

전자서명인증관리업무보안관리지침

제정 2009. 12. 31.

개정 2013. 9. 1.

개정 2014. 1. 24.

개정 2021. 8. 24.

제1장 총 칙

제1조(목적) 이 지침은 한국인터넷진흥원(이하 “인터넷진흥원”이라 한다)의 전자서명인증관리센터의 보안관리에 필요한 사항을 정함을 목적으로 한다.

제2조(적용범위) 전자서명인증관리센터의 보안관리는 이 지침에 의하여 처리한다.

제3조(용어의 정의) ① 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. “전자서명인증관리센터”(이하 “인증관리센터”라 한다)라 함은 전자서명법 부칙 제5조(공인인증업무 등에 관한 경과조치)에 따라, 종전의 전자서명법 제25조에 의하여 전자서명인증관리업무를 담당하고 이에 필요한 기반시설을 운영·관리하는 부서를 말한다. <개정 2021. 8. 24.>
 2. “인증시스템”이라 함은 가입자의 등록정보 관리, 전자서명키 생성·관리, 공인인증서 생성·발급·관리, 시점확인 기능 등을 지원하는 시스템들을 말한다.
- ② 이 지침에서 사용하는 용어의 정의는 제1항에서 정하는 것을 제외하고는 전자서명법이 정하는바에 의한다.

제4조(인증관리센터장) ① 인증관리센터장은 인증관리센터의 보안관리에 관한 계획, 조정, 감독 및 통제에 관한 사항을 결정하여야 한다.

② 인증관리센터장은 인증관리업무를 원활한 수행을 위하여 각 업무별로 관리자를 지정하여 운영하여야 한다.

③ 인증관리센터장은 인증관리업무를 보안에 대한 책임을 지닌다.

제5조(보안관리자) ① 보안관리자는 인증관리센터장이 임명하는 인증관리센터의 직원으로 하여야 한다.

② 보안관리자는 효율적인 보안업무를 위하여 다음 각 호의 사항을 수행하여야 한다.

1. 인증관리센터 직원에 대한 보안교육
2. 인증관리센터의 각종 보안사고 예방 및 조치
3. 비밀문서의 관리
4. 업무수행 상 보안을 요하는 사항의 협조
5. 기타 소관센터의 보안에 관한 사항
6. 인증관리센터 보안경비요원의 근무관리

제6조(비밀유지의무) ① 인증관리센터의 직원은 인증관리업무 수행과정에서 알게 된 비밀 사항을 외부에 유출하거나 공개하여서는 아니 된다.

② 인증관리센터의 직원은 인증서 발급 등과 관련하여 공인인증기관이 제출한 신청서 및 제출 서류 등을 안전하게 보관·관리하여 외부에 유출 되지 않도록 하여야 한다.

③ 인증관리센터에 출입하는 외부용역업체에 대하여 용역업무 수행과정에서 알게 된 비밀사항을 외부에 유출하거나 공개하지 않도록 별지 제1호(보안준수 서약서) 서식을 작성하도록 하여야 한다.

제2장 자산 분류 및 운영

제7조(자산 분류) ① 인증관리센터의 자산은 자산의 성질의 따라 시스템자산, 소프트웨어자산, 정보자산, 문서자산 및 설비자산으로 구분한다.

② 시스템자산이라 함은 하드웨어, 네트워크 장비, 백업 장치 및 프린터 등의 시스템을 말한다.

③ 소프트웨어자산이라 함은 소스코드, 운영체제 및 응용프로그램 등의 소프트웨어를 말한다.

④ 정보자산이라 함은 전자서명키, 데이터베이스, 감사기록 및 백업기록 등의 정보를 말한다.

⑤ 문서자산이라 함은 업무지침서, 운영지침서, 문서관리대장, 백업관리대장, 보고서, 공문 및 실질심사 관련자료 등의 문서를 말한다.

⑥ 설비자산이라 함은 항온항습기, 방법장치, 출입통제설비 및 무정전전원공급장치 등의 설비를 말한다.

제8조(자산 관리) ① 제7조제1항에서 분류된 사항에 대해서는 다음과 같이 관리하여야 한다.

1. 자산목록은 계량적 수치로 관리번호를 부여하여 기록
2. 자산의 반출입, 신규도입 및 폐기 등 변동사항이 발생할 경우 사전에 인증관리센터장 또는 보안관리자에게 승인을 받고 변경사항을 기록

② 시스템 및 소프트웨어자산은 시스템관리자가 관리한다.

③ 정보, 문서 및 설비자산은 보안관리자가 관리하며, 정보자산의 경우 잠금장치가 있는 안전한 장소에 보관한다.

④ 자산별 세부 담당자는 인증관리센터장이 별도로 정한다.

제9조(문서처리 및 운영절차) ① 인증관리업무와 관련된 문서처리 절차는 전자서명인증관리업무 규칙을 준수하여야 한다.

② 인증시스템에 대한 운영절차는 해당 업무지침서를 준수하여야 한다. 해당 업무지침서는 다음 각호와 같다.

1. 신청서수발업무지침서
2. 인증서 등록·발급 및 키생성업무 지침서
3. 웹공고업무지침서
4. 감사기록백업업무지침서

③ 제2항 이외의 인증관리업무와 관련된 시스템의 운영은 해당 운영지침서를 준수하여야 한다. 해당 운영지침서는 다음 각호와 같다.

1. 라우터운영지침서
2. 침입차단시스템운영지침서
3. L4 스위치운영지침서
4. 네임서버운영지침서
5. 네트워크관리시스템운영지침서
6. 로그서버운영지침서
7. 메일서버운영지침서
8. 서버관리시스템운영지침서
9. 침입탐지시스템운영지침서
10. 기타 운영지침서

④ 제2항의 업무지침서 및 제3항의 운영지침서는 해당 시스템 운영담당자만이 접근할 수 있도록 하여야 한다.

제10조(문제보고) ① 인증관리센터의 직원은 업무와 관련하여 네트워크를 통한 시스템의 침입 및 기타 시스템의 안전성에 관하여 의심이 갈 경우 즉시 인증관리센터장 또는 보안관리자에게 보고하여야 한다.

② 인증관리센터장 또는 보안관리자는 관련 기록을 검토하여 안전성에 문제가 있을 경우 이를 부서장에게 보고하고 적절한 조치를 취하여야 한다.

제3장 물리적·환경적 보안관리

제11조(제한구역 및 통제구역) ① 인증관리센터는 제한구역, 통제구역 및 사무공간으로 구분한다.

- ② 중앙통제실, 공조실, 인증S/W평가실은 제한구역으로 정한다.
- ③ 무게감자기가 설치된 구역 이후의 공간을 통제구역으로 정한다.
- ④ 제2항 및 제3항을 제외한 공간은 사무공간으로 정한다.

제12조(보호조치) 인증관리센터의 일반적인 물리적, 환경적 보호조치는 공인인증기관의보호 조치에관한규정을 준용하여야 한다.

제13조(출입인가) ① 제한구역 및 통제구역의 출입은 인증관리센터장이 승인하는 인증관리 센터의 직원으로 제한하여야 한다.

- ② 제1항에서 정한 자 이외의 업무상 인증관리센터의 제한구역 및 통제구역에 출입할 필요가 있는 자는 인증관리센터장의 사전 승인을 얻은 후에 제1항에서 인가된 직원의 안내를 받아 출입하고 별지 제2호(출입대장)서식에 해당 사항을 기록하여야 하고, 작업을 수행할 경우에는 별지 제3호(작업계획및결과서)서식도 기록하여야 한다.

제14조(보안경비요원) ① 인증관리센터는 보안경비요원을 24시간 배치하여 출입을 통제하여야 한다.

- ② 보안경비요원이 통제구역 내의 상황을 CCTV 카메라로 감시하고 이상이 있을 시에는 비상 연락 등 필요한 조치를 취하여야 한다.

제4장 네트워크 · 시스템 보안관리

제15조(네트워크 보안) ① 인증관리센터는 인증관리업무를 제공하기 위하여 운영하고 있는 네트워크에 대해, 공인인증기관의시설및장비등에관한규정(운영기준 별표)을 충족하는 네트워크보안기능을 갖추고 안전하게 운영하여야 한다.

- ② 시점확인시스템을 제외한 인증시스템은 내·외부의 정보통신망과 분리하여 독립적으로 운영한다.

제16조(시스템 보안) ① 인증관리센터는 인증관리업무를 제공하기 위하여 운영하고 있는 시스템에 대해 공인인증기관의시설및장비등에관한규정을 충족하는 시스템보안기능을 갖추고 안전하게 운영하여야 한다.

- ② 보안관리자는 시스템 사용자의 권한이 정당한지에 대하여 주기적으로 검토하고 필요한 조치를 취하여야 한다.

제17조(비밀번호 관리) ① 비밀번호는 해당 업무의 담당자만이 알고 있어야 하며, 분기별 1회

또는 필요시마다 변경하여야 한다.

② 비밀번호는 해당 업무의 담당자가 기록하여 보안금고에 안전하게 관리하여야 한다.

③ 비밀번호를 업무상 사용할 필요가 있을 때는 보안관리자의 사전 승인을 얻은 후 별지 제4호 (비밀번호이용대장) 서식에 기록한 후 사용하여야 한다.

④ 비밀번호는 다음 각호에 해당하는 사항을 충족하여야 한다.

1. 숫자와 문자 등을 혼합하여 8자리 이상을 부여할 것
2. 사용자계정과 동일하지 않을 것
3. 일반사전에 등록된 단어의 사용을 피할 것
4. 조직 관련명칭, 연속된 숫자 또는 문자 등의 사용을 피할 것
5. 수첩, 노트에 기록하는 등 문서화 금지
6. 플로피디스크, 공유 디렉토리 등의 저장매체에 보관 금지
7. 통신매체 또는 온라인매체를 통한 공개 금지

제5장 재해복구 관리

제18조(취약점 분석·평가) 인증관리센터는 정기적으로 인증시스템의 취약점을 점검하여야 한다.

제19조(비상대책) ① 인증관리센터는 각종 재난 및 재해로부터 인증관리업무의 연속성을 보장하기 위하여 비상대책을 수립하고 이를 시행하여야 한다.

② 비상대책은 다음 각호의 내용을 포함하여야 한다.

1. 인증시스템 및 네트워크의 복구절차
2. 복구절차의 검증, 보수 및 재평가
3. 보안사고의 보고 및 처리절차

제20조(백업사이트 운영) 인증관리센터는 인증관리업무의 지속성, 안전성 및 신뢰성을 보장하기 위하여 백업사이트를 운영할 수 있다.

제21조(백업) ① 인증관리센터는 주요 자료를 주기적으로 백업하여야 한다.

② 인증관리센터는 안전한 백업을 위하여 백업지침서를 작성하고 준수하여야 한다.

③ 백업지침서는 백업의 대상 및 절차를 포함하여야 한다.

④ 백업한 자료는 월1회 인증관리센터 및 백업사이트에 보관하여야 한다.

제22조(비상연락체계) 인증관리센터는 각종 재난 및 재해로부터 신속한 대응조치를 취할 수 있

도록 관련기관을 포함하는 비상연락체계를 갖추고 이를 유지하여야 한다.

제6장 기타

제23조(보조기억매체 취급과 보안) ① 인증관리센터의 직원은 인증관리업무 수행 시에 보안 관리자가 승인한 보조기억매체만을 사용하여야 한다.

② 제1항에서 사용된 보조기억매체는 안전한 장소에 보관하여야 한다.

③ 전자서명생성정보 등이 저장된 보조기억매체는 관리번호를 부여하고 별도의 대장을 두어 관리하여야 한다.

④ 제1항에서 사용된 보조기억매체를 폐기하는 경우 보안관리자의 입회하에 재사용이 불가능하도록 안전하게 폐기하여야 한다.

제24조(일일보안점검) 일일보안점검은 인증관리센터의 보안 상태를 점검하고 별지 제5호(전자서명인증관리센터보안당직점검일지)서식에 기록하여 인증관리센터 관리자 및 센터장에게 관리·감독 받아야 한다. <개정 2021. 8. 24.>

제25조(감사) 감사관리자는 인증관리센터의 인증관리업무 수행 중 발생하는 다음 각 호에 대한 정기적인 감사를 실시하여야 한다.

1. 인증관련 시스템 로그기록
2. 네트워크 로그기록
3. 출입자 로그기록
4. 보안 및 안전교육 실시현황

제26조(교육) 인증관리센터의 직원은 인증관리업무의 원활한 수행을 위하여 다음 각 호에 대한 적절한 교육을 받아야 한다.

1. 인증관련 시스템 사용방법
2. 비상대응절차

제27조(신규 시스템 도입 및 기존 시스템 변경) 인증관리센터의 직원은 신규 시스템을 도입하거나 기존의 소프트웨어와 프로그램을 변경하는 경우 작업계획서를 작성하여 인증관리센터장의 승인을 받아야 한다. 또한, 이를 개발환경에서 검증테스트 결과를 확인 완료 후에 운영환경으로 적용하여야 한다.<신설 2014.1.24>

부 칙

이 지침은 원장의 승인을 받은 날로부터 시행한다.

부 칙<2013. 9. 1>

이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

부 칙<2014. 1. 24>

이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

부 칙<2021. 8. 24.>

이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

보안서약서

본인은 한국인터넷진흥원(이하 “진흥원”)에서 용역을 수행함에 있어 다음사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 “진흥원”에서 “용역” 수행중 취득한 제반 비밀사항을 업무 수행중은 물론 복귀 후에도 일체 누설하지 않을 것을 서약합니다.
2. 본인은 “진흥원”의 기밀을 누설하였을 때는 동기여하를 막론하고 그 결과에 대한 제반 법규에 의거하여 엄중한 처벌을 받을 것을 서약 합니다.
3. 본인은 업무상 고의 또는 중대 과실로 인해 “진흥원”에 재산상 손해를 끼쳤을 경우에 그에 대한 형사 및 민사상 책임을 집니다.

년 월 일

업 체 명 :

직 위 :

성 명 : (인)

[별지 제2호 서식] <개정 2021. 8. 24.>

출입 통제 대장

[illegible]

작업계획 및 결과서

작업자 성명		소 속		연락처 (전화번호)	
		직 위			

<작업 예정사항>

1. 의뢰일시: 20 년 월 일 시 분
2. 의뢰내용:

<조치사항>

1. 작업일시: 20 년 월 일 시 분 ~ 20 년 월 일 시 분
2. 작업내용:

처리일자 : 20 년 월 일

작 업 자 : (인)

담 당 자 : (인)

조 치 결 과	담당확인	팀장확인	단장확인	특 기 사 항
		전결		

한국인터넷진흥원

[별지 제4호 서식]

비밀번호 이용대장

[illegible]

전자서명인증관리센터 보안당직 점검일지

20 년 월 일 요일 :00 ~ 익일 :00

반 장	관리자	센터장

당직자 : (인)

1. 인증관리센터 보안당직 점검사항

구 분	업무내용 (상황보고)	특이사항
메인센터 주출입구		
메인센터 4층 복도		
나주 백업센터		

2. 총기 관리현황

제품 번호	반출				반납			
	시간	수령자	서명	확인자	시간	반납자	서명	확인자

3. 기타 특이사항

--