1.3. 관리체계 운영

정보보호 및 개인정보보호 관리체계 운영명세서	
설명	• 정보보호 및 개인정보보호 관리체계 운영명세서는 보호대책 구현 및 운영 현황을 확인할 수 있는 증적자료 중 하나로, 통제항목별 운영현황과 관련 증빙을 구체적으로 작성하여야 한다..
관련 통제항목	**1.3.1 보호대책 구현**
인증기준	**선정한 보호대책은 이행계획에 따라 효과적으로 구현하고, 경영진은 이행결과의 정확성과 효과성 여부를 확인하여야 한다.**

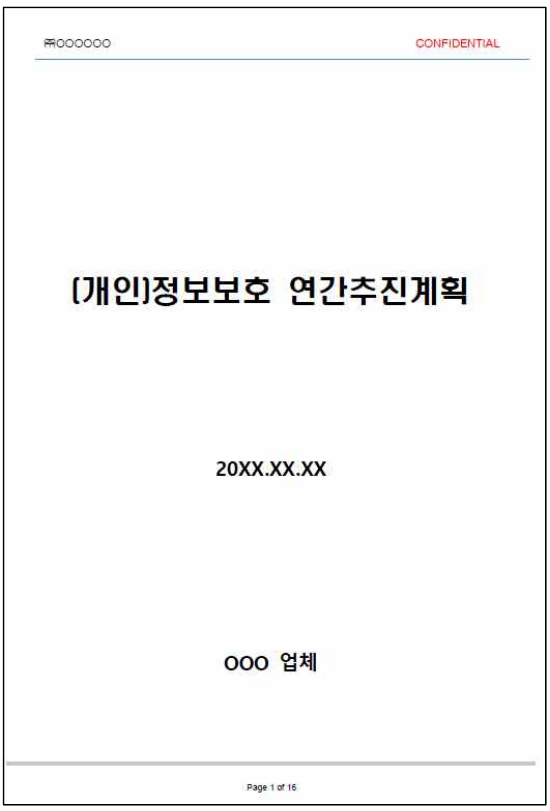
별지. 정보보호 및 개인정보보호 관리체계 운영명세서

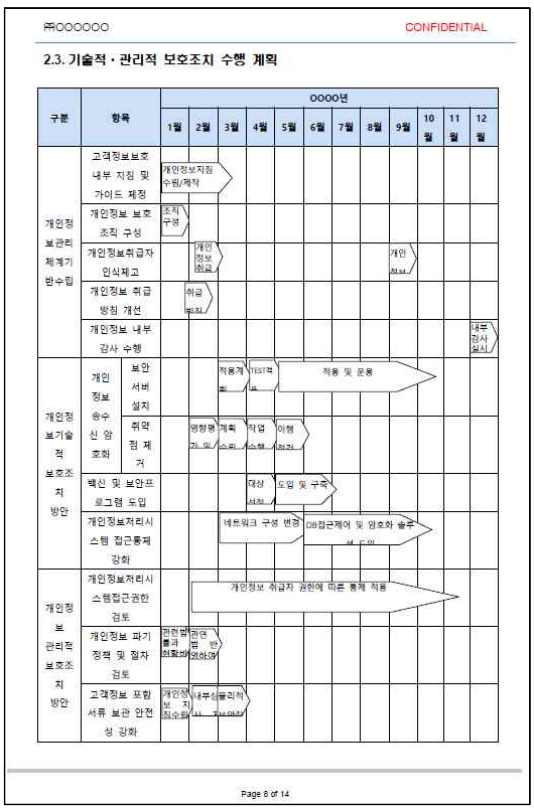
No		통제분야	No	통제항목	통제목적
1. 관리체계 수립 및 운영	1.1	관리체계 기반 마련	1.1.1	경영진의 참여	최고경영자는 정보보호 및 개인정보보호 관리체계의 수립과 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여 운영하여야 한다.
			1.1.2	최고책임자의 지정	최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보보호 업무를 총괄하는 개인정보보호 책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.
			1.1.3	조직 구성	최고경영자는 정보보호와 개인정보보호의 효과적 구현을 위한 실무조직, 조직 전반의 정보보호와 개인정보보호 관련 주요 사항을 검토 및 의결할 수 있는 위원회, 전사적 보호활동을 위한 부서별 정보보호와 개인정보보호 담당자로 구성된 협의체를 구성하여 운영하여야 한다.
			1.1.4	범위 설정	조직의 핵심 서비스와 개인정보 처리 현황 등을 고려하여 관리체계 범위를 설정하고, 관련된 서비스를 비롯하여 개인정보 처리 업무와 조직, 자산, 물리적 위치 등을 문서화하여야 한다.
			1.1.5	정책 수립	정보보호와 개인정보보호 정책 및 시행문서를 수립·작성하며, 이때 조직의 정보보호와 개인정보보호 방침 및 방향을 명확하게 제시하여야 한다. 또한 정책과 시행문서는 경영진 승인을 받고, 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.
			1.1.6	자원 할당	최고경영자는 정보보호와 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고, 관리체계의 효과적 구현과 지속적 운영을 위한 예산 및 자원을 할당하여야 한다.

수립여부	운영현황	관련 문서	보유 증적
Y	o 최고경영자(나최고)는 정보보호 조직 및 정보보호 위원회를 구성하고 책임자로 CISO(최전산 / CIO, CPO겸직)을 임명함 o 정보보호 책임 및 개인정보보호 활동은 CISO가 승인하며 중요 결정사항은 정보보호 위원회를 거쳐 최고경영자의 승인을 득함	정보보호정책서: 제 4조	o (개인)정보보호 조직도 o CISO/CPO 임명장
Y	o 최고경영자(나최고)는 최전산 CIO를 CISO 및 CPO로 임명함 o CISO/CPO는 개인정보보호 및 정보보호 활동 총괄의 책임을 가지며 정보보호 정책서를 통해 역할과 책임을 정의함	정보보호 및 개인정보보호 업무지침: 제 7조	o CISO/CPO 임명장
Y	o 인프라 본부는 (개인)정보보호 조직의 업무를 수행하며, CISO가 임명한 정보보호 관리자, 정보보호 담당자로 구성됨 o 정보보호 위원회는 위원장 CISO/CPO(최전산), 간사 (개인)정보보호 담당자, 각 본부별 본부장으로 구성되어 있음 o 정보보호 위원회는 개인정보보호 및 정보보호 활동 중 중요 사항에 대해 의결하며, 해당 역할을 정보보호정책서로 정의하고 있음 o 정보보호 위원회는 반기 1회 이상 운영하고 있으며, 위원회 결과 회의	정보보호 및 개인정보보호 업무지침: 제 15조	o (개인)정보보호 조직도 o 정보보호 위원회 조직도 o 정보보호 위원회 결과 회의록
Y	o S-Book의 홈페이지를 통한 도서판매 서비스를 관리체계 범위로 정의하고 관련 조직 및 시스템 등을 범위정의를 통해 문서화하고 있음	정보보호 및 개인정보보호 업무지침: 제 3조	o 범위정의서(신청서내 포함)
Y	o 조직이 수행하는 모든 정보보호 활동의 근거를 포함할수 있도록 정보보호정책(1종), 지침(총 4종)을 수립하여 운영하고 있음 o 정보보호정책은 최상위 문서로 최고경영자의 승인을 받아 개정하며, 지침(4종)은 CISO/CPO의 승인을 받아 개정을 실시함 o 정책, 지침은 유관 법률개정, 내부 업무프로세스 변경 등의 사유 발생 시 개정을 실시하며 개정 시 전사 게시판을 통해 공표함	정보보호정책서: 제 6조	o 정책,지침 제개정 승인 이력 o 정책 전사게시판 공표화면
Y	o 인프라 본부는 (개인)정보보호 조직의 업무를 수행하며, CISO가 임명한 정보보호 관리자, 정보보호 담당자로 구성됨 o 정보보호 및 개인정보보호 활동에 필요한 예산을 계획하고 있으며, 최고경영자에 의해 승인을 득함	정보보호 및 개인정보보호 업무지침: 제 15조	o 정보보호 예산 각목명세서

정보보호 및 개인정보 관리계획 내부공유 증적	
설명	• 정보보호 및 개인정보 관리계획 내부공유 증적은 조직이 관리체계 내재화를 위하여 관련 문서의 내부공유 여부를 확인 할 수 있는 증적자료 중 하나로, 정책의 제·개정 사항 등과 같이 구현된 보호대책을 운영 또는 시행할 부서에 관련 내용을 게시판 등에 공유 또는 교육하여야 한다.
관련 통제항목	**1.3.2 보호대책 공유**
인증기준	**보호대책의 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여 지속적으로 운영되도록 하여야 한다.**

정보보호 및 개인정보보호 연간계획서	
설명	• 정보보호 및 개인정보보호 연간계획서는 조직이 주기적 또는 상시적으로 수행하여야 하는 활동을 식별하고, 그 운영현황을 확인하는지 여부를 확인할 수 있는 증적자료 중 하나로, 수행 주기, 시점, 주체 등을 정의하여야 한다.
관련 통제항목	**1.3.3 운영현황 관리**
인증기준	**조직이 수립한 관리체계에 따라 상시적 또는 주기적으로 수행하여야 하는 운영활동 및 수행 내역은 식별 및 추적이 가능하도록 기록하여 관리하고, 경영진은 주기적으로 운영활동의 효과성을 확인하여 관리하여야 한다.**





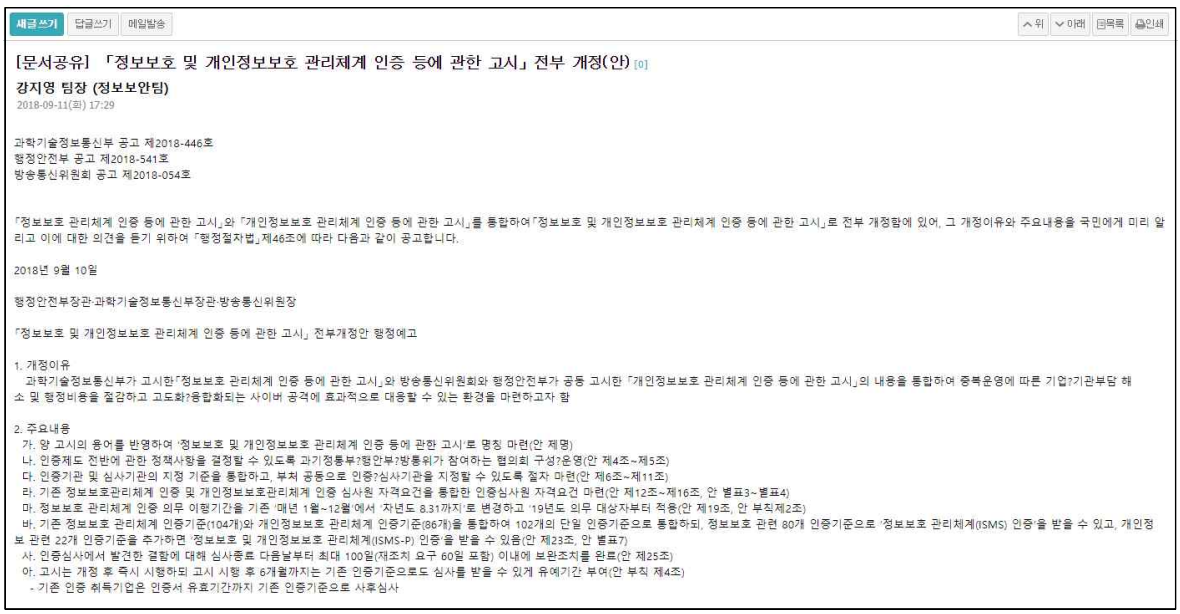
1.4. 관리체계 점검 및 개선

정책/지침 신구대조표	
설명	• 정책/지침 신구대조표는 정책의 주기적 검토 여부를 확인할 수 있는 증적자료 중 하나로, 개정부분 및 사유를 확인할 수 있어야 한다.
관련 통제항목	1.4.1 법적 요구사항 준수 검토
인증기준	조직이 준수하여야 할 정보보호 및 개인정보보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토하여야 한다.

<OOO 업체 정책·지침 신구대조표>

구분	종전	수정 후	개정사유
정보보호 및 개인정보보호 업무지침	**제 22조 보안사고 예방 활동** ① 정보보호 담당자는 보안사고 발생 가능성을 사전에 점검하고 보안사고를 감지할 수 있는 대책을 마련하여야 한다. ② 정보보호 담당자는 보안사고 관련 정보를 사내 게시판 등을 이용하여 임직원들에게 공지하여야 한다 ③ 정보보호 관리자는 보안사고 발생 시 신속한 대응을 위하여 절차를 마련하여야 한다.	**제 93조 보안사고 예방 활동** ① 정보보호 담당자는 보안사고 발생 가능성을 사전에 점검하고 보안사고를 감지할 수 있는 대책을 마련하여야 한다. ② 정보보호 담당자는 보안사고 관련 정보를 사내 게시판 등을 이용하여 임직원들에게 공지하여야 한다 ③ 정보보호 관리자는 보안사고 발생 시 신속한 대응을 위하여 절차를 마련하여야 한다. ④ ***임직원 및 관련 외부인력은 정보시스템에서 보안 취약점이 발견되거나 의심될 시 기록 및 정보보호 담당자에게 보고하여야 한다.***	시스템의 취약점 발견 시 보고절차 수립
	제 23조 보안사고 대응관리 ① 보안사고 발생시 선 보고 후 조치를 원칙으로 한다. 다만, 긴급 상황일 경우에는 선 조치 후 보고할 수 있다. ② 모든 이상 징후에 대해서는 분석을 실시한다. 정보보호 관리자는 이를 총괄한다. ③ 보안사고 발생이 의심되거나 실제 사고가 발생했을 경우, 법적 증거 확보를 위하여 시스템에 대한 보안 공격 시도나 침해 사실을 판단할 수 있는 로그, 보안사고 발생 흔적 및 파일이나 기타 정보 등을 수집하여 보관한다. ④ 모든 보안사고 관련 분석, 조치, 보고에 대한 사항은 "별첨 #5. 보안사고 대응 보고서"에 작성한다.	**제 94조 보안사고 대응관리** ① 보안사고 발생시 선 보고 후 조치를 원칙으로 한다. 다만, 긴급 상황일 경우에는 선 조치 후 보고할 수 있다. ② ***모든 이상 징후에 대해서는 분석을 실시하여 보안사고를 식별하여야 한다.*** 정보보호 관리자는 이를 총괄한다. ③ 보안사고 발생이 의심되거나 실제 사고가 발생했을 경우, 법적 증거 확보를 위하여 시스템에 대한 보안 공격 시도나 침해 사실을 판단할 수 있는 로그, 보안사고 발생 흔적 및 파일이나 기타 정보 등을 수집하여 보관한다. ④ 모든 보안사고 관련 분석, 조치, 보고에 대한 사항은 "별첨 #5. 보안사고 대응 보고서"에 작성한다.	문구 수정

법 개정사항 내부공유 자료	
설명	• 법 개정사항 내부공유 자료는 조직은 관련 법규의 제·개정 현황을 지속적으로 모니터링 하는지 여부를 확인할 수 있는 증적자료 중 하나로, 법 개정이 이루어질 경우 관리체계를 운영하는 부서에 관련 제·개정 사항을 게시판 등에 공유하여야 한다.
관련 통제항목	**1.4.1 법적 요구사항 준수 검토**
인증기준	**조직이 준수하여야 할 정보보호 및 개인정보보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토하여야 한다.**



새글쓰기 답글쓰기 메일발송 위 아래 목록 인쇄

[문서공유] 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 전부 개정(안) [0]

강지영 팀장 (정보보안팀)

2018-09-11(화) 17:29

과학기술정보통신부 공고 제2018-446호
행정안전부 공고 제2018-541호
방송통신위원회 공고 제2018-054호

「정보보호 관리체계 인증 등에 관한 고시」와 「개인정보보호 관리체계 인증 등에 관한 고시」를 통합하여 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」로 전부 개정함에 있어, 그 개정이유와 주요내용을 국민에게 미리 알리고 이에 대한 의견을 듣기 위하여 「행정절차법」 제46조에 따라 다음과 같이 공고합니다.

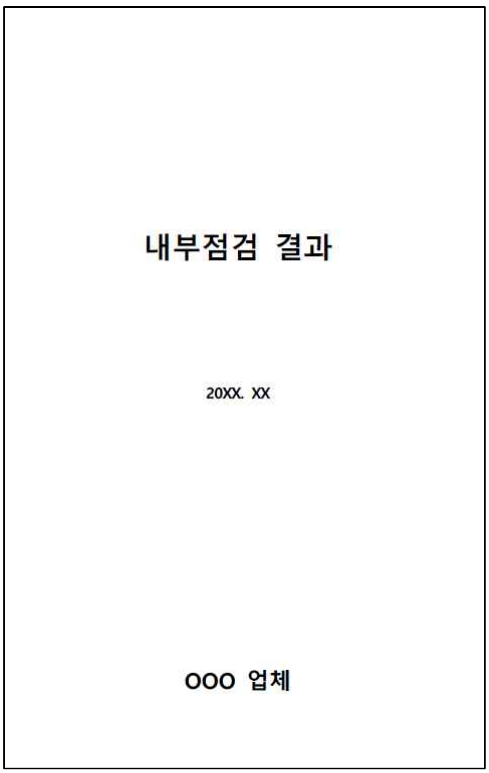
2018년 9월 10일

행정안전부장관·과학기술정보통신부장관·방송통신위원장

「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 전부개정안 행정예고

1. 개정이유
과학기술정보통신부가 고시한「정보보호 관리체계 인증 등에 관한 고시」와 방송통신위원회와 행정안전부가 공동 고시한 「개인정보보호 관리체계 인증 등에 관한 고시」의 내용을 통합하여 중복운영에 따른 기업?기관부담 해소 및 행정비용을 절감하고 고도화?융합화되는 사이버 공격에 효과적으로 대응할 수 있는 환경을 마련하고자 함

2. 주요내용
가. 양 고시의 용어를 반영하여 '정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시'로 명칭 마련(안 제명)
나. 인증제도 전반에 관한 정책사항을 결정할 수 있도록 과기정통부?행안부?방통위가 참여하는 협의회 구성?운영(안 제4조~제5조)
다. 인증기관 및 심사기관의 지정 기준을 통합하고, 부처 공동으로 인증?심사기관을 지정할 수 있도록 절차 마련(안 제6조~제11조)
라. 기존 정보보호관리체계 인증 및 개인정보보호관리체계 인증 심사원 자격요건을 통합한 인증심사원 자격요건 마련(안 제12조~제16조, 안 별표3~별표4)
마. 정보보호 관리체계 인증 의무 이행기간을 기존 '매년 1월~12월'에서 '차년도 8.31까지'로 변경하고 '19년도 의무 대상자부터 적용(안 제19조, 안 부칙제2조)
바. 기존 정보보호 관리체계 인증기준(104개)와 개인정보보호 관리체계 인증기준(86개)을 통합하여 102개의 단일 인증기준으로 통합하되, 정보보호 관련 80개 인증기준으로 '정보보호 관리체계(ISMS) 인증'을 받을 수 있고, 개인정보 관련 22개 인증기준을 추가하면 '정보보호 및 개인정보보호 관리체계(ISMS-P) 인증'을 받을 수 있음(안 제23조, 안 별표7)
사. 인증심사에서 발견한 결함에 대해 심사종료 다음날부터 최대 100일(재조치 요구 60일 포함) 이내에 보완조치를 완료(안 제25조)
아. 고시는 개정 후 즉시 시행하되 고시 시행 후 6개월까지는 기존 인증기준으로도 심사를 받을 수 있게 유예기간 부여(안 부칙 제4조)
- 기존 인증 취득기업은 인증서 유효기간까지 기존 인증기준으로 사후심사

<table>
<tr><th colspan="2">내부점검 보고서</th></tr>
<tr><td>설명</td><td>• 내부점검 보고서는 조직이 관리체계 점검을 수행하는지 여부를 확인할 수 있는 증적자료 중 하나로, 내부점검 결과 및 개선방안 제시여부를 확인할 수 있어야 한다.</td></tr>
<tr><td>관련 통제항목</td><td>1.4.3 관리체계 개선</td></tr>
<tr><td>인증기준</td><td>법적 요구사항 준수검토 및 관리체계 점검을 통해 식별된 관리체계상의 문제점에 대한 원인을 분석하고 재발방지 대책을 수립·이행하여야 하며, 경영진은 개선 결과의 정확성과 효과성 여부를 확인하여야 한다.</td></tr>
<tr><td colspan="2">

내부점검 결과

20XX. XX

OOO 업체


1. 내부점검 결과
□ 점검 결과 백분율 환산
◦ Y(Yes) 완료 : 17건 (63 점)
◦ P(Partial) 부분 완료 : 10건 (18.5 점)
◦ N(No) 미완료 : 0건
◦ N/A 해당 없음 : 0건
- 합계 : 81.5점

□ 부분완료 및 미완료 상세내용
<table>
<tr><th>분야</th><th colspan="2">주요 문제점</th><th>점검결과</th><th>비고</th></tr>
<tr><td>정보보호 정책</td><td>1</td><td>매뉴얼 내 수행 주기 누락</td><td>P</td><td>매뉴얼 업데이트 예정</td></tr>
<tr><td rowspan="3">정보보호 책임</td><td>2</td><td>이행 증적 미존재</td><td>P</td><td>이행 증적 작성 예정</td></tr>
<tr><td>3</td><td>이행 증적 미존재</td><td>P</td><td>이행 증적 작성 예정</td></tr>
<tr><td>4</td><td>매뉴얼 내 수행 주기 누락</td><td>P</td><td>매뉴얼 업데이트 예정</td></tr>
<tr><td>자산 관리</td><td>8</td><td>매뉴얼 내용 정합성 미흡</td><td>P</td><td>매뉴얼 업데이트 예정</td></tr>
<tr><td rowspan="3">시스템 운영</td><td>20</td><td>매뉴얼 내 법률 요구사항 누락</td><td>P</td><td>매뉴얼 업데이트 예정</td></tr>
<tr><td>22</td><td>매뉴얼 내 수행 주체 누락</td><td>P</td><td>매뉴얼 업데이트 예정</td></tr>
<tr><td>23</td><td>이행 증적 미존재</td><td>P</td><td>이행 증적 작성 예정</td></tr>
<tr><td rowspan="2">사무환경 보안</td><td>24</td><td>매뉴얼 내 승인 주체 누락</td><td>P</td><td>매뉴얼 업데이트 예정</td></tr>
<tr><td>27</td><td>이행 증적 미존재</td><td>P</td><td>이행 증적 작성 예정</td></tr>
</table>
</td></tr>
</table>