전산정보 업무 관리 규칙

제정 2009. 07. 13. 규칙 제19호
개정 2018. 10. 10. 규칙 제106호
개정 2019. 03. 14. 규칙 제109호
개정 2019. 06. 28. 규칙 제116호
개정 2020. 09. 04. 규칙 제139호
개정 2025. 03. 07. 규칙 제191호

제1장 총 칙

제1조(목적) 이 규칙은 재단법인 한국만화영상진흥원(이하 “진흥원”이라 한다)의 전산정보 업무 관리를 위한 종합적인 체계를 마련하고, 정보시스템 운용의 안정성 및 신뢰성을 보장할 수 있는 체계적인 업무절차 및 방법의 확립을 목적으로 한다.

제2조(관리책임) ① 이 규칙을 시행하기 위한 전산정보 업무 관리 책임자는 다음과 같다.

1. 정책임자 : 진흥원의 정보화 업무 담당 부서장(이하 “정보화책임자”이라 한다.
2. 부책임자 : 진흥원의 정보화 업무 담당(이하 “정보화담당”이라 한다)

② 정보화책임자 및 정보화담당은 진흥원 업무분장에 의하여 발령된 것으로 한다.

제3조(업무) 정보화책임자 및 정보화담당의 업무는 다음과 같이 구분한다.

1. 진흥원의 정보화 추진 및 장단기 계획 수립
2. 정보시스템실 운영 및 관리, 통제, 보안 업무
3. 정보시스템실 관리 상태점검 및 관련설비의 유지보수 업무 관리감독
4. 정보시스템 및 전산장비, 설비의 운영상태 수시 진단, 장애 조치 및 최적상태 유지
5. 정보시스템 및 전산장비, 설비 유지보수 및 유지보수 업체 관리
6. 소프트웨어 관리 업무 총괄

제4조(용어) 본 규칙에서 사용되는 용어의 정의는 다음과 같다.

1. “정보시스템실”이란 웹서버, 데이터베이스서버, NMS(Network Management System)서버, TCO(Total Cost of Ownership)서버, 백본스위치, 방화벽, 전자교환기(IP-PBX) 등 진흥원이 보유하고 있는 전산장비를 관리·운영하는 공간을 말한다.
2. “출입통제장치”란 정보시스템실에 대해 허가되지 않은 자의 출입을 제한하고 허가된 자만이 출입할 수 있도록 설치된 개폐장치를 말한다.

3. “인가자”란 진흥원에 소속된 근무자로서 정보시스템실 운영을 담당하는 자 또는 정보화책임자가 승인한 자를 말한다.
4. “비인가자”란 인가자 이외의 자로 정보화 업무와 관련하여 정보시스템실의 출입이 필요하다고 정보화책임자가 승인한 자를 말한다.
5. “출입기록”이란 정보시스템실에 출입하는 모든 출입자에 대해 인적사항과 출입목적 및 출입일자 등을 출입관리대장에 기록하여 관리하거나 CCTV 및 출입통제장치를 사용하여 출입자의 출입기록을 관리하는 행위를 말한다.
6. “출입통제장치”란 생체나 카드 정보를 이용하여 정보시스템실 출입허용 여부를 판단하고 출입이력을 기록하는 장비를 말하며 지문감지기, 카드리더기 등이 있다.
7. “보안 경보장치”란 보안 감지장치로 위험요소가 감지되는 경우, 이를 근무자가 인지할 수 있도록 소리나 빛으로 알려 주는 장치를 말한다.
8. “전산기계실”이란 정보시스템실 내에 서버, 스위치 등 정보시스템이 정상적으로 운영될 수 있도록 전력 및 공조시설, 네트워크 설비 등이 갖추어진 장소를 말한다.
9. “상황실”이란 정보시스템실 내의 전기, 보안, 소방 등 주요 시설물의 가동상황을 감시하고 장애 발생시 조치를 수행하는 역할을 담당하는 장소를 말한다.
10. “분전반”이란 전기를 분기하여 정보시스템실 내의 각각의 장비에 공급하는 시설을 말한다.
11. “케이블 트레이(Cable Tray)”란 케이블이 지나가는 통로로써 케이블을 지지하고 보호하는 역할을 한다.
12. “항온항습기”란 정보시스템실 내부의 일정 온도와 습도를 유지하는 시설을 말한다.
13. “누수감지기”란 정보시스템실 내에 결로나 배관의 문제로 누수가 발생할 경우 감지하고 경보해 주는 시설을 말한다.
14. “이중마루(Access Floor)”란 공조와 각종 케이블, 전기, 통신, 데이터의 관리를 용이하게 하기 위하여 바닥을 이중화 하는 것을 말한다.
15. “바이러스”란 컴퓨터 프로그램이나 실행 가능한 부분을 변형하여, 여기에 자기 자신 또는 자신의 변형을 복사하여 컴퓨터 작동에 피해를 주는 악성코드를 말한다.
16. “백신 프로그램”이란 바이러스를 찾아 기능을 정지시키거나 제거하는 프로그램을 말한다.
17. “IP 주소”란 인터넷규약주소로 컴퓨터 네트워크에서 장치들이 서로를 인식하고 통신을 하기 위해서 사용하는 특수한 번호를 말한다.
18. “방화벽”이란 서로 다른 네트워크를 지나는 데이터를 허용하거나 거부하거나 검열, 수정하는 하드웨어나 소프트웨어 장치를 말한다.
19. “IDS(Intrusion Detection System)”란 네트워크 트래픽을 감시하여 서비스 거부 공격(DoS 공격), 포트 스캔, 컴퓨터를 크랙하려는 시도 등과 같은 악의적인 동작들을 탐지하는 시스템을 말한다.

20. “웹 취약점 점검도구”란 SQL Injection, Cross Site Scripting, 암호취약점 등 웹 애플리케이션의 허점을 탐지하는 점검 도구를 말한다.
21. “소프트웨어(S/W)”란 컴퓨터·통신·자동화 등의 장비와 그 주변장치에 대하여 명령·제어·입력·처리·저장·출력·상호 작용이 가능하도록 하게 하는 지시·명령(음성이나 영상정보 등을 포함한다)의 집합과 이를 작성하기 위하여 사용된 기술서 및 기타 관련 자료를 말한다.
22. “불법복제”란 컴퓨터프로그램보호법에 의하여 저작권자에게 부여된 권리를 침해하는 행위를 말한다.
23. “소프트웨어 관련문서”란 정보화담당이 소프트웨어 보유 및 사용 현황 등에 관한 사항을 기재하는 각종 문서들을 말한다.
24. “휴대용 저장매체”란 디스켓, CD, 외장형 하드디스크, USB메모리, 메모리카드, 스마트폰 등 정보를 저장할 수 있는 것으로 PC 등의 정보시스템과 분리할 수 있는 기억장치를 말한다. <신설 2018. 10. 10.>
25. “저장장치(기억장치)”란 주기억장치(하드디스크), 보조기억장치(ROM, RAM), 휴대용 저장매체 등 정보를 일시적으로, 또는 영구히 보존하는 비휘발성의 장치를 말한다. <신설 2018. 10. 10.>
26. “출력장치”란 모니터, 프린터, 프로젝터, 스피커 등을 이용하여 사람이 읽고 들을 수 있는 빛, 소리, 인쇄등의 방식으로 컴퓨터의 결과물을 출력하는 장치를 말한다. <신설 2018. 10. 10.>
27. “입력장치”란 키보드, 마우스, 터치패드 등을 이용하여 사용자가 원하는 문자, 기호, 그림 등의 데이터를 컴퓨터 내부의 메모리에 전달하는 장치를 말한다. <신설 2018. 10. 10.>
28. “백도어”란 인증되지 않은 사용자에 의해 컴퓨터의 기능이 무단으로 사용될 수 있도록 컴퓨터에 몰래 설치된 통신 연결 기능을 말한다. <신설 2018. 10. 10.>
29. “가상사설망(VPN)”이란 인터넷망과 같은 공중망을 사설망처럼 이용해 멀리 떨어진 지역의 PC를 같은 네트워크망으로 사용하는 통신 연결 기능을 말한다. <신설 2018. 10. 10.>
30. “정보시스템”이란 정보를 수집, 처리, 저장, 전송, 전시, 전파, 적용 및 제공하는 전반적인 기술의 집합체를 말한다. <신설 2018. 10. 10.>

제2장 정보시스템실 운영

제5조(출입통제장치) ① 정보시스템실은 물리적 보안을 위하여 출입통제장치 및 보안 경보장치를 설치·운영한다.
② 출입통제장치와 보안 경보장치는 정보화담당이 관리·운영한다.

제6조(출입자 관리) ① 정보시스템실의 출입관리는 정보화담당이 담당한다.
② 정보시스템실 출입은 인가자를 원칙으로 한다. 다만 비인가자는 정보화담당의

허가를 득한 후 출입토록 한다.

제7조(비인가자의 출입절차) ① 비인가자가 정보시스템실에 출입하고자 할 경우에는 사전에 정보시스템실 출입 관리대장 “별지 제1호 서식”에 기록하고 정보화담당에게 제출하여 승인을 득하여야 한다.

② 정보시스템실에 출입하는 비인가자는 관계 직원과 동행하여 작업을 수행하여야 하며 작업이 종료되는 즉시 작업 처리 결과를 작성하여 제출하여야 한다.

제8조(반출입관리) ① 정보시스템실에 반입되거나 정보시스템실로부터 반출되는 모든 장비와 물품에 대하여 정보화 기자재 통합물품출납대장 “별지 제18호 서식”에 기록하고 정보화담당에게 제출하여 승인을 득하여야 한다. <개정 2025. 03. 07.>

② 정보시스템실 반출입관리 대상은 다음과 같다.

1. 전산작업 산출물(전산발행보고서나 인쇄물등을 포함)
2. 정보기록매체(자기테이프, 광디스크, 디스켓, 메모리장치 등)
3. 개인용 컴퓨터 및 노트북을 포함한 휴대용 컴퓨터
4. 하드웨어 장비 및 부대설비나 장치
5. 진흥원의 자산으로 분류되는 물품
6. 위험물품, 약품
7. 기타 비품 등

제9조(정기점검) ① 정보화책임자는 다음 각 호에 대하여 시설의 관리실태를 매일 1회 이상 점검하고 매월 정밀 정기점검 해야 할 책임이 있다.

1. 각종 시설 및 장비의 동작 상태
2. 전원 시설 및 장비의 동작 상태
3. 각종 시설의 배선 및 주위 환경 정리 상태
4. 보안 관리 상태

② 제1항에 의한 정기점검 결과를 정보시스템실 업무일지 “별지 제4호 서식” 및 별도 양식에 기록, 관리한다.

제10조(장애 접수 및 보고) ① 이용자로부터 장비에 이상 발생 통보를 받은 자는 그 사실을 지체 없이 정보화담당에게 보고하여야 한다.

② 제1항에 의하여 보고받은 정보화담당은 장애내용 및 조치결과를 정보화책임자에게 보고하여야 한다.

③ 정보화책임자는 장애접수대장 “별지 제5호 서식”을 비치 기록·유지한다.

제11조(대장비치) 시설관리를 위해 정보시스템실 업무일지 “별지 제4호 서식” 및 전산장비관리대장 “별지 제6호 서식” 등 필요한 대장을 비치하고 기록·유지한다.

제12조(지침) 정보화책임자는 관련 법령이나 상급기관의 지침에 따라 합리적인정보통신 업무가 진행 될 수 있도록 신속한 대책을 강구하여야 한다.

제3장 설비 관리

제13조(항온항습기) ① 정보시스템실 내부의 각종 전산 장비의 정상적인 가동을 위해 일정한 온도와 습도를 유지시켜주는 항온항습기를 설치·운영한다.
② 정보화담당은 매일 시간대별로 항온항습기를 점검하고 이상유무를 정보시스템실 업무일지 "별지 제4호 서식"에 기록하여야 한다.

제14조(누수감지기) ① 정보시스템실 내부의 이중마루 바닥에 각종 배관의 누수를 감지하기 위한 누수감지기를 설치·운영한다.
② 정보화담당은 매일 시간대별로 누수감지기를 점검하고 이상유무를 정보시스템실 업무일지 "별지 제4호 서식"에 기록하여야 한다.

제15조(분전반) ① 정보시스템실 내부의 전기의 공급과 차단을 조작하고 부하 및 단락 등의 전기적인 이상 상태 발생시 전기를 자동적으로 차단하기 위한 분전반을 설치·운영한다.
② 정보화담당은 매일 분전반을 점검하고 정보시스템실 업무일지 "별지 제4호 서식"에 기록하여야 한다.

제4장 보안 관리

제16조(업무용 컴퓨터 보안관리) ① 정보화담당은 진흥원의 업무용 컴퓨터 및 노트북 운용 현황을 관리하고 임직원이 외부로 반출하고자 할 경우 저장 내용에 대한 보안 취약성 여부를 점검 후 점검 결과에 대한 정보화책임자의 승인을 얻어야 반출할 수 있다.
② 개인 소유의 저장장치가 포함된 컴퓨터, 노트북, 태블릿PC 등은 반입하여 사용할 수 없다. 다만 업무에 활용하고자 할 경우에는 정보화책임자의 확인 후 전산장비 반입 신청서 "별지 제12호 서식"을 작성하여 원장의 승인을 얻어야 반입할 수 있다. 입력장치와 출력장치의 경우 반입 관리 대장 "별지 제12호 서식"을 작성하여 정보화 책임자의 승인을 얻어야 한다. <개정 2019. 03. 14.>
③ 업무용 컴퓨터를 교체·반납하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 하드디스크에 수록된 자료가 유출되지 않도록 정보화담당을 통한 하드디스크 자료 백업 및 보안 서약서 "별지 제13호 서식" 작성 등의 보안조치를 하여야 한다.
④ USB, 스마트폰 등 개인 소유의 휴대용 저장매체를 업무용 컴퓨터에 연결하여 활용하고자 할 경우 반입 관리 대장 "별지 제12호 서식"을 작성하여 정보화 책임자의 승인을 얻어야 한다. <개정 2019. 03. 14.>

⑤ 인사발령에 의한 자리이동시 업무용 컴퓨터는 이동할 수 없으며, 자리 이동 전 업무용 컴퓨터 내 업무자료는 보존하고 개인정보는 삭제하여야 한다.

⑥ 휴직 및 퇴직자는 배정된 업무용 컴퓨터의 비밀번호를 후임자 또는 정보화담당에게 인계하여야 한다.

⑦ 개인 소유의 저장장치가 포함된 컴퓨터, 노트북 또는 휴대용 저장매체 등은 반출 시 수록된 자료가 유출되지 않도록 정보화담당을 통한 완전 포맷 등의 보안조치 후 정보화책임자의 반출내역 승인을 받아야 한다.

⑧ 업무용 컴퓨터 사용자는 다음 각 호의 정보보안 활동을 수행하여야 한다.

1. 업무상 생산 및 수집된 전자정보 및 자료에 대한 위·변조 훼손 및 유출 금지
2. 업무상 불필요한 인터넷사이트 및 응용프로그램 사용 금지
3. 퇴근 시 업무용 컴퓨터 전원 차단
4. 각종 시스템 오류에 대해서 정보화담당에게 신고
5. 그 밖에 개인의 정보보안에 대한 사항

[전문개정 2018. 10. 10.]

제17조(사용자 계정 관리) ① 사용자 계정(ID)은 비인가자 도용 및 정보시스템 불법 접속에 대비하여 다음 각 호의 사항을 반영하여 관리한다.

1. 사용자별 또는 그룹별로 접근 권한을 부여해야 한다.
2. 외부 사용자의 계정 부여는 불허하되 부득이한 경우에는 정보화책임자의 책임하에 유효 기간을 한정하는 등 보안조치를 강구한 후 허용할 수 있다.
3. 비밀번호가 없는 사용자 계정은 사용을 금지한다.

② 정보화담당은 사용자 계정의 등록・변경・폐기 등을 정보화책임자의 승인 하에 각 호의 사항을 반영하여 수행하고 원장에게 그 결과를 통보하여야 한다. <개정 2019. 06. 28.>

1. 적용대상
2. 유효기간
3. 접근권한범위(별표1)

③ 퇴직 또는 보직 변경 발생 시 정보화담당은 사용하지 않는 사용자계정 및 비밀번호를 신속히 삭제하여야 한다.

④ 정보화담당은 반기별 1회 또는 필요에 따라 사용자의 계정에 대한 관리 접근권한을 점검하고 정보화책임자에게 보고하여야 한다. <신설 2018. 10. 10.>

⑤ 원장은 부서별 사업에 필요한 정보시스템 담당자를 지정하여 정보시스템 도입 및 운용 권한을 부여하고, 필요 시 시스템 사용자 계정을 점검할 수 있다. <신설 2018. 10. 10.> <개정 2019. 06. 28.>

제18조(비밀번호 관리) ① 비밀번호는 다음 각 호의 사항을 반영하여 정한다.

1. 숫자와 문자 등으로 6자리 이상으로 정하고 분기별 1회 이상 주기적으로 변경, 사용하여야 한다.<개정 2018. 10. 10.>
2. 사용자 계정(ID)과 동일하지 않아야 한다.

3. 개인 신상 및 부서 명칭 등과 관계가 없어야 한다.
4. 일반 사전에 등록된 단어는 사용을 피해야 한다.
5. 동일 단어 또는 숫자를 반복하여 사용하지 말아야 한다.
6. 사용된 비밀번호는 재사용하지 말아야 한다.
7. 동일 비밀번호를 여러 사람이 공유하여 사용하지 말아야 한다.
8. 비밀번호를 외부로 표시되도록 하지 말아야 한다. <신설 2018. 10. 10.>

② <삭제 2018. 10. 10.>

1. 주기적으로 최소 90일 단위로 변경, 사용한다.
2. 비밀번호를 외부로 표시되도록 하지 말아야 한다.

③ 정보화담당은 공용 전산장비의 비밀번호 변경 이력을 비밀번호관리대장 “별지 제7호 서식”에 기록, 관리하여야 한다.

제19조(바이러스 방지대책) ① 악성 바이러스 감염을 방지하기 위하여 다음 각 호에 따라 정보시스템을 운영, 관리한다.

1. 출처·유통경로 및 제작자가 명확하지 않은 응용 프로그램은 바이러스 검색 프로그램으로 진단 후 사용해야 한다.
2. 익명으로 사용가능한 서비스를 제한해야 한다.
3. 실행파일은 읽기 전용으로 속성 변경해야 한다.
4. 인터넷 등 상용 통신망으로 입수한 자료는 필히 바이러스 검색 후 사용해야 한다.
5. 바이러스 조기 발견을 위하여 최신의 백신 프로그램을 활용해야 한다.
6. 시스템이 작동할 때 마다 컴퓨터 하드디스크의 부트섹터 및 메모리에 바이러스가 감염 되었는지 검색해야 한다.

② 바이러스 감염이 발견되었을 경우에는 정보화담당이 다음 각 호의 조치를 하여야 한다.

1. 바이러스 감염 피해의 최소화를 위하여 감염된 시스템을 사용 중지해야 한다.
2. 백신 프로그램을 이용하여 바이러스를 퇴치해야 한다.
3. 바이러스 감염 확산 방지를 위하여 사용자에게 관련 사실 및 보안조치사항을 즉시 전달해야 한다.

③ 원장은 “보안진단의 날”을 이용하여 진흥원 및 진흥원 입주업체에서 사용하는 전산시스템에 대해 바이러스 감염 여부 진단을 명할 수 있다.

제20조(외부망 연동) ① 원장은 지자체 또는 다른 기관과의 정보통신망과 연결, 사용하고자 할 경우에는 보안 관리 책임 한계를 설정하여야 한다.

② 외부망과 접속하는 경우에는 전산 자료의 제공범위 및 이용자의 접근 제한 등에 대하여 내부 심의를 거쳐야 한다.

③ 외부망 연결에 따른 보안 취약성 해소를 위하여 접속 자료를 주기적으로 분석하고 보안도구를 이용하여 정보통신망의 취약성을 수시 점검하여야 한다.

제21조(인터넷 등 상용망 연동) ① 전산망을 인터넷 등 상용망과 접속하고자 할 경우에는 악의적인 목적으로 접속을 시도하는 무단침입을 방지하기 위하여 침입차단 시스템 설치 운용 등 보안대책을 강구한다.

② 인터넷 등 상용망과의 접속은 불법침해(해킹)를 방지하고 효율적인 보안관리를 위하여 가급적 외부로의 접속점을 지정 운용함으로써 임의 접속을 차단한다.

③ 정보통신망에 사용되는 IP 주소는 체계적으로 관리하여야 하며, 내부정보 통신망을 보호하기 위하여 가급적 사설주소체계(NAT : Network Address Translation)를 이용하도록 한다. <개정 2018. 10. 10.>

④ 정보화담당은 네트워크 IP 주소 할당 내역을 네트워크 IP 관리대장 “별지 제8호 서식”에 기록, 관리하여야 한다.

⑤ 원격지 근무자가 내부망에 접속하고자 할 경우 정보화책임자의 승인을 받아야 하며, 각 호에 해당되거나 이 외에 승인하지 아니한 접속이 발견될 경우 즉시 시정조치 하여야 한다. <신설 2018. 10. 10.>

1. 백도어
2. VPN
3. 기타 원격 접속 소프트웨어

제22조(홈페이지 등 공개용 웹서버 보안) ① 웹서버는 방화벽을 네트워크 앞 단에 설치하여 내부망의 정보자원을 보호하여야 한다.

② 서버에 접근할 수 있는 사용자 계정을 제한하며 불필요한 계정들은 삭제 하여야 한다.

③ 홈페이지 게재 내용은 개인정보 및 비밀 내용 등 중요자료가 공개되지 아니하도록 하여야 한다.

④ 공개용 웹서버는 웹서비스를 제외한 모든 서비스 및 시험·개발도구 등의 사용을 제한하여야 한다.

⑤ IDS, 웹 취약성 점검도구 등 보안 도구를 이용하여 서버의 취약점 또는 무결성을 수시 점검하고 주기적으로 원래의 내용과 상이 여부를 점검하여야 한다.

⑥ 보안 사고에 대비하여 서버에 저장된 자료의 철저한 백업 체계를 수립, 시행하여야 한다.

제23조(방화벽 등 보안시스템 관리) ① 비밀번호는 제18조에 의거하여 반영하되 주기적으로 최소 60일마다 변경 사용한다.

② 보안관련시스템의 비밀번호는 정보화책임자 및 정보화담당 외에 공개 되지 않도록 한다. 만약 유지보수를 위하여 비밀번호가 외부에 노출되었을 경우 유지보수가 끝나면 즉시 수정하고 정보화책임자에게 보고해야 한다.

③ 보안관련시스템이 최적화된 환경에서 운영될 수 있도록 6개월마다 수립된 정책에 대해 분석하고 문제가 있을 경우 다시 정책을 수립해야 한다.

제5장 소프트웨어 관리

제24조(소프트웨어 관리업무) 정보화담당은 소프트웨어 관리를 위하여 다음의 업무를 수행한다.

1. 매 회계연도 마다 필요한 소프트웨어의 조달계획을 수립해야 한다.
2. 소프트웨어의 구입, 계약체결, 등록 등과 관련된 업무를 협조해야 한다.
3. 소프트웨어 관련문서를 작성・보관해야 한다.
4. 원본 CD, 디스크 및 라이선스를 증명하는 문서를 보관해야 한다.
5. 소프트웨어 관리실태를 점검 확인해야 한다.
6. 주기적으로 소프트웨어 관리 검사를 실시하고 검사결과를 원장에게 보고해야 한다.
7. 정품 소프트웨어 분실방지를 위해 조치를 취해야 한다.
8. 기타 소프트웨어 관리를 위하여 직원들을 교육・감독하여야 하며, 입주자(작가, 업체 등)가 사용하는 소프트웨어의 불법사용 등의 여부를 점검하고5 그 시정을 요구할 수 있다.

제25조(소프트웨어 구입) ① 소프트웨어는 구매부서를 통한 일괄구매를 원칙으로 하되, 진흥원의 예산 사정 및 일괄 구매 대상에서 제외된 소프트웨어의 경우 부서별로 구매가 가능하다.

② 정보화담당은 매 구입 시기 전에 진흥원 내 필요한 소프트웨어에 대한 수요조사를 하여 일괄구매를 실시한다.

③ 타 사업비로 구매할 경우 각 담당자는 가격, 구매조건 등을 정보화담당과 사전에 협의하여야 한다.

④ 구입한 소프트웨어는 상세내역을 소프트웨어보유대장 “별지 제9호 서식”에 등록하여야 한다.

제26조(소프트웨어 관리대장) ① 정보화담당은 정기적으로 소프트웨어 관련문서 등을 작성하여 보관하여야 한다.

② 설치된 소프트웨어의 내역은 개인(PC)별 설치현황표 “별지 제10호 서식”, 소프트웨어별 설치현황표 ”별지 제11호 서식“에 등록하여 관리하여야 한다.

③ 정보화담당은 변경된 사항이 있을 시에는 지체 없이 소프트웨어 관련문서를 갱신하여야 한다.

④ 소프트웨어 관련문서는 비공개사항을 제외하고는 누구든지 열람할 수 있도록 공개하여야 한다.

제27조(소프트웨어 점검) ① 정보화담당은 정기적으로 진흥원 내 소프트웨어 사용현황을 파악하여야 한다.

② 정보화책임자는 연 1회 소프트웨어 관리에 관한 실태를 점검하여야 한다.

③ 정보화책임자는 제2항에 의한 점검결과를 14일 이내에 원장에게 보고하고, 각 호에 해당하는 경우 즉시 시정조치 하여야 한다. <개정 2018. 10. 10.>

1. 업무와 관련없는 소프트웨어
2. 불법 설치 소프트웨어
3. 상업용과 비상업용이 구분되어 있는 소프트웨어
4. 기타 정보화담당의 승인없이 설치된 소프트웨어

제28조(임직원의 준수사항) 진흥원의 전 임직원은 소프트웨어 관리에 관하여 다음 각 호의 사항을 준수하여야 한다. <개정 2018. 10. 10.>

1. 정보화책임자의 승인 없이 진흥원이 소유하는 컴퓨터에 소프트웨어를 설치하여서는 아니 된다. <개정 2018. 10. 10.>
2. 정보화책임자의 승인 없이 진흥원이 보유하는 소프트웨어의 원본 CD, 디스크 및 그 복제물을 원외로 반출하여서는 아니 된다. <개정 2018. 10. 10.>
3. 정보화책임자의 승인 없이 개인이 소유하는 소프트웨어를 원내에 반입하여 설치하여서는 아니 된다. <개정 2018. 10. 10.>
4. 개인별 컴퓨터에서 소프트웨어에 대한 변경이 있는 경우에는 신속하게 정보화책임자에게 통보하여야 한다. <개정 2018. 10. 10.>
5. 소프트웨어 점검에 적극 협력하여야 한다.
6. 임직원은 제16조 8항을 준수하여야 한다. <신설 2018. 10. 10.>

[제목개정 2018. 10. 10.]

제6장 보칙

제29조(다른 법령과의 관계) 이 규칙에 명시되지 않은 사항은 다음 각 호의 법령 및 지침 등을 따른다.

1. 『정보통신망 이용촉진 및 정보보호 등에 관한 벌률』 및 동법 시행령, 시행규칙
2. 『개인정보보호법』 및 동법 시행령, 시행규칙
3. 『부천시 정보보안 기본지침』
4. 『국가사이버안전매뉴얼』
5. 『공공기관 영상정보처리기기 설치・운영 가이드라인』
6. 『그 밖의 관계 법령』

[본조신설 2018. 10. 10.]

부 칙 (2009. 07. 13. 규칙 제19호)

이 규칙은 원장이 확정한 날부터 시행한다.

부 칙 (2018. 10. 10. 규칙 제106호)

제1조(시행일) 이 규칙은 2018년 10월 19일부터 시행한다.

부 칙 (2019. 03. 14. 규칙 제109호)

제1조(시행일) 이 규칙은 공포 후 3일이 경과한 날부터 시행한다.

부 칙 (2019. 06. 28. 규칙 제116호)

제1조(시행일) 이 규칙은 공포 후 3일이 경과한 날부터 시행한다.

부 칙 (2020. 09. 04. 규칙 제139호)

제1조(시행일) 이 규칙은 공포 후 3일이 경과한 날부터 시행한다.

부 칙 (2025. 03. 07. 규칙 제191호)

제1조(시행일) 이 규칙은 공포 후 3일이 경과한 날부터 시행한다.

(별표 제1호) <신설 2019. 06. 28.> <개정 2025. 03. 07.>

전자결재시스템 접근권한 부여기준

구 분	기 록 물		기록물철	
	일 반	보 안	공 개	비 공 개
기 안 자	○	○	○	○
비기안자	○	X	○	○
결재권자	○	○ (협조자 포함)	○	○
시스템관리자	○	○	○	○
기록물 열람 신청자	○	△ (신청 내용에 한함)	○	○

※ 기록물 열람 신청자는 별지 제17호 서식 기록물 열람 신청서로 열람 신청

(별지 제1호 서식)

정보시스템실 출입 관리 대장

일시	입실 시간	퇴실 시간	용무	출입자			입회자			결 재	
				소속	직위	성명	소속	직위	성명	담당	책임자

(별지 제2호 서식) <삭제 2025. 03. 07.>

(별지 제3호 서식) <삭제 2025. 03. 07.>

(별지 제4호 서식)

정보시스템실 업무 일지

결 재	정보화담당	정보화책임자	진흥원장

▣ 근무일자 : . . . (요일)

▣ 시스템 점검 및 관리

업 무	장애 현황		
	H/W	O/S, DB	App.

업 무	장애 현황		
	H/W	O/S, DB	App.

구 분	운영 및 장애 현황

▣ 시스템 점검 및 관리

백업 내용	백업형태 (F/S,DB)	백업대상 서버	백업 매체	백업 주기	백업 결과			비고
					성공	부정확	실패	

▣ 보안 관리

구 분	운영 현황
침해사고 발생 및 대응현황	
보안장비 설정운영	

▣ 시설/장비 관리

구 분	운영 현황
설치 및 업그레이드 내역	
고장 및 수리 내역	

▣ 공조 설비 관리

구 분	9	11	13	15	17	19	21	23	1	3	5	7

항온 항습기	설정온도												
	현재온도												
	설정습도												
	현재습도												
	조작판이벤트												
	냄새, 이상소음												
누수	누수감지기												
	드레인												

▣ 전원 설비 관리

차단기 번호	차단기 용량	전력 사용량			기기명	역할	비고
		R	S	T			

(별지 제5호 서식)

장애 접수 대장

연번	월 일	접수 시간	장애내용	조치결과	처리 시간	신고자 (연락처)	접수자	결 재	
								담당	책임자

(별지 제6호 서식)

전산장비 관리 대장

연번	도입일	장비 번호	업무명	종료	제조사	모델명	규격	설치 위치	결 재	
									담당	책임자

(별지 제7호 서식)

공용전산장비 비밀번호 관리 대장

도입일	장 비 명	사용자 계정	비밀번호	비고	결 재	
					정보화 담당	정보화 책임자

(별지 제8호 서식)

네트워크 IP 관리 대장

결재	정보화담당	정보화책임자	진흥원장

변경이력번호 : V.　　(설정일 :　.　.　.)

순번	담당자	부서	IP	S/M	G/W	DNS	장비명	MAC ADD.	비고

(별지 제9호 서식)

소프트웨어 보유 대장

결재	정보화담당	정보화책임자	진흥원장

S/W 고유번호		제작사	
S/W명			
제품(인증)번호			
도입시 버젼		사용가능 버젼	
라이센스 유형		라이센스 기간	
도입 일자		고객지원 기간	
도입 수량		설치 수량	
제공 회사		담당자	
연락처		E-mail	
폐기 일자			

(별지 제10호 서식)

개인(PC)별 설치 현황표

설치일	
PC고유번호	
부 서	
성 명	

결재	정보화담당	정보화책임자	진흥원장

순번	S/W 번호	S/W명(및 버젼)	설치일	라이센스 만료일	유형				비고
					상용	쉐어	공개	번들	

(별지 제11호 서식)

소프트웨어별 설치 현황표

설치일	
PC고유번호	
부 서	
성 명	

결재	정보화담당	정보화책임자	진흥원장

순번	PC 고유번호	사용자	설치일	비 고

(별지 제12호 서식) <신설 2018. 10. 10.>, <개정 2019. 03. 14.>

전산 장비 반입 신청서

부서명	
신청자	

결재	정보화담당	정보화책임	원장

반입신청품목	□ PC □ 노트북 □ 태블릿PC □ 이동식저장장치 □ 모니터 □ 기타( )
네트워크	선로 신규 설치 (□ 업무망 □ 인터넷망 □ 해당없음) IP 신규 발급 (□ 업무망 □ 인터넷망 □ 해당없음)
신청사유	※ PC 및 노트북 반입 시 포맷 후 우리원 사무용 소프트웨어 또는 뷰어 설치 ※ PC, 노트북, 태블릿PC 등은 원장의 승인을 얻어야 하며, 휴대용 저장매체와 기타 입출력장치는 정보화책임자의 승인을 얻어야 함

상기와 같이 신청합니다.

20 . . .

신청인 : (인)

등록번호		실사용자	

(별지 제13호 서식) <신설 2018. 10. 10.>

보안 서약서

본인은 년 월 일부로 관련 용역사업(업무)을 수행함에 있어 다음사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 관련 업무 중 알게 될 일체의 내용이 직무상 기밀 사항임을 인정한다.

2. 본인은 이 기밀을 누설함이 국가안전보장 및 국가이익에 위해가 될 수 있음을 인식하여 업무수행 중 지득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.

3. 본인이 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다.

4. 본인은 하도급업체를 통한 사업 수행 시 하도급업체로 인해 발생하는 위반사항에 대하여 모든 책임을 진다.

년 월 일

서 약 자 (업체 대표)	업 체 명 : 직 위 : 성 명 : 생 년 월 일 :	(서명)
서약집행자 (담당자)	소 속 : 한국만화영상진흥원 직 위 : 성 명 : 생 년 월 일 :	(서명)

(별지 제14호 서식) <신설 2020. 09. 04.>

보안 서약서

본인은 년 월 일부로 사업을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 과 관련된 소관업무가 기밀(개인정보 포함) 사항임을 인정하고 제반 보안관계규정 및 지침을 성실히 준수한다.

2. 본인은 이 기밀(개인정보 포함)을 누설함이 이적 및 불법 행위임을 명심하고 재직 중은 물론 퇴직 후에도 알게 된 모든 기밀사항을 일절 타인에게 누설하지 아니한다.

3. 본인은 반드시 기밀(개인정보 포함)을 업무 수행 목적 외 처리 하지 않고 분실·도난·유출·변조·훼손되지 않도록 안전하게 관리한다.

4. 본인이 이 기밀(개인정보 포함)을 누설하거나 관련 규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다.

년 월 일

서 약 자 (참여자)	업 체 명 :		
	직 위 :		
	성 명 :		(서명)
	생 년 월 일 :		
서약집행자 (담당자)	소 속 :	한국만화영상진흥원	
	직 위 :		
	성 명 :		(서명)
	생 년 월 일 :		

(별지 제15호 서식) <신설 2020. 09. 04.>

보안 확약서

본인은 업무(용역 사업)와 관련한 장비, 서류, 중간·최종 산출물 등 모든 제반자료(개인정보 포함) 등에 대하여 다음과 같이 이행하였음을 확약합니다.

1. 용역사업(업무) 관련한 모든 제반자료 반환(인계인수대장 확인 완료)

2. 용역사업(업무) 관련한 저장매체 내 자료 삭제

3. 용역사업(업무) 관련한 사업산출물 복사본 등을 별도 보관하지 않음

4. 본인이 이 기밀(개인정보 포함)을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다.

년 월 일

서 약 자 (업체 대표)	업 체 명 :	
	직 위 :	
	성 명 :	(서명)
	생 년 월 일 :	
서약집행자 (담당자)	소 속 : 한국만화영상진흥원	
	직 위 :	
	성 명 :	(서명)
	생 년 월 일 :	

(별지 제16호 서식) <신설 2020. 09. 04.>

용역업체 참여직원 보안교육

교육내용	교육여부(O, X)
○유지보수 인력은 당해 기관의 사전 승인을 득하고 보안서약서 제출	( )
○통제구역 출입 시 담당자와 동석해야 하고 임의 출입금지	( )
○통제구역 출입 시 화재위험이 있는 물품 소지 금지	( )
○유지보수 업무 영역 외 타시스템 접근 금지	( )
○정보시스템과 연결하여 자료 유출 가능성이 있는 USB, 스마트폰 등 휴대용 저장매체의 비인가 사용금지	( )
○카메라 내장 휴대폰, 디지털 카메라 등 소지 및 촬영 금지	( )
○노트북 및 USB 등 정보시스템 사용 시 악성코드 등 감염여부 확인 및 자료 복사, 이동 금지	( )
○취급하는 대외비(정보통신망, IP주소, 비밀번호 등) 복사 및 유출 금지	( )

교육일시	20 . . .
피교육자	※ 위 사항을 위반할 시 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다. (소속) (성명) (서명)
교 육 자	(소속) (성명) (서명)
비 고	

(별지 제17호 서식) <신설 2025. 03. 07.>

<table>
<tr><td colspan="2" rowspan="4">기록물 열람 신청서</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">협조</td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td>목 적</td><td colspan="5"></td></tr>
<tr><td rowspan="2">신청자</td><td>성 명</td><td></td><td>연락처</td><td colspan="2"></td></tr>
<tr><td>부서명</td><td colspan="4"></td></tr>
<tr><td rowspan="5">요청 정보</td><td rowspan="2">열람일시</td><td>☐</td><td colspan="3">업무 인수인계 관련 사항으로 영구 지정 요청</td></tr>
<tr><td>☐</td><td colspan="3">특정 업무 수행으로 기간 지정 요청</td></tr>
<tr><td>생산부서</td><td colspan="4"></td></tr>
<tr><td>연도범위</td><td colspan="4"></td></tr>
<tr><td>문서정보</td><td colspan="4"></td></tr>
<tr><td>주의 사항</td><td colspan="5">※ 기록물 열람 신청을 통해 취득한 자료는 우리 기관의 재산임을 명확히 인지하고 지정된 업무 외에 사용하지 않으며 복제하거나 사본 등의 형태로 보관하지 않는다에 동의한 것으로 간주합니다.
※ 열람 기간 종료 도래 전 해제요청을 하지 않을 시 열람 신청자 귀책사유입니다.
※ 공공기록물법 제19조의2(기록물의 무단 은닉 등의 금지), [내규]취업 규정 제8조(부작위 의무)에 따라 모든 기록물 열람을 통해 취득한 자료를 무단으로 유출, 사적 이용 등을 할 경우 공공기록물법 제51조(벌칙), [내규]취업 규정 시행규칙 별표1(징계양정기준)에 따라 조치될 수 있습니다.</td></tr>
<tr><td rowspan="2">접수</td><td></td><td></td><td></td><td></td><td></td><td rowspan="2"></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

(별지 제18호 서식) <신설 2025. 03. 07.>

정보화 기자재 통합물품출납대장

반 출		사용장소	사유	품명	수량	물품번호	반 입	
일시	반출자						일시	반입자