정보보안기본지침[목차로]

제정 2017. 12. 28.
개정 2021. 12. 28.

제 1 장 총 칙

제1조(목적) 이 지침은 「국가 정보보안 기본지침」에 의거 한국콘텐츠진흥원(이하 "진흥원"이라 한다)의 「보안업무규칙」에서 위임한 사항과 그 시행에 필요한 절차와 세부사항을 규정함을 목적으로 한다.

제2조(적용범위) 이 지침은 전산장비 또는 정보통신망을 운용하고 있는 진흥원 및 그 부설기관 전 부서에 적용된다.

제3조(용어의 정의) 이 지침에서 정하는 용어의 정의는 다음 각 호와 같다.

1. "사용자"라 함은 원장으로부터 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 자를 말한다.
2. "정보통신망"이란 「전기통신기본법」 제2조 제2호의 규정에 따른 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집 · 가공 · 저장 · 검색 · 송수신하는 정보통신체제를 말한다.
3. "인터넷서비스망"(이하 "인터넷망"이라 한다)이란 진흥원의 네트워크 중에서 인터넷을 사용할 수 있도록 연결되어 있는 인터넷 전용망을 말한다.
4. "업무전산망"(이하 "내부망"이라 한다)이란 진흥원의 네트워크 중에서 내부 업무를 수행할 수 있도록 연결되어 있는 전산망을 말한다.
5. "정보시스템"이란 PC · 서버 등 단말기, 보조기억매체, 전산 · 통신장치, 정보통신기기, 응용프로그램 등 정보의 수집 · 가공 · 저장 · 검색 · 송수신에 필요한 하드웨어 및 소프트웨어 일체를 말한다.

6. “저장매체”라 함은 자기저장장치·광 저장장치·반도체 저장장치 등 자료기록이 가능한 전자장치를 말한다.
7. “휴대용 저장매체”라 함은 디스켓, 이동형 하드디스크(HDD), USB 메모리, Flash메모리, CD, DVD 또는 IC칩 등에 정보를 저장할 수 있는 모든 것으로 정보통신망과 분리할 수 있는 기억장치를 말한다.
8. “정보보안” 또는 “정보보호”란 정보시스템 및 정보통신망을 통해 수집·가공·저장·검색·송수신되는 정보의 유출·위변조·훼손 등을 방지하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위로서 사이버안전을 포함한다.
9. “전자문서”란 컴퓨터 등 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 정보를 말한다.
10. “전자기록물”이란 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 기록정보자료를 말한다.
11. “전자정보”란 업무와 관련하여 취급하는 전자문서 및 전자기록물을 말한다.
12. “정보자산”이란 하드웨어(서버, 워크스테이션, 개인용컴퓨터, 통신장비, 보안장비, 저장매체, 프린터 등), 소프트웨어, 응용프로그램, 개발산출물, 운영산출물 등을 말한다.
13. “정보보안시스템”이란 정보의 수집·저장·검색·송신·수신 시 정보의 유출, 위·변조, 훼손 등을 방지하기 위한 하드웨어 및 소프트웨어를 말한다.
14. “사이버공격”이란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스방해 등 전자적 수단에 의하여 정보통신망을 불법침입·교란·마비·파괴하거나 전자정보를 절취·훼손하는 공격 행위를 말한다.
15. “완전포맷”이란 저장매체 자료저장 전체의 위치에 새로운 자료(0 또는 1)를 중복하여 저장하는 것을 말한다.
16. “보안담당관”이라 함은 보안책임자로서 보안계획 및 운영 등 보안업무 총괄기능을 수행하는 자로 전산업무담당 본부장을 말한다. <개정 2021.12.28.>
17. “정보보안담당관”이라 함은 전산분야의 보안계획 및 운용 등의 기능

을 수행하는 자로 전산업무담당 부서장을 말한다. <개정 2021.12.28.>

18. “분임정보보안담당관”이라 함은 정보시스템을 운영하는 소관부서의 팀장을 말한다. <개정 2021.12.28.>

19. “정보보안담당자”라 함은 정보보안 담당관의 임무를 위임받아 원내 정보보안업무 실무를 수행하는 부서원을 말한다. <신설 2021.12.28>

제 2 장 정보보안 기본활동

제4조(기본원칙) ① 원내 사업 추진 시 발생된 정보자산은 진흥원 소유이며, 관리는 각 팀 단위로 한다.

② 진흥원 정보자산은 업무상 필요한 최소한의 접근권한이 부여되어야 한다.

③ 인가된 사용자는 전자정보를 사용함과 동시에 보호할 책임을 가지며, 비인가자는 자신의 업무와 무관한 어떠한 정보자산에도 접근을 시도해서는 아니 된다.

④ 진흥원 직원은 정보보안기본지침을 준수 할 의무가 있으며 이를 위반할 시에는 주의, 경고 등을 포함한 인사규정에 따라 징계의 사유가 될 수 있다.

제5조(정보보안 조직의 운영) ① 보안담당관은 「보안업무규칙」제8조 제4항의 임무를 수행하기 위하여 정보보안담당관, 분임정보보안담당자, 정보보안담당자를 지정하여 운영할 수 있다. <개정 2021.12.28.>

② 정보보안담당관은 다음 각 호의 정보보안 기본활동을 수행하여야 한다.

1. 정보보안 정책 및 세부추진계획 수립 · 시행
2. 정보보안 관련 규정 · 지침 등 제 · 개정
3. 보안심사위원회에 정보보안 분야 안건 심의 주관
4. 정보보안 업무 지도 · 감독, 정보보안 감사 및 심사분석
5. 정보보안 보안관리 실태에 대한 자체 조사 · 평가
6. 사이버공격 초동조치 및 대응
7. 사이버위협정보 수집 · 분석 및 보안관제

8. 정보보안 예산 및 전문인력 확보
9. 정보보안 사고 조사 결과 처리
10. 정보보안 교육 및 정보협력
11. 정보통신망 보안대책의 수립 · 시행
12. “사이버보안진단의 날” 수립 · 시행
13. 그 밖에 정보보안 관련 사항

③ 정보보안담당관은 보안담당관의 업무를 위임하여 수행하며, 정보보안 업무 실무를 수행하고 현황을 주기적으로 보고하여야 한다. <개정 2021.12.28.>

④ 분임정보보안담당자는 소관부서 정보시스템의 보안대책을 수립·이행하고 현황을 주기적으로 보고하여야 한다. <개정 2021.12.28.>

제6조(활동계획 수립 및 심사분석) ① 보안담당관은 진흥원의 정보보안 업무 세부추진계획(「국가사이버안전관리규정」 제9조에 따른 사이버안전대책을 포함한다)을 수립 · 시행하고 그 추진결과를 심사분석 및 평가하여야 한다. <개정 2021.12.28.>

② 보안담당관은 세부추진계획 및 심사분석을 별지 제1호 및 제2호 서식에 따라 다음 각 호의 기한 내에 작성하여야 한다. <개정 2021.12.28.>

1. 당해 연도 보안업무 추진계획을 1월 25일 까지 수립한다.
2. 전년도 하반기 및 당해 연도 상반기 보안업무 심사분석을 7월 31일 까지 실시한다.

제7조(정보보안 내규 제 · 개정) 정보보안담당관은 정보보안 관련 내규를 주기적으로 검토하고 제 · 개정하여야 한다. <개정 2021.12.28.>

제8조(정보보안 감사) ① 정보보안담당관은 연 1회 이상 자체 정보보안 감사를 실시할 수 있다. <개정 2021.12.28.>

② 감사수행 시, 정보보안담당관은 효율적인 정보보안 감사 수행을 위하여 감사 방향, 중점사항 등을 선정하여 보안담당관에게 보고한다. <개정 2021.12.28.>

제9조(정보보안 교육) ① 정보보안담당관은 정보보안 교육계획을 수립하여 연 1회 이상 전 직원을 대상으로 관련 교육을 실시하여야 한다. <개정 2021.12.28.>

② 정보보안담당관은 정보보안 관련 전문기관 교육 및 기술 세미나 참석을 장려하는 등 정보보안담당자의 업무 전문성을 제고하기 위하여 연간 40시간 이상 관련 전문기관 교육 및 기술 세미나 참석을 적극 장려하여야 한다. <개정 2021.12.28.>

제10조(사이버보안진단의 날) ① 정보보안담당관은 정보보호를 위해 매월 셋째 주 수요일 전 임직원이 참여하는 '사이버보안진단의 날'을 운영하여야 한다. <개정 2021.12.28.>

② 분임정보보안담당자는 '사이버보안진단의 날'에 소관 정보통신망 악성코드 감염여부, 정보시스템 보안 취약점 점검 등 정보보안 업무전반에 대하여 보안진단을 실시하여야 한다. <개정 2021.12.28.>

③ 분임정보보안담당자는 제1항 및 제2항에 따른 보안진단 결과를 정보보안담당관에게 통보하여야 한다. <개정 2021.12.28.>

④ 사용자는 '사이버보안진단의 날' 또는 월 1회 에 해당 보안 프로그램을 반드시 실행하고 미비점을 보완하여야 한다. <신설 2021.12.28.>

제11조(정보보안 사고 조사) ① 정보보안담당관은 정보보안 사고 발생 시 즉시 피해확산 방지조치를 취하여야 한다. 이 경우, 사고원인규명 시까지 피해 시스템에 대한 증거를 보전하고 임의로 관련 자료를 삭제하거나 포맷하여서는 아니 된다. <개정 2021.12.28.>

1. 일시 및 장소
2. 사고 원인 및 피해 현황 등 개요
3. 사고자 및 관계자의 인적 사항
4. 조치내용 등

② 정보보안담당관은 사고원인 및 피해 현황을 파악하고, 재발방지 대책의 수립 · 시행 등 사고조사 결과에 따라 보호대책을 마련하고 조치하여야 한다. <개정 2021.12.28.>

제12조(정보통신망 현황·자료 관리) 분임정보보안담당자는 다음 각 호에 해당하는 정보통신 운용현황을 관리하여야 하며, 정보보안담당관의 요청 시 관련 자료를 제출하여야 한다. <개정 2021.12.28.>

1. 정보시스템 운용현황
2. 정보통신망 구성현황
3. IP주소할당 현황
4. 주요 정보화사업 추진현황

제 3 장 정보통신시설 및 정보시스템 보안관리

제 1 절 기본사항

제13조(정보보안 활동) 정보보안담당관은 진흥원의 정보보안 강화를 위하여 다음 각 호의 사항을 수행할 수 있다. <개정 2021.12.28.>

1. 모의 사이버테러 훈련(모의해킹, 모의침투 훈련 등)
2. 정보보안대책 수립·이행에 대한 점검
3. 사이버 침해사고 발생시 대응·복구 현황 점검
4. 그 밖에 정보보안을 위하여 필요한 사항

제14조(정보통신시설 보안) ① 정보보안담당관은 「보안업무규칙」 제15조에 따라 정보통신시설 및 장소를 보호구역으로 지정하여 관리하여야 한다. <개정 2021.12.28.>

② 정보보안담당관은 제1항에서 지정된 보호구역에 대한 보안 대책을 강구할 경우 다음 각 호의 사항을 조치하여야 한다. <개정 2021.12.28.>

1. 정보통신시설에 대한 방호 및 방재대책
2. 상시 이용하는 출입문은 한 곳으로 정하고 이중 잠금장치 설치
3. 출입자 인증·식별 등을 위한 출입문 보안장치 설치
4. 정전에 대비한 비상전원 공급, 시스템의 안정적 중단 등 전력관리 대책
5. 비인가자에 대한 출입 및 정보자산의 반·출입 통제

제15조(정보시스템 보안) ① 직원은 PC 등 정보시스템을 사용하거나 본인 계정으로 정보통신망에 접속하는 것과 관련한 보안책임을 가진다.

② 분임정보보안담당자는 서버·네트워크 장비 등 부서 공통으로 사용하는 정보시스템의 운용과 관련한 보안책임을 가진다. <개정 2021.12.28.>

③ 분임정보보안담당자는 해당 부서 정보시스템의 변경 현황을 유지하여야 하며 정보보안담당관 요청 시 사본을 제출하여야 한다. <개정 2021.12.28.>

④ 분임정보보안담당자는 정보시스템이 비인가자에게 불필요한 서비스를 허용하지 않도록 보안기능을 설정하여야 하며, 보안취약점을 제공할 수 있는 다음 각 호의 프로그램 설치를 제한하여야 한다. <개정 2021.12.28.>

1. P2P, 웹 하드 등 파일 공유 프로그램
2. 비인가 프로그램
3. 출처가 불분명한 응용프로그램
4. 업무상 불필요한 프로그램

⑤ 분임정보보안담당자는 소관 시스템의 안정적 운영을 위해 다음 각 호에 따라 관리해야 한다.

1. 신규로 설치되는 시스템의 취약점 점검 및 조치
2. 시스템의 운영체제 등 최신 패치 실행
3. 설치·운영 중인 시스템의 수시 보안취약점 점검 및 조치

⑥ 정보보안담당관은 제1항부터 제5항까지에 명시된 정보시스템 운용과 관련한 보안취약점을 발견하거나 보안대책 강구가 필요하다고 판단할 경우, 분임정보보안담당자에게 개선을 요구할 수 있다. <개정 2021.12.28.>

제16조(보안성 검토) ① 분임정보보안담당자는 다음 각 호에 해당하는 경우에 자체 보안대책을 강구하고 사업 계획단계에서 정보보안담당관과 협의를 거쳐 보안성 검토를 요청하여야 한다. <개정 2021.12.28.>

1. 유·무선 네트워크를 신·증설하거나 서버 등 정보시스템을 구축하는 경우
2. 내부 정보통신망을 외부망과 연결하고자 하는 경우
3. 암호장비·보안자재·암호논리·암호모듈을 도입 운용하고자 하는 경우
4. 원격근무 지원 등을 위해 시스템을 도입하는 경우

5. 외부기관에 보안감리 또는 보안컨설팅을 의뢰하거나 정보처리·보안관제 등의 업무를 위탁하는 경우
6. 그 밖에 정보통신망 및 정보시스템 운용환경 변화로 인하여 별도의 보안대책 수립이 필요하다고 인정되는 경우

② 그 밖에 규정하지 않은 사항은 「국가 정보보안 기본지침」에 따른다.

제 2 절 전자정보 보안대책

제17조(PC 등 단말기 보안관리) ① 단말기 사용자는 PC · 노트북 · 스마트기기 등 단말기(이하 "PC 등"이라 한다) 사용과 관련한 일체의 보안관리 책임을 가진다.

② PC 등에 적용되는 사용자계정(ID) 및 비밀번호의 취급관리는 제21조(사용자계정 관리)와 제22조(비밀번호 관리)의 사항을 준용한다.

③ 사용자는 PC 등의 보안관리를 위해 다음 각 호의 사항을 준수하여야 한다.

1. 부팅 시 CMOS 비밀번호 설정
2. 컴퓨터명은 성명으로 설정하고 작업그룹명은 부서명으로 설정
3. 최대 10분을 초과하지 않도록 화면보호기 설정
4. IP주소 임의변경 금지
5. 최신 보안업데이트, 바이러스 치료 프로그램 등 보안프로그램 설치 및 주기적 검사

④ 정보보안담당관은 비인가자가 PC 등을 무단으로 조작하여 전자정보를 유출하거나, 위·변조 및 훼손시키지 못하도록 다음 각 호에 따른 보호대책을 강구하여야 한다. <개정 2021.12.28.>

⑤ 분임정보보안담당자는 PC 등을 교체·반납·폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 하드디스크에 수록된 자료가 유출, 훼손되지 않도록 완전삭제 등 보안조치를 수행하고, 정보보안담당관 요청 시 결과를 제출하여야 한다. <개정 2021.12.28.>

⑥ PC 등의 외부 반출을 제한하며, 외부 업무용으로 사용하는 PC 등에 한하여 분임정보보안담당자의 책임 하에 반출 할 수 있다.<개정 2021.12.28.>

⑦ 분임정보보안담당자는 PC 등의 반출·입 통제조치를 수행하여야 한다. <개정 2021.12.28.>

⑧ 정보보안담당관 요청 시 분임정보보안담당자는 반출·입 현황을 제공하여야 한다. <개정 2021.12.28.>

제18조(서버 보안관리) ① 분임정보보안담당자는 서버 도입 시, 정보보안담당관과 협의하여 다음 각 호의 보안대책을 수립하고 시행하여야 한다. <개정 2021.12.28.>

1. 저장자료의 절취, 위·변조 등에 대한 대비
2. 업무별·자료별 중요도에 따른 접근권한 차등 부여
3. 인가된 범위 이외의 접근통제
4. 서버 운용에 필요한 서비스 포트 외에 불필요한 서비스 포트 차단
5. 운영·관리 목적으로 접속 시 내부망 IP 주소가 부여된 관리용 단말기 지정
6. 서버 설정정보 및 저장된 자료의 정기적 백업

② 분임정보보안담당자는 데이터베이스에 대하여 사용자의 직접적인 접속을 차단하고 개인정보 및 중요정보를 안전하게 저장할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치를 하여야 한다. <개정 2021.12.28.>

제19조(웹서버 등 공개서버 보안관리) ① 분임정보보안담당자는 외부인에게 공개할 목적으로 설치하는 공개서버에 대해 홈페이지 위변조, 분산서비스거부(DDoS)공격 등으로부터 보호하기 위한 다음 각 호의 보안대책을 수립하여 시행하여야 한다. <개정 2021.12.28.>

1. 내부망과 분리된 영역(DMZ)에 설치·운용
2. 접근할 수 있는 사용자계정을 제한하고 불필요한 계정 삭제
3. 비공개 자료 및 개인정보가 유·노출, 위·변조되지 않도록 보안조치
4. 프로그램 개발·시험에 사용된 도구(컴파일러 등)는 개발 완료 후 사용이 제한되도록 보안기능 설정 또는 삭제

② 정보보안담당관은 공개서버의 보안취약점을 수시로 점검하고, 홈페이지 위변조, 분산서비스거부(DDoS)공격, 악성코드, 민감정보의 위·변조 및 훼손 여부를 주기적으로 확인하여야 한다. <개정 2021.12.28.>

③ 신규 홈페이지 구축 시에는 행정안전부 등 국가 기준에 준하는 홈페이지 개발 보안 가이드에 따라 웹 취약점 보안점검을 실시한 후 점검결과를 정보보안담당관에 제출하여야 한다. <개정 2021.12.28.>

④ 만약 신규 홈페이지 시스템에서 개인정보를 취급할 경우에는 개인정보 내부관리규칙에 따라 개인정보처리시스템에 대한 자체점검을 실시하고 점검결과를 정보보안담당관에 제출하여야 한다. <개정 2021.12.28.>

⑤ 정보보안담당관은 보안점검 결과의 취약점에 대해 개선조치를 요구할 수 있으며, 조치결과 확인 후 신규 개설을 승인하여야 한다. <개정 2021.12.28.>

제20조(홈페이지 게시자료 보안관리) ① 분임정보보안담당자는 개인정보를 포함한 중요 업무자료가 홈페이지에 무단 게시되지 않도록 정보공개절차를 마련하여 시행하여야 한다. <개정 2021.12.28.>

② 분임정보보안담당자는 개인정보, 비공개 문서, 민감정보 등이 포함된 자료를 홈페이지에 공개하여서는 아니 된다.<개정 2021.12.28.>

③ 직원은 인터넷 블로그 · 카페 · 게시판 · 개인홈페이지 또는 소셜네트워크 서비스 등 공개된 전산망에 업무관련 자료를 무단 게재하여서는 아니 된다.

④ 정보보안담당관은 홈페이지 등에 비공개 내용이 게시되었는지 여부를 주기적으로 확인하여야 한다. <개정 2021.12.28.>

⑤ 정보보안담당관은 홈페이지에 중요정보가 공개된 것을 인지할 경우 이를 즉시 삭제하는 등의 보안조치를 강구하여야 한다. <개정 2021.12.28.>

제21조(사용자계정 관리) ① 정보보안담당관은 사용자계정(ID)의 비인가자 도용 및 정보시스템 불법접속 등을 방지하기 위해 다음 각 호의 사항을 조치하여야 한다. <개정 2021.12.28.>

1. 신규 사용자계정 생성 시 별지 제5호에 따라 신청서 작성, 신원확인

등의 절차를 거쳐 발급

2. 직무변경, 퇴직 등 인사이동이 있을 경우 관련 정보시스템 접근권한을 조정
3. 사용자별·그룹별 접근권한 부여 및 사용자계정 공용 금지
4. 외부 사용자의 계정부여는 불허하되, 부득이한 경우 유효기간을 설정하는 등의 보안조치 후 허용
5. 비밀번호 등 사용자 식별·인증 수단이 없는 사용자계정 사용 금지
6. 장기간 사용하지 않는 휴면계정을 점검하여 불필요시 삭제
7. 사용자계정을 주기적(관리자 계정 3개월, 사용자계정 6개월)으로 점검하여 접근권한 재검토

② 정보시스템의 계정은 사용목적 및 권한에 따라 관리자계정과 사용자계정으로 구분하여 관리하여야 한다.

③ 관리자계정은 관리자로 지정된 자만이 사용할 수 있으며, 타인에게 대여할 수 없다. 다만, 업무상 필요에 의해 타인에게 대여한 경우에는 회수 후 즉시 비밀번호를 변경하여야 한다.

④ 분임정보보안담당자는 별지 제6호에 따라 소관 정보시스템별 계정발급현황을 관리하여야 한다. <개정 2021.12.28.>

제22조(비밀번호 관리) ① 비밀번호는 다음 각 호의 사항을 반영하여 숫자와 영문자, 특수문자 등을 혼합하여 9자리 이상으로 정하여야 한다. 다만, 정보시스템에서 기능을 지원하지 않는 경우는 예외로 한다.

1. 사용자계정(ID)과 동일하지 않을 것
2. 개인신상 및 부서명칭 등과 관계가 없을 것
3. 일반 사전에 등록된 단어 또는 추측하기 쉬운 단어는 사용을 피할 것
4. 동일단어 또는 숫자를 반복하여 사용하지 말 것
5. 사용된 비밀번호는 재사용하지 말 것
6. 비밀번호를 여러 사람이 공유하여 사용하지 말 것
7. 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지
8. 비밀번호에 유효기간을 선정하여 주기적으로 변경할 것

② 서버에 등록된 비밀번호는 암호화하여 저장하여야 한다.

③ 비밀이나 중요자료는 자료별 비밀번호를 부여하여야 한다.

제23조(네트워크장비 보안관리) ① 분임정보보안담당자는 라우터, 스위치 등 네트워크 장비 운용과 관련하여 다음 각 호의 보안조치를 강구하여야 한다. <개정 2021.12.28.>

1. 네트워크 장비에 대한 원격접속은 원칙적으로 금지하되 불가피할 경우 장비 관리용 목적으로 접근제어솔루션(NAC)의 통제에 따라 내부에 지정된 단말기 IP 주소에서만 접속 허용
2. 물리적으로 안전한 장소에 설치하여 비인가자의 무단접근 통제
3. 최초 설치 시 보안취약점을 점검하여 제거하고 주기적으로 보안패치 실시
4. 불필요한 서비스 포트 제거

② 네트워크 장비의 접근기록은 6개월 이상 보관하고 비인가자의 침투 여부를 주기적으로 점검하여야 한다.

③ 분임정보보안담당자는 임직원의 원격접근을 허용하는 경우 사용시간, 접속자, 수행업무 등을 검토하여야 한다. <개정 2021.12.28.>

④ 업무망과 용역망의 경우 분리하여 운영하여야 한다.

제24조(전자우편 보안대책) ① 정보보안담당관은 웜·바이러스 등 악성코드로부터 직원의 전자우편 시스템 일체를 보호하기 위하여 백신, 방화벽, 악성메일 차단시스템 등의 보안대책을 강구하여야 한다. <개정 2021.12.28.>

② 사용자는 메일에 포함된 첨부파일이 자동 실행되지 않도록 설정하고 첨부파일 다운로드시 반드시 최신 백신으로 악성코드 은닉여부를 검사하여야 한다.

③ 직원은 출처가 불분명하거나 의심되는 제목의 전자우편은 열람하지 않고 악성메일로 의심되는 전자우편은 즉시 정보보안담당관에게 신고하여야 한다. <개정 2021.12.28.>

④ 사용자는 상용 전자우편을 이용한 업무자료를 송·수신 및 저장을 할 수 없으며 기관 전자우편으로 송·수신한 업무자료는 활용 후 메일함에서 즉시 삭제하여야 한다.

제25조(휴대용 저장매체 보안대책) ① 휴대용 저장매체 관리책임자(이하

‘관리책임자’라 한다)라 함은 각 팀별 휴대용 저장매체 관리상의 임무를 맡은 팀장을 말한다.

② 관리책임자는 휴대용 저장매체를 사용하여 업무자료를 보관할 필요가 있을 때에는 위변조, 훼손, 분실 등에 대비한 보안대책을 강구하여야 한다.

③ 관리책임자는 휴대용 저장매체를 비밀용, 일반용으로 구분하고 주기적으로 수량 및 보관 상태를 점검하며 반출·입을 통제하여야 한다.

④ 관리책임자는 USB 관리시스템을 도입할 경우 국가정보원장이 안전성을 확인한 제품을 도입하여야 한다.

⑤ 관리책임자는 사용자가 USB 메모리를 PC 등에 연결 시 자동실행 되지 않도록 하고 최신 백신으로 악성코드 감염여부를 자동 검사하도록 보안 설정하여야 한다.

⑥ 보안담당관은 비밀자료가 저장된 휴대용 저장매체는 매체별로 비밀등급 및 관리번호를 부여하고 비밀관리기록부에 등재 관리하여야 한다. 이 경우에는 매체 전면에 비밀등급 및 관리번호가 표시되도록 하여야 한다. <개정 2021.12.28.>

⑦ 관리책임자는 휴대용 저장매체를 파기 등 불용처리 하거나 비밀용을 일반용 또는 다른 등급의 비밀용으로 전환하여 사용할 경우 저장되어 있는 정보의 복구가 불가능 하도록 완전삭제 프로그램을 사용하여야 한다.

⑧ 관리책임자는 사용자의 휴대용 저장매체 무단 반출 및 미등록 휴대용 저장매체 사용 여부 등 보안관리 실태를 주기적으로 점검하여야 한다.

⑨ 그 밖에 명시되지 않은 사항은 국가 정보보안 기본지침의 「USB메모리 등 휴대용 저장매체 보안관리 지침」에 따른다.

제26조(악성코드 감염 방지대책) ① PC 등의 사용자는 웜·바이러스, 해킹프로그램, 스파이웨어 등 악성코드 감염을 방지하기 위하여 다음 각 호의 보안조치를 강구하여야 한다.

1. PC 등에서 사용하는 응용프로그램에 대한 보안패치 실시
2. 백신은 최신상태로 업데이트 및 상시 감시상태로 설정
3. 출처가 불분명한 응용프로그램 사용 금지
4. 업무상 불필요한 비인가 프로그램 사용 금지

② 분임정보보안담당자 또는 직원은 악성코드가 설치되거나 감염된 사실을 발견하였을 경우에 다음 각 호의 조치를 취하여야 한다. <개정 2021.12.28.>

1. 악성코드 감염원인 규명 등을 위하여 파일 임의삭제 등 감염 시스템 사용을 중지하고 전산망과 접속 분리
2. 악성코드의 감염확산 방지를 위하여 정보보안담당관에게 관련 사실 즉시 통보 <개정 2021.12.28.>

③ 정보보안담당관은 악성코드에 감염되어 피해가 심각한 경우 문화체육관광부(정보화담당관, 사이버안전센터), 국가정보원 등 유관기관에게 통보하여야 한다. <개정 2021.12.28.>

제27조(접속기록 관리) ① 분임정보보안담당자는 정보시스템의 효율적인 통제 · 관리, 사고 발생 시 추적 등을 위하여 접속기록을 유지 · 관리하여야 한다. <개정 2021.12.28.>

② 제1항의 접속기록에는 다음 각 호의 내용이 포함되어야 한다.

1. 접속자, 정보시스템 · 응용프로그램 등 접속 대상
2. 로그 인 · 아웃, 파일 열람 · 출력 등 작업 종류, 작업 시간
3. 접속 성공 · 실패 등 작업 결과
4. 전자우편 외부발송 정보 등

③ 접속기록 분석 시, 비인가자의 접속 시도, 정보 위변조 및 무단 삭제 등의 의심스러운 활동 사실을 발견한 경우 정보보안담당관에게 즉시 보고하여야 한다. <개정 2021.12.28.>

④ 접속기록은 최소 1년 이상 보관하여야 하며 위 · 변조 및 외부유출 방지 대책을 강구하여야 한다. <개정 2021.12.28.>

제28조(정보시스템 개발환경 보안) ① 분임정보보안담당자는 정보시스템을 자체적으로 개발하고자 하는 경우 다음 각 호의 보안대책을 수립하여야 한다. <개정 2021.12.28.>

1. 독립된 개발시설을 확보하고 비인가자의 접근 통제

2. 개발시스템과 운영시스템의 물리적 분리
3. 소스코드 관리 및 소프트웨어 보안관리

② 외부용역 업체와 계약하여 정보시스템을 개발하는 경우 제36조, 제37조, 제38조, 제39조, 제40조에 따라 보안대책을 강구하여야 한다.

제29조(데이터베이스 보안) ① 데이터베이스의 추가, 변경, 삭제 권한은 소수의 인가자로만 제한되도록 운영하여야 한다.

② 분임정보보안담당자는 정보의 중요도에 따라 사용자 접근권한을 부여하고, 모니터링 하여야 한다. <개정 2021.12.28.>

③ 분임정보보안담당자는 사용자별 접속기록을 관리하여야 하며 제27조(접속기록 관리)에 따라 보안대책을 강구하여야 한다. <개정 2021.12.28.>

④ 정보보안담당관은 주기적으로 보안점검을 수행하여야 한다. <개정 2021.12.28.>

제30조(정보시스템 유지보수) ① 분임정보보안담당자는 정보시스템 유지보수 수행업체에 대하여 다음 각 호의 보호대책을 강구하여야 한다. <개정 2021.12.28.>

1. 투입인력 보안서약서, 교육 등 인적 보안관리
2. 물리적 출입통제
3. 정보시스템 접근통제
4. 주기적인 정보보안 점검 등

② 분임정보보안담당자는 유지보수 절차에 따라 정기점검을 수행하고 기록하여야 한다. <개정 2021.12.28.>

③ 분임정보보안담당자는 유지보수와 관련된 장비 · 도구 등을 반 · 출입할 경우, 악성코드 감염여부, 자료 무단반출 여부를 확인하는 등의 보안조치를 하여야 한다. <개정 2021.12.28.>

④ 외부에서 원격으로 유지보수를 수행할 경우에는 별지 5호에 따라 접근제어시스템 등 보안대책(별지 16호 보안서약서 징구)을 강구한 후 한시적으로 허용한다.

제31조(전자정보 저장매체 불용처리) ① 분임정보보안담당자는 하드디스크 등

전자정보 저장매체를 불용처리(교체 · 반납 · 양여 · 폐기 등)할 경우 저장매체에 수록된 자료가 유출되지 않도록 보안대책을 강구하여야 한다. <개정 2021.12.28.>

② 자료의 삭제는 해당 정보가 복구될 수 없도록 저장매체별, 자료별 차별화된 삭제방법을 적용하여야 한다.

③ PC 등의 사용자가 변경된 경우, 비밀처리용은 완전포맷 3회 이상, 그 외는 완전포맷 1회 이상으로 저장자료를 삭제하여야 한다.

④ 정보시스템 저장자료의 삭제를 외부업체에 의뢰할 경우 작업 장소에 입회하여 삭제 절차 및 방법의 준수여부 등을 확인·감독하여야 한다.

⑤ 정보시스템을 외부로 반출시 다음 각 호의 보안조치를 하여야 한다.

1. 불용처리 등을 위해 정보시스템을 외부로 반출할 경우 현황을 기록 유지
2. 저장매체의 고장수리·저장자료 복구 등을 외부에 의뢰할 경우 저장매체에 저장된 자료의 유출 방지를 위해 수리 또는 복구 참여자에 대해 보안서약서 징구, 교육 등 필요한 보안조치 수행
3. 정보시스템을 불용 처리할 경우 당해 시스템의 부서·사용자 등을 인식할 수 있는 표시를 모두 제거

제32조(무선인터넷 보안관리) ① 보안담당관은 무선인터넷(NESPOT, Wibro, HSDPA 등) 시스템을 구축하여 업무자료를 소통하고자 할 경우 자체 보안대책을 수립하여 관련 사업계획단계(사업공고 전)에서 문화체육관광부장관을 통해 국정원장에게 보안성 검토를 의뢰하여야 한다. <개정 2021.12.28.>

② 정보보안담당관은 기관 전역에 무선인터넷 사용을 제한하고 민원실 등 외부인에게 특별히 무선인터넷 사용이 필요한 구역에 한해 보안담당관 책임 하에 운용한다. <개정 2021.12.28.>

③ 정보보안담당관은 업무용PC에서 무선인터넷 접속장치(USB형 등)가 작동되지 않도록 관련 프로그램 설치 금지 등 기술적 보안대책을 강구하여야 한다. <개정 2021.12.28.>

④ 보안담당관은 개인 휴대폰을 제외한 무선인터넷 단말기의 사무실 무

단 반입·사용을 금지하는 한편 제1항부터 제3항까지와 관련한 보안대책의 적절성을 수시로 점검하고 보완하여야 한다. <개정 2021.12.28.>

제33조(보안 프로그램 설치·운영) 정보보안담당관은 사용자 PC 등의 안정성을 강화하기 위하여 다음 각 호의 보안프로그램 설치 및 운용방안을 강구할 수 있다. <개정 2021.12.28.>

1. 바이러스백신 소프트웨어
2. 패치관리 소프트웨어

제 3 절 주요상황별 보안대책

제34조(정보시스템 위탁운영 보안관리) ① 분임정보보안담당자는 정보시스템 위탁운영 시 관리적·물리적·기술적 보안대책을 수립하여 시행하여야 한다. <개정 2021.12.28.>

② 정보시스템의 위탁 운영은 외주업체 직원이 진흥원에 상주하여 수행하여야 한다. 다만, 진흥원 위탁업무 수행 직원의 상주가 불가한 사유가 있을 경우, 관련 보안대책을 수립·시행하는 조건으로 그러하지 아니할 수 있다.

③ 분임정보보안담당자는 정보화용역사업 보안대책에 대한 이행실태를 주기적으로 점검하고 미비점 발견 시 보완 조치하여야 한다. <개정 2021.12.28.>

제35조(원격근무 보안관리) ① 분임정보보안담당자는 재택·파견·이동근무 등 원격 근무를 지원하기 위한 정보시스템을 도입·운영할 경우 정보보안담당관과 협의하여 기술적·관리적·물리적 보안대책을 수립하여야 한다. <개정 2021.12.28.>

② 원격근무자는 해킹을 통한 업무자료 유출방지를 위하여 최신 백신으로 원격근무용 PC 등을 점검하고 업무자료 저장금지 등 보안조치 후 사용하여야 한다.

제 4 절 정보화용역사업 관리

제36조(용역사업 계획단계) ① 분임정보보안담당자는「국가계약법」시행령 제76조 제1항 제18호에 따라 용역사업 추진 시 과업지시서·입찰공고·계약서에 다음 각 호의 누출금지 대상정보를 명시하며 해당정보 누출 시 입찰 참가자격 제한을 위한 부정당업자로 등록하여야 한다. <개정 2021.12.28.>

1. 진흥원 소유 정보시스템의 내·외부 IP주소 현황
2. 세부 정보시스템 구성 현황 및 정보통신망 구성도
3. 사용자계정·비밀번호 등 정보시스템 접근권한 정보
4. 정보통신망 취약점 분석·평가 결과물
5. 정보화 용역사업 결과물 및 관련 프로그램 소스코드(유출시 안보·국익에 피해가 우려되는 중요 용역사업에 해당)
6. 정보보호시스템 도입 현황
7. 침입차단시스템·방지시스템(IPS) 등 정보보호제품 및 라우터·스위치 등 네트워크 장비 설정 정보
8. 「공공기관의 정보공개에 관한 법률」제9조 제1항에 따라 비공개 대상 정보로 분류된 기관의 내부문서
9. 「개인정보보호법」제2조 제1호의 개인정보
10. 기타 보안담당관이 공개가 불가하다고 판단한 자료 <개정 2021.12.28.>

② 분임정보보안담당자는 사업수행을 위한 제안요청서 및 계약서에 참가직원의 보안준수 사항과 보안 위규자 처리기준 및 위약금 부과기준을 명시할 수 있다. <개정 2021.12.28.>

③ 분임정보보안담당자는 제안평가요소에 자료·장비·네트워크 보안대책 등 보안관리 계획의 평가항목 및 배점기준을 마련하여야 한다. <개정 2021.12.28.>

제37조(용역사업 입찰·계약단계) ① 분임정보보안담당자는 입찰 공고 시 누출금지대상정보, 부정당업자 제재조치, 기밀유지 의무 및 위반 시 불이익 등 보안준수사항을 공지하여야 한다. <개정 2021.12.28.>

② 분임정보보안담당자는 제안업체가 제시한 보안관리 계획의 타당성을 검토하여 사업자 선정 시 반영하여야 한다. <개정 2021.12.28.>

③ 분임정보보안담당자는 사업에 투입되는 자료·장비 등에 대해 대외 보안이 필요한 경우 보안의 범위·책임을 명확히 하기 위하여 사업수행 계약서와 별도로 비밀유지계약서를 작성하여야 한다. 비밀유지계약서에는 비밀정보의 범위, 보안준수 사항, 위반 시 손해배상 책임, 지적재산권 문제, 자료의 반환 등이 포함되도록 명시하여야 한다. <개정 2021.12.28.>

④ 분임정보보안담당자는 외부용역을 추진할 경우 사업 책임자로 하여금 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다. <개정 2021.12.28.>

1. 용역사업 계약서에 참가직원의 보안준수사항과 위반 시 손해배상 책임 등 명시
2. 용역사업 수행 관련 보안교육·점검 및 용역기간 중 참여인력 임의 교체 금지
3. 정보통신망도·IP주소현황 등 용역업체에 제공할 자료는 인계인수 대장을 비치, 보안조치 후 인계·인수하고 무단 복사 및 외부반출 금지
4. 사업 종료시 외부업체의 노트북·휴대용 저장매체 등을 통해 비공개 자료가 유출되는 것을 방지하기 위하여 복구가 불가능하도록 완전 삭제
5. 용역업체로부터 용역 결과물을 전량 회수하고 비인가자에게 제공·열람 금지
6. 용역업체의 노트북 등 관련 장비를 반출·반입시마다 악성코드 감염 여부, 자료 무단반출 여부를 확인
7. 기타, 보안담당관이 보안관리가 필요하다고 판단하는 사항이나 국정원장이 보안조치를 권고하는 사항 <개정 2021.12.28.>

⑤ 분임정보보안담당자는 용역업체가 사업의 일부 또는 전부에 대하여 하도급 계약을 체결하는 경우에 용역업체로 하여금 하도급 계약서에 본 사업계약 수준의 비밀유지 조항을 포함하도록 조치하여야 한다. <개정 2021.12.28.>

⑥ 분임정보보안담당자는 용역사업에 대한 보안관리를 위하여 사업관리 담당과 보안관리담당을 분리하여야 한다. 다만, 사업규모가 작아 분리가

곤란한 경우에는 사업관리담당이 병행할 수 있다. <개정 2021.12.28.>

제38조(용역사업 수행단계) ① 분임정보보안담당자는 참여인원에 대하여 다음 각 호에 따라 관리하여야 한다. <개정 2021.12.28.>

1. 용역사업의 참여인력에 대하여 보안서약서 징구
2. 용역업체 참여인원에 대해 법적 또는 발주기관 규정에 따른 비밀유지 의무준수 및 위반 시 처벌 내용 등에 대한 보안교육
3. 사업수행 중 업체 인력에 대한 보안점검 실시
4. 제36조 제1항의 “누출금지대상정보” 외부 유출여부 확인
5. 비밀관련 용역사업을 수행할 경우, 참여인원에 대한 비밀취급인가 등 보안조치를 수행하고 정보보안담당관에게 보안측정을 요청 <개정 2021.12.28.>

② 정보보안담당관은 용역업체에게 자료를 제공하거나 용역사업수행 중에 생산된 산출물에 대하여 다음 각 호에 따라 관리하여야 한다. <개정 2021.12.28.>

1. 계약서 등에 명시한 누출금지 대상정보를 업체에 제공할 경우 별지 제15호에 의한 인수자료 관리대장을 작성, 인계자・인수자가 직접 서명한 후 제공하고 사업완료시 관련자료 회수
2. 용역사업 관련자료 및 사업과정에서 생산된 산출물은 발주기관의 파일서버에 저장하거나 사업의 보안담당이 지정한 PC에 저장・관리
3. 용역사업 관련 자료는 인터넷 웹하드・P2P 등 인터넷 공유사이트 및 개인메일함에 저장을 금지하고 용역발주기관과 용역업체간 전자우편을 이용해 자료전송이 필요한 경우에는 자체 전자우편을 이용, 첨부자료 암호화 수발신
4. 진흥원 사무실에서 용역사업을 수행할 경우, 제공한 비공개 자료는 매일 퇴근 시 반납하고 비밀문서를 제외한 일반문서는 시건장치가 된 보관함에 보관
5. 용역사업 수행으로 생산된 산출물 및 기록은 보안담당관이 인가하지 않은 비인가자에게 제공・대여・열람 금지 <개정 2021.12.28.>

③ 분임정보보안담당자는 용역사업을 수행하는 사무실과 장비에 대하여

다음 각 호에 따라 관리하여야 한다. <개정 2021.12.28.>

1. 시건장치가 구비되고 비인가자 출입통제가 가능한 사무실 사용
2. 용역업체의 사무실과 인원·장비를 대상으로 정기적으로 보안점검 실시
3. 진흥원 내부에서 용역사업을 수행하는 경우 용역 참여직원이 노트북 등 관련 장비를 외부에 반출·입시마다 악성코드 감염여부 및 자료 무단반출 여부 확인
4. 인가받지 않은 USB 등 휴대용 저장매체 사용을 금지하며 산출물 저장을 위하여 휴대용 저장매체가 필요한 경우 사업 보안관리담당의 승인하에 사용

④ 분임정보보안담당자는 용역업체가 이용하는 전산망에 대하여 다음 각 호에 따라 관리하여야 한다. <개정 2021.12.28.>

1. 용역업체 사용전산망은 방화벽 등을 활용하여 내부망과 분리하고 업무상 필요한 서버에만 제한적 접근
2. 사업 참여 인원에 대한 사용자 계정은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 차등 부여하되 진흥원 내부문서 접근 금지하고 불필요 시 곧바로 권한을 해지하거나 계정을 폐기
3. 참여인원에게 부여한 비밀번호는 사업 보안관리담당이 별도로 기록·관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력 확인
4. 용역사업 보안관리담당은 서버 및 장비운영자로 하여금 내부서버 및 네트워크 장비에 대한 접근 기록을 매일 확인하여 이상 유무 보고
5. 용역업체에서 사용하는 PC 등은 인터넷 연결을 금지하되, 사업수행상 연결이 필요한 경우에는 발주기관의 보안통제 하에 제한적 허용
6. 발주기관 및 용역업체 전산망에서 P2P, 웹하드 등 인터넷 자료공유 사이트로의 접속을 방화벽 등을 이용해 원천차단

제39조(용역사업 종료단계) ① 분임정보보안담당자는 최종 용역산출물 중 대외보안이 요구되는 자료는 대외비 이상으로 작성·관리하고 불필요한 자료는 반드시 삭제 및 폐기하여야 한다.

② 분임정보보안담당자는 용역업체에 제공한 자료·장비·문서 및 중간·

최종산출물 등 사업 관련 제반자료를 확인하여 전량 회수하며, 업체에 복사본 등 별도 보관을 금지시켜야 한다.

③ 분임정보보안담당자는 사업완료 후 업체 소유 PC·서버의 하드디스크·휴대용저장매체 등 전자기록 저장매체는 국가정보원장이 안전성을 검증한 삭제 S/W로 완전 삭제 후 반출하여야 한다.

④ 분임정보보안담당자는 제2항의 용역사업 관련자료 회수 및 삭제조치 후에 용역업체가 용역산출물의 복사본 등 용역사업 관련 자료를 보유하고 있지 않다는 용역업체 대표명의 보안확약서를 징구하여야 한다.

제40조(용역사업 보안관리실태 점검) 보안담당관은 정보화용역사업 관련 규정에서 정한 보안대책에 대한 이행실태를 주기적으로 점검하여야 한다. <개정 2021.12.28.>

제41조 (정보화심의위원회) ① 정보화업무의 효율적인 운영과 업무계획의 수립 및 기타 정보화에 관한 중요한 사항을 심의하기 위하여 정보화심의위원회(이하 “위원회”라 한다)를 둔다.

② 위원회는 다음 각 호의 사항을 심의한다.

1. 우리원 정보화 전략계획 수립에 관한 사항
2. 우리원 정보화 전략계획 사업추진 예산의 적절성 평가
3. 기타 정보화추진 업무 수행 상 조정과 협의를 요하는 사항

③ 위원회는 위원장 1명과 4명 이내의 위원으로 구성하며, 위원장은 전산업무담당 본부장으로 하고 위원은 정보보안담당관 및 원장이 위촉하는 관계분야 전문가 3명 이내로 한다.

④ 부서에서 추진하는 개별 정보화 사업은 해당 사안에 대한 과업심의위원회를 통해 예산과 사업추진의 적정성을 심의한다.

⑤ 위촉위원의 임기는 2년으로 하되 연임할 수 있다. 다만, 원장이 필요하다고 인정되는 경우에는 임기 만료전이라도 위원을 교체할 수 있으며, 교체된 위원의 임기는 전임 위원의 남은 기간으로 한다.

⑥ 위원회는 간사 1명을 두며 간사는 정보화업무 담당부서의 직원이 한다.

⑦ 위원회 회의는 위원장이 필요하다고 인정할 때 또는 위원 과반수의

요구가 있을 때 이를 소집한다.

⑧ 위원회의 소집이 곤란하거나 긴급을 요할 경우에는 서면심의를 할 수 있다.

⑨ 위촉한 위원에게는 우리원 평가(심의) 수당 지급 기준에 의해 수당을 지급한다.

⑩ 위원은 직무상 취득한 비밀에 대해서는 재임 중은 물론 퇴임 후에도 비밀을 엄수하여야 한다.

⑪ 위원장 또는 위원이 일신상의 이유로 심의를 수행할 수 없는 경우 5명의 위원회를 유지하기 위해 관계분야 전문가풀의 전문가를 위촉하여 해당사안에 대해 심의할 수 있다.

[본조신설 2021.12.28]

부 칙

이 지침은 원장의 승인을 받은 날부터 시행한다.

부 칙(2021.12.28.)

이 지침은 원장의 승인을 받은 날부터 시행한다.

<별지 제1호>

정보보안업무 세부 추진계획

1. 활동 목표

2. 기본방침

3. 세부 추진계획

분야별	사업명	세부 추진계획	주관·관련부서	비고

※ 보안성검토 대상여부 표기

4. 전년도 보안감사 · 지도방문 시 도출내용과 조치내역

도 출 내 용	조 치 내 역	담 당 부 서

※ 형식위주의 계획수립을 지양하고 소속기관의 추진계획을 종합, 자체 실정에 맞게 작성

<별지 제2호>

정보보안업무 심사분석

1. 총 평

2. 주요 성과 및 추진사항

3. 세부 사업별 실적 분석

추 진 계 획	추 진 실 적	문 제 점	개 선 대 책

※ 추진실적은 목표량과 대비하여 성과 달성도를 계량화

4. 부진(미진)사업

부 진 사 업	원인 및 이유	익년도 추진계획

5. 애로 및 건의사항

6. 첨부(정보통신망 및 정보보호시스템 운용현황 등)

〈별지 제3호〉

정보시스템(PC · 노트북 등) 관리대장

〈관리책임자 : 각 팀장〉

연번	소속	취급자 (성명)	종류 (PC•노트북 등)	관리번호	도입일자	IP

〈별지 제4호〉

정보시스템(PC · 노트북 등) 반출 · 입 대장

〈관리책임자 : 각 팀장〉

장비명	관리번호 (시리얼번호)	사용자	용도	전출입 일시 (입•출 구분)	확인

<별지 제5호> <개정 2021.12.28.>

계정발급(삭제) 신청서(접근제어 신청서)

작성자	팀장	정보보안 담당자	정보보안 담당관

[신청 정보]

소속사		부서/팀명	
성 명		전화번호	
e-Mail		신청일자	
신청근거			

[세부 내역]

구 분			내 용
신청 구분			□ 신규 □ 연장 □ 삭제 요청
작업자	사용자 ID		
서버 접근 허용 대상	목적지 주소 (Destination IP Address)		
	접근 서버	포트	
신청 기간			
사용 용도			
조치사항			

〈별지 제6호〉

사용자계정 관리대장(접근제어사용자관리대장)

No.	회사명	사용자 그룹	사용자명	사용자 ID	사용자 권한	등록일자	계정사용 만료일자

〈별지 제7호〉

관리자계정(비밀번호) 관리대장

담당자	관리자

No.	시스템명	분류	위치	ID	Password	관리자(성명)

<별지 제8호> <개정 2021.12.28.>

VPN 허용신청서

작성자	팀장	정보보안 담당자	정보보안 담당관

[신청 정보]

소 속		부서/팀명	
성 명		전화 번호	
신청 일자			

[세부 내역]

구 분	내용
신청 구분	□ 신규 □ 재발급 □ 기간연장 □ 삭제
사용 기간	
접속 대상 VPN	□ VPN (http://vpn.kocca.kr) ※ win8 이상 미지원 □ VPN2 (https://vpn2.kocca.kr:10443)
아이디	
신청사유	

[조치 결과]

조치사항 (IDC담당자가 기재)	

<별지 제9호> <개정 2021.12.28.>

상용 메일 허용신청서

작성자	팀장	정보보안 담당자	정보보안 담당관

[신청 정보]

소 속	KOCCA	부서/팀명	
성 명		전화 번호	
신청 일자			

[세부 내역]

구 분	내용
신청구분	□ 신규 □ 기간 연장 □ 삭제
사용기간	. . . ~ . . .
상용메일	□ 네이버 □ 네이트 □ 다음 □ 지메일 □ 기타 ( )
신청 IP (사용자IP)	
신청사유	

[조치 결과]

조치사항 (IDC담당자가 기재)	

<별지 제10호> <개정 2021.12.28.>

네임서버 도메인등록(변경)신청서

작성자	팀장	정보보안 담당자	정보보안 담당관

[신청 정보]

서비스명		부서/팀명	
성 명		전화번호	
신청일자		서비스담당자	

[세부 내역]

구 분	내 용
신청 구분	□ 신규 □ 서비스 수정 □ 일시중단 □ 서비스종료
서비스 URL	
서비스	□ WEB □ WAS □ DBMS □ SSL □ 휴대폰 본인인증 □ IPIN 본인인증 □ 공인인증 □ DNS
서버 위치	□ IDC □ 문화정보원 □ 기타 외부( )
서비스 운영 조직	□ IDC 운영팀 □ 외부 ( )
서비스 기간	
백업 보존기간	□ 1 년 □ 2 년 □ 기타 ( )
개인정보 보유여부	□ ○ □ X
조치사항	

<별지 제11호> <개정 2021.12.28.>

방화벽 정책등록 신청서

작성자	팀장	정보보안 담당자	정보보안 담당관

[신청 정보]

소속사		부서/팀명	
성 명		전화번호	
e-Mail		신청일자	
신청근거			

[세부 내역]

구 분			내 용
신청 구분			□ IP 신규 □ Port 허용 □ 삭제 요청
작업IP	출발지 주소 (Source IP Address)		
포트 허용 대상	목적지 주소 (Destination IP Address)		
	요청 포트	TCP Port	
		UDP Port	
신청 기간			
사용 용도			
조치사항			

<별지 제12호>

휴대용 저장매체 관리대장(일반용)

<관리책임자 : 각 팀장>

연번	관리번호 (S / N)	매체형태	등록일자	취급자	불용처리일자	불용처리방법 (재사용 용도)	비고

〈별지 제13호〉

휴대용 저장매체 관리대장(비밀용)

〈관리책임자 : 각 팀장〉

연번	관리번호 (S / N)	등급	매체형태	등록일자	취급자	불용처리일자	불용처리방법 (재사용 용도)	비고 (사유)

〈별지 제14호〉

휴대용 저장매체 반출·입 대장

〈관리책임자 : 각 팀장〉

장비명	관리번호 (시리얼번호)	사용자	용도	전출입 일시 (입•출 구분)	비고

〈별지 제15호〉

인수자료 관리대장

No.	인수자료 목록	인수일자	구분	담당자	용역업체 담당자
		. . .	문서		
			파일		

〈별지 제16호〉

보 안 서 약 서

본인은 년 월 일부로 과 관련한 업무(연구, 개발, 제작, 입찰, 기타)를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 나는 과 관련된 소관업무가 기밀 사항임을 인정하고 제반 보안관계규정 및 지침을 성실히 수행한다.
2. 나는 이 기밀을 누설함이 국가이익을 침해할 수도 있음을 인식하고 재직 중은 물론 퇴직 후에도 알게 된 모든 기밀사항을 일체 타인에게 누설하지 아니한다.
3. 나는 기밀을 누설한 때에는 아래의 관계법규에 따라 엄중한 처벌을 받을 것을 서약한다.

가. 전자정부법 제35조(금지행위) 및 제76조(벌칙)

년 월 일

서약자
소 속 :
직 급 :
직 위 :
생 년 월 일 :
성 명 : (날인 또는 서명)

한국콘텐츠진흥원 귀하

〈별지 제17호〉

보 안 확 약 서

본인은 귀 기관과 계약한 의 수행을 완료함에 있어, 다음 각 호의 보안사항에 대한 준수 책임이 있음을 서약하며, 이에 확약서를 제출합니다.

1. 본 업체는 업체 및 사업 참여자가 사업수행 중 취득한 모든 자료를 반납 및 파기하여 복사본 등 용역사업 관련 자료를 보유하지 않으며, 취득한 정보에 대한 유출을 절대 금지하겠습니다.
2. 본 업체는 하도급업체에 대해 상기 항과 동일한 보안사항 준수 책임을 확인하고 보안확약서를 징구하였으며, 하도급업체가 위의 보안사항을 위반할 경우에 주사업자로서 이에 동일한 법적 책임을 지겠습니다.
3. 본 업체는 상기 보안사항을 위반할 경우에 귀 기관의 사업에 참여 제한 또는 기타 관련 법규에 따른 책임과 손해배상을 감수하겠습니다.

년 월 일

서약자 (대표자)

상 호 :

사업자등록번호 :

생 년 월 일 :

성 명 : (날인 또는 서명)

한국콘텐츠진흥원 귀하