책 간에 일관성 여부를 검토하여야 한다.

제6조(정보보안 조직의 운영) ① 정보보안최고책임자(CISO)는 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 기준 준수 여부를 총괄 한다.

② 정보보안최고책임자(CISO)는 정보보안조직구성원에게 업무를 부여하고 관리 감독하여야 한다.

③ 정보보안조직구성원은 정보보호 활동을 원활하게 수행할 수 있도록 다음 각 호의 사항을 고려하여 구성하여야 한다.

1. 정보보호 전문지식 보유 여부 (정보보호 관련 학위 또는 자격증 보유 여부 포함)

2. 정보보호 관련 실무경력

3. 정보보호 관련 직무교육 이수 등

제7조(주요 직무자 지정 및 감독) ① 분임보안담당관은 다음 각 호의 업무를 담당하는 직원에 대하여 주요 직무자로 지정하고 그 목록을 정기적으로 갱신하여 관리하여야 한다.

1. 주요 정보시스템이 집적되어 설치되어 있는 통제구역에 출입권한을 부여 받은 내부직원

2. 개인정보처리시스템에서 계정 생성 및 접근권한을 설정, 데이터베이스에 직접 접속 및 정보시스템에 관리자권한으로 접속 등 을 할 수 있는 직원

② 분임보안담당관은 주요 직무자로 지정된 직원 PC에 대한 인터넷 제한 등의 보호조치를 적용하여야 한다.

제8조(직무분리 원칙) ① 정보자산에 대한 접근 및 열람 등의 권한은 개인의 보직 및

임무에 따라 정보보안최고책임자(CISO)가 검토하여 상이한 권한을 부여하며, 권한의 남용을 방지하기 위하여 직무역할을 명확히 분리·운영한다.

② 다음 각 호의 직무에 대해서는 분리·운영 할 수 있다.

1. 개발과 운영 직무 분리
2. 정보시스템(서버, DB, 네트워크 등)간 운영 직무 분리
3. 정보보호 관리와 정보시스템 운영 직무 분리
4. 정보보호 관리와 정보시스템 개발 직무 분리 등

③ 제2항의 경우에도 불구하고 인적자원 부족 등의 사유로 불가피하게 직무분리가 어려운 경우 직무자간의 상호 검토, 상위 관리자의 주기적인 직무수행 모니터링, 변경사항 검토 및 직무자의 책임 추적성 확보 등 보완대책을 수립하여야 한다.

제3장 정보자산 분석 위험평가

제9조(인증범위 설정) ① 심사평가원 대국민 홈페이지(이하 “홈페이지”라 한다) 서비스 내 조직의 핵심 서비스 및 개인정보 처리에 영향을 줄 수 있는 핵심자산을 포함하도록 관리체계 범위를 설정하여야 한다.

② 홈페이지 서비스 내 정의된 범위 내에서 예외사항이 있을 경우 명확한 사유 및 관련자 협의·책임자 승인 등 관련 근거를 기록·관리하여야 한다.

③ 홈페이지 서비스 내 정보보호 및 개인정보보호 관리체계 범위를 명확히 확인할 수 있도록 관련된 내용(주요 서비스 및 업무 현황, 정보시스템 목록 및 문서목록 등)이 포함된 문서를 작성하여 관리하여야 한다.

제10조(정보자산 식별) ① 시스템담당자는 인증범위 내 자산을 식별하여 기록하여 관리하여야 한다.

② 시스템담당자는 "정보자산 분류 및 중요도 평가분석 결과서" 내 "자산분류기준"에 명시된 자산에 대해 연 1회 이상 그 현황을 최신 내용으로 유지하여야 한다.

③ 심사평가원의 정보시스템관련부서는 시스템담당자의 정보자산 목록정보 요청에 협조하여 정보자산의 목록이 최신으로 유지될 수 있도록 한다.

④ 정보자산 분류에 대한 세부적인 사항은 "정보자산 분류 및 중요도 평가분석 결과

서" 내 "자산분류기준"을 참조한다.

제11조(정보자산의 중요도 평가) 시스템담당자는 "기반시설 위험평가 관리 매뉴얼"의 "4. 자산의 중요도 평가" 기준을 참조하여 정보자산의 중요도(보안등급)를 평가하며, 이 경우 중요도 평가는 평가자의 주관에 따라 중요도 산정에 오류가 생길 수 있으므로 취급부서의 의견 및 외부전문가의 의견 등을 함께 고려하여 정확한 중요도 등급 산정이 이루어지도록 한다.

제12조(현황 및 흐름분석) ① 홈페이지 서비스 내 관리체계 전 영역에 대한 정보서비스 현황을 파악하고 업무 절차와 흐름을 파악하여 문서화하여야 한다.

② 홈페이지 서비스 내 관리체계 범위 내에서 개인정보 처리 현황을 식별하고 개인정보의 흐름을 파악하여 개인정보흐름도 등으로 문서화 할 수 있다.

③ 홈페이지 서비스 내 서비스 및 업무, 정보자산 등의 변화에 따른 업무절차 및 정보서비스 흐름을 주기적으로 검토하여 흐름도 등 관련 문서의 최신성을 유지하여야 한다.

제13조(취약점 분석) ① 분임보안담당관은 취약점 점검 항목을 참조하여 상세한 진단 항목이 포함된 관리적, 법적 및 기술적 취약점 진단계획을 수립하고 정보보안최고책임자(CISO)의 승인을 받아야 한다. 이 경우 대상 정보자산의 취약점 진단 시 업무 연속성 등에 문제 발생 우려가 있을 때에는 사전에 취급 부서에 대한 업무 협조를 요청할 수 있다.

② 분임보안담당관은 관리적, 법적 및 기술적 취약점 진단을 연 1회 이상 수행한다.

③ 발견된 취약점에 대하여 즉시 조치(Quick Fix)가 가능한 경우 취약점을 제거할 수 있으며, 이 경우 제거된 취약점은 대상 정보자산에 위험을 주지않으므로 위험평가 대상에서 제외하여야 한다.

④ 분임보안담당관은 제3항의 취약점 제거를 포함하여 관리적, 법적 및 기술적 취약점 진단결과를 도출하고 이를 별도의 위험분석 결과 보고서로 작성하여 정보보안최고책임자(CISO)에게 보고하여야 한다.

⑤ 제4항의 경우 관리적, 법적 및 기술적 취약점 진단결과는 위험분석 결과 보고에

포함하여 보고할 수 있다.

제14조(위협분석) ① 정보자산의 취약점을 이용하여 피해를 줄 수 있는 잠재적 가능성인 위협을 관련 시스템담당자와 인터뷰 및 실사를 통하여 식별한다.

② 식별된 위협은 “기반시설 위험평가 관리 매뉴얼”의 ″6. 위협 분석″ 기준을 참고하여 위협등급을 산정하여야 한다.

제15조(위험분석) ① 분임보안담당관은 다음 각 호의 위험분석 방법을 기준으로 위험을 분석하여야 한다.

1. 기준선 접근법 : 도출된 모든 위험에 대하여 점검기준에서 요구하는 수준의 보호대책을 적용 (관리적 위험분석 및 법적 준거성 위험분석)
2. 상세위험분석법 : 각 위험에 대하여 위험도를 산정하고 위험도에 따라 서로 다른 위험대응방안을 적용. 수용 가능한 위험수준(DoA)를 결정하고 DoA를 기준으로 위험대응방법 결정 (기술적 위험분석)

② 기술적 위험분석 대한 세부사항은 기반시설 위험평가 관리 매뉴얼의 ″8. 위험 시나리오(우려사항) 수준 평가 기준″ 기준을 참조한다.

제16조(위험도 산정) ① 위험도는 정보자산(Assets) 등급 및 취약점(Vulnerability) 등급, 위협(Threats) 등급을 평가요소로 하여 평가한다.

② 위험도 평가에 따라 허용 가능한 위험수준(DoA : Degree of Assurance)를 산정하여 위험을 관리한다.

③ 허용 가능한 위험수준(DoA : Degree of Assurance)에 대한 산정은 유관부서와 인터뷰 등을 통하여 적절한 수준으로 결정하고 정보보안최고책임자(CISO)의 승인을 받아야 한다.

④ 위험도 산정에 대한 세부사항은 “기반시설 위험평가 관리 매뉴얼”의 ″10. 위험도 산정″ 기준을 참조한다.

제17조(보호대책의 수립 및 공유) ① 분임보안담당관은 관련 시스템 담당자와 협의하여 도출된 위험 중 허용 가능한 위험수준 이상인 위험에 대해 위험회피, 위험전가

및 위험감소 등의 위험관리 전략을 수립한다.

② 허용 가능한 위험수준 이하인 위험에 대해서도 서비스 영향 정도 등을 고려하여 조치가 가능한 위험에 대해서는 보호대책을 수립하여 조치할 수 있다.

③ 분임보안담당관은 제2항의 보호대책을 수립한 경우 정보보안최고책임자(CISO)의 승인을 받아야 한다.

④ 수립된 보호대책을 각 담당자에게 공유하고, 보호대책에 대한 해결방법을 알기 쉽게 교육을 하여야 하며, 향후 동일한 보호대책 재발방지를 위해 숙지하여야 한다.

제18조(위험관리 조치계획의 수립) ① 수립된 보호대책을 바탕으로 법률적 시급성, 사업적 시급성, 예산운용 가능성 및 구현 가능성 등을 고려하여 다음 각 호의 조치계획을 수립한다.

1. 단기 : 6개월 이내
2. 중기 : 1년 이내
3. 장기 : 1년~3년 이내

② 제2항에서 중·장기 계획에 대해서는 연 1회 이상 수립하는 정보보호 연간 계획에 반영하여 보호대책이 지속적으로 관리될 수 있도록 한다.

③ 분임보안담당관은 수립된 위험관리 조치계획에 대해 정보보안최고책임자(CISO)의 승인을 받아야 한다.

제4장 응용프로그램 운영

제19조(개발과 운영 환경 분리) ① 홈페이지의 개발 및 시험 시스템을 운영시스템과 분리하여 운영하여야 한다.

② 불가피한 사유로 개발과 운영환경의 분리가 어려운 경우 상호검토, 상급자 모니터링, 변경 승인 및 책임 추적성 확보 등의 보안통제를 수행한다.

제20조(테스트 데이터 관리) ① 응용프로그램을 테스트할 때에는 임의의 테스트 데이터를 생성하여 활용하거나 실제 운영 데이터를 가공하여 사용하도록 하며 실제 운영 데이터의 원본 그대로의 사용을 하여서는 아니된다.

② 테스트 데이터는 테스트 완료 후 삭제하는 것을 원칙으로 한다.

③ 개발담당자는 테스트 데이터를 보호하고 통제하여야 한다.

④ 개발담당자는 응용프로그램 테스트를 목적으로 실제 운영 DB에 접근하여서는 아니된다.

제21조(응용프로그램 이관) ① 개발 관리자는 신규 개발 및 변경이 완료된 응용프로그램의 운영환경 적용을 위하여 이관(배포) 담당자를 지정하여야 한다.

② 개발 담당자는 응용프로그램의 테스트가 완료된 후 운영환경 이관을 위하여 내부 시스템을 이용하여 이관(배포) 내용을 작성하여 이관 담당자에게 운영환경 적용을 요청하여야 한다.

③ 이관(배포) 담당자는 개발 관리자의 승인을 받은 후에 뒤 운영환경에 적용하여야 한다.

④ 이관(배포) 담당자는 응용프로그램의 적용 이전에 기존 운영 환경을 백업하여야 한다.

⑤ 응용프로그램을 적용한 후, 기존의 운영 환경에 미치는 영향을 분석하고 이상이 발생할 경우 즉시 원위치로 복원하여야 한다.

⑥ 응용프로그램을 운영 환경에 적용하는 변경관리는 제23조(정보시스템 변경)와 동일한 절차를 따른다.

제5장 정보시스템 서비스 운영 및 보안관리

제22조(정보시스템 도입 및 설치) ① 보안적합성 검증 대상 외 신규 정보시스템 도입 시 다음 각 호의 내용을 참고하여 도입 타당성 분석 등의 내용이 포함된 도입 계획을 수립 할 수 있다.

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

② 분임보안담당관은 보안장비 및 보안 솔루션 도입 시에는 국가 기관 및 국제기관의 평가인증을 받은 제품을 우선하여 검토할 수 있다.

③ 신규 정보시스템을 운영하기 전에 알려진 보안 취약점을 제거한 후 운영하고 보안 취약점 결과를 분임보안담당관이 취합 관리하여야 한다.

④ 정보시스템의 도입 및 변경으로 네트워크 구성이 변경되는 경우, 네트워크담당자는 변경 사항을 네트워크 구성도에 반영하여 관리하여야 한다.

⑤ 신규 정보시스템 도입이 완료된 경우 각 정보시스템담당자는 정보자산 목록을 갱신하여 관리하여야 한다.

제23조(정보시스템 변경) ① 시스템담당자는 정보시스템 변경 시 발생할 수 있는 위험에 대응하기 위해 변경 전 작업 계획을 수립하여 작업 내역을 기록 관리하여야 한다.

② 정보시스템 운영을 위한 권한 생성 및 변경이 필요한 경우 시스템관리자의 승인하에, 시스템담당자가 발급하는 것으로 하며, 시스템담당자는 권한 부여에 대한 이력을 기록 관리하여 주기적으로 시스템관리자에게 보고하여야 한다.

③ 서버, 네트워크 구성의 변경이 발생되는 경우, 서비스영향도를 고려하여 사전에 관련 담당자 및 부서와 협의를 거쳐 보호 대책을 수립하고, 시스템관리자의 승인을 받은 후에 진행하여야 한다.

④ 데이터베이스 내용의 수정 및 변경이 필요한 경우 다음 각 호의 사항을 준수하여야 한다.

1. 데이터의 정확성을 유지하기 위해서 데이터의 수정, 변경 등은 로깅이 가능한 어플리케이션을 통해서만 수행하고 데이터베이스의 직접적인 접속 및 변경을 제한
2. 데이터의 무결성을 보장하기 위하여, 데이터베이스에 직접 접속(DB Tool)하여 데이터의 추가, 변경 및 삭제는 신뢰할 수 있는 소수의 인가자(데이터베이스담당자)만 수행
3. 데이터베이스 사용자는 개인정보처리시스템의 데이터 테이블 및 파일에 대한 추가, 변경 및 삭제에 대한 작업수행이 필요한 경우 데이터베이스담당자에게 해당 작업을 요청하고 관리자의 승인 후 해당 작업을 수행

⑤ 정보보호시스템 정책이 추가·변경이 발생되는 경우에는 정보시스템 관리자의 승

인을 받아야 하며, 이 경우 변경 내역을 기록 관리하여 주기적으로 정보시스템 관리자에게 보고하여야 한다.

제24조(전자거래 및 핀테크 보안) ① 전자거래 및 핀테크 서비스를 제공하는 경우 거래의 안전성과 신뢰성 확보를 위한 보호대책을 수립·이행하여야 한다.

② 전자거래 및 핀테크 서비스 제공을 위하여 결제시스템 등 외부 시스템과 연계하는 경우 송·수신되는 관련 정보의 보호를 위한 대책을 수립·이행하고 안전성을 점검하여야 한다.

제25조(정보전송 보안) ① 외부 조직에 개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립하여야 한다.

② 업무상 조직 간에 개인정보 및 중요정보를 상호 교환하는 경우 안전한 전송을 위한 협약체결 등 보호대책을 수립·이행하여야 한다.

제26조(패치관리) ① 정보시스템담당자는 보안 취약점을 보완할 수 있는 권고안이나, 패치 정보를 지속적으로 모니터링 하고, 적용 가능성과 시급성 등을 분석하여 필요하다고 판단된 경우 이를 적용하여야 한다.

② 패치작업 수행 시에는 수행내역을 기록하여 관리하여야 한다.

③ 사용자는 PC에 최신 보안패치를 설치하여야 한다. 다만, 자동화된 패치 설치 시스템이 구축되어 있는 경우 이를 통해 설치 할 수 있다.

④ 취약점 개선 패치(patch) 프로그램이나 공개 소프트웨어는 신뢰할 수 있는 사이트나 소프트웨어 제작사 홈페이지로부터 받도록 한다.

⑤ 서비스 팩 등은 현재 사용하고 있는 심사평가원 프로그램들과의 충돌 가능성 및 설치 후 프로그램 사용 환경에 악영향이 있는지 관계부서와 함께 검토한 후 설치하여야 한다.

⑥ 서비스 팩의 설치에는 많은 시간이 소요될 수도 있으므로, 중요하고 급박한 업무가 이루어지지 않는 시간에 실행하여야 한다.

제27조(웜 및 바이러스 예방) ① 심사평가원에서 운영되는 서버에는 바이러스 백신

프로그램을 설치하여 운영해야 한다. 다만, 백신 소프트웨어 license 부족으로 미설치된 서버에는 예산을 확보하여 계획을 수립하여야 한다.

② 정보시스템담당자는 서버에 설치된 바이러스 백신 프로그램을 자동 업데이트하거나, 주기적으로 업데이트 할 수 있도록 한다.

제28조(시간 동기화) ① 시스템담당자는 로그 및 접속기록의 정확성을 보장하고 신뢰성 있는 로그 분석을 위하여 정보시스템의 시간을 표준시간으로 동기화 하여야 한다.

② 시스템담당자는 시간 동기화가 정상적으로 이루어지고 있는지 주기적으로 점검하여야 한다.

부칙<지침 제330호, 2021. 4. 12.>

이 지침은 2021년 4월 12일부터 시행한다.

부칙<지침 제412호, 2023. 12. 18.>

(상임이사·지원·지원장 명칭 변경 등에 따른 계약사무처리지침 등 26개 지침의 일부개정에 관한 지침)

이 지침은 2024년 1월 1일부터 시행한다.