정보보안 업무요령

제정 2014. 7. 23

제1장 총칙

제1조(목적) 이 요령은 중소기업기술정보진흥원(이하 "기정원"이라 한다)의 「보안규정」에서 위임한 사항과 그 시행에 필요한 절차와 세부사항 규정함을 목적으로 한다.

제2조(적용범위) 기정원의 정보보안 업무는「국가 사이버안전 관리규정」, 「국가 정보보안 기본지침」, 그 밖에 정보보안 관계 법령 및 지침·기준·가이드에서 정한 사항을 제외하고는 이 요령에서 정한 바에 따른다.

제3조(용어의 정의) 이 요령에서 사용하는 용어의 뜻은 다음과 같다.

1. “정보보안책임자”란 정보보안 조직을 지휘하고 정보보안 업무를 총괄하기 위해 직제규정의 업무분장표에 따른 업무담당 부서장을 말한다.
2. “정보보안관리자”란 정보보안 업무를 수행하기 위해 정보보안책임자가 지정한 업무담당자를 말한다.
3. “시스템관리자”란 기정원의 전산실 및 정보시스템 운영을 담당하는 업무담당자를 말한다.
4. “정보시스템 운영책임자”란 업무 수행을 위해 구축·운영하는 정보시스템별 운영책임자로써, 소관 부서의 장을 말한다.
5. “정보시스템 운영자”란 부서별 정보시스템 운영책임자가 지정한 정보시스템 운영 실무 담당자를 말한다.
6. “정보통신망”이란 「전기통신기본법」 제2조 제2호에 따른 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송수신하는 정보 통신체제를 말한다.
7. “업무전산망”(이하 “내부망”이라 한다)이란 기정원의 네트워크 중에서 내부 업무용으로 사용되는 영역으로 인터넷서비스도 병행 제공되는 내부전산망을 말한다.

8. “정보시스템”이란 PC·서버 등 단말기, 보조기억매체, 전산·통신장치, 정보통신기기, 응용프로그램 등 정보의 수집·가공·저장·검색·송수신에 필요한 하드웨어 및 소프트웨어 일체를 말한다.
9. “저장매체”라 함은 자기저장장치·광 저장장치·반도체 저장장치 등 자료기록이 가능한 전자장치를 말한다.
10. “휴대용 저장매체”란 디스켓·CD·USB메모리 등 정보를 저장할 수 있는 것으로 PC 등의 정보시스템과 분리하여 이동이 가능한 기억장치를 말한다.
11. “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 행위를 말한다.
12. “전자문서”란 컴퓨터 등 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 정보를 말한다.
13. “전자기록물”이란 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 기록정보자료를 말한다.
14. “전자정보”란 업무와 관련하여 취급하는 전자문서 및 전자기록물을 말한다.
15. “정보자산”이란 하드웨어(서버, 워크스테이션, 개인용컴퓨터, 통신장비, 보안장비, 저장매체, 프린터 등), 소프트웨어, 응용프로그램, 개발산출물, 운영산출물 등을 말한다.
16. “정보보안시스템”이란 정보의 수집·저장·검색·송신·수신시 정보의 유출, 위·변조, 훼손 등을 방지하기 위한 하드웨어 및 소프트웨어를 말한다.
17. “사이버공격”이란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스방해 등 전자적 수단에 의하여 정보통신망을 불법침입·교란·마비·파괴하거나 전자정보를 절취·훼손하는 공격 행위를 말한다.
18. “완전포맷”이란 저장매체 자료저장 전체의 위치에 새로운 자료(0 또는 1)를 중복하여 저장하는 것을 말한다.
19. “관리자계정”이란 정보시스템에서 제공하는 모든 기능과 데이터에 접근할 수 있는 최상위 권한이 부여된 계정을 말한다.
20. “사용자계정”이란 정보시스템에서 제공하는 일부 기능과 데이터에 접근할 수 있도록 제한적으로 권한이 부여된 계정을 말한다.

제4조(기본원칙) ① 우리 원 고유 업무수행으로 발생된 정보자산은 기정원 소유이며, 관리는 각 부서 단위로 한다.

② 기정원 정보자산은 업무상 필요한 최소한의 접근권한이 부여되어야 한다.

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

제2장 정보보안 기본활동

제5조(정보보안 조직의 운영) 정보보안책임자는 다음 각 호의 업무를 수행하기 위하여 정보보안관리자, 시스템관리자를 지정하여 운영할 수 있다. 정보보안책임자에 부여하는 기본활동은 다음 각 호와 같다.

1. 정보보안 정책 및 기본계획 수립·시행
2. 정보보안 관련 규정·요령 등 제·개정
3. 보안심사위원회에 정보보안 분야 안건 심의 주관
4. 정보보안 업무 관리·감독
5. 정보통신실(전산실), 정보통신망 및 정보자료 등의 보안관리
6. 정보보안 관리실태 평가(별지 제1호)
7. 사이버공격 대응 및 조치활동
8. 정보보안 교육 및 정보협력

제6조(정보보안 교육) ① 정보보안책임자는 정보보안 교육계획을 수립하여 정보시스템 운영자 및 직원을 대상으로 관련 교육을 실시하여야 한다.

② 정보보안책임자는 정보보안 관련 전문기관 교육 및 기술 세미나 참석을 장려하는 등 정보보안관리자의 전문성을 제고하기 위하여 노력하여야 한다.

제7조(사이버보안진단의 날) ① 매월 세 번째 수요일을 '사이버보안진단의 날'로 지정·운영하여야 한다.

② 정보보안관리자는 '사이버보안진단의 날'에 소관 정보통신망 악성코드 감염여부, 정보시스템 보안 취약점 점검 등 정보보안 업무 전반에 대하여 보안진단을 실시하여야 한다.
③ 정보보안책임자는 제1항 및 제2항에 따른 보안진단 결과를 게시할 수 있고, 개인 및 부서평가에 활용할 수 있다.

제8조(정보보안 사고 조사) ① 정보보안책임자는 정보보안 사고 발생시 즉시 피해확산 방지조치를 취하여야 한다.
② 정보보안책임자는 사고원인 및 피해 현황을 파악하고, 재발방지 대책의 수립·시행 등 사고조사 결과에 따라 보호대책을 마련하고 조치하여야 한다.

제9조(정보시스템 현황·자료 관리) 정보시스템별 운영책임자는 해당 정보시스템의 현황·자료를 관리하여야 하며, 정보보안책임자의 요청시 관련 자료를 제출하여야 한다.
1. 정보시스템 이용현황(개인회원 수, 기업(관)회원 수)
2. 정보시스템 접속현황(일, 월, 년 단위 접속통계)
3. 정보시스템 구성현황(H/W, S/W(개발, 상용))
4. 정보시스템 구축·운영비 현황(초기구축, 업그레이드, 유지보수 비용)

제3장 정보통신시설 및 정보시스템 보안관리

제10조(정보통신시설 보안) ① 정보보안책임자는 「보안규정」 제10조에 따라 정보통신시설 및 장소를 보호구역으로 지정하여 관리하여야 한다.
② 제1항에서 지정된 보호구역에 대한 보안 대책을 강구할 경우 다음 각 호의 사항을 조치하여야 한다.
1. 정보통신시설에 대한 방호 및 방재대책
2. 출입자 인증·식별 등을 위한 출입문 보안장치 설치
3. 정전에 대비한 비상전원 공급, 시스템의 안정적 중단 등 전력관리 대책
4. 비인가자에 대한 출입 및 정보자산의 반·출입 통제

제11조(정보시스템 보안) 정보보안책임자는 다음 각 호에 명시된 정보시스템 운용과 관련한 보안취약점을 발견하거나 보안대책 강구가 필요하다고 판단할 경우, 개선을 요구할 수 있다.

1. 사용자는 PC 등 정보시스템을 사용하거나 본인 계정으로 정보통신망에 접속하는 것과 관련한 보안책임을 가진다.
2. 정보보안관리자는 서버·네트워크 장비 등 부서 공통으로 사용하는 정보시스템의 운용과 관련한 보안책임을 가진다.
3. 정보시스템 운영책임자는 소관 시스템의 운용과 관련된 보안책임을 가진다.

제12조(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 제17조 "사용자계정 관리"와 제18조 "비밀번호 관리"의 규정을 준용한다.

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

1. 부팅 시 비밀번호 설정
2. 최대 10분을 초과하지 않도록 화면보호기 설정
3. IP주소 임의변경 금지
4. 최신 보안업데이트, 백신 프로그램 등 보안프로그램 설치 및 주기적 검사

④ 정보보안관리자는 비인가자가 PC 등을 무단으로 조작하여 전자정보를 유출하거나, 위·변조 및 훼손시키지 못하도록 다음 각 호에 따른 보호대책을 강구하여야 한다.

1. 제18조에 따라 장비별·사용자별 비밀번호 설정 관리
2. 백신, 자료유출방지시스템, 패치관리시스템 등의 운용
3. P2P 등 업무와 무관하거나 보안에 취약한 프로그램의 사용 금지

⑤ 자산관리 주관부서는 PC 등을 교체·반납·폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 하드디스크에 수록된 자료가 유출, 훼손되지 않도록 보안조치를 수행하고, 정보보안관리자 요청시 결과를 제출하여야 한다.

제13조(업무용 PC 사용제한) 정보보안책임자는 업무용 PC에서 내부 정보 유출 가능성이 있는 다음 각 호에 해당하는 경우 서비스를 차단할 수 있다.

1. 침입차단시스템을 우회하여 접속하는 프로그램을 이용하여 서비스를 연결할 경우
2. 외부 웹하드 등에 파일 업로드를 시도하는 경우
3. 비업무용사이트(게임, 증권, 음악 사이트 등)에 접속할 경우
4. 그 밖에 정보보안을 위하여 서비스 차단이 필요하다고 판단되는 경우

제14조(서버 보안관리) ① 정보시스템 운영책임자는 서버 증설·교체시, 정보보안관리자와 협의하여 다음 각 호의 보안대책을 수립하고 시행하여야 한다.

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 접속시 내부망 IP 주소가 부여된 관리용 단말기 지정
6. 서버 설정정보 및 저장된 자료의 정기적 백업

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

제15조(웹서버 등 공개서버 보안관리) ① 시스템관리자는 외부인에게 공개할 목적으로 설치하는 공개서버에 대해 홈페이지 위변조, 분산서비스거부(DDoS)공격 등으로부터 보호하기 위한 다음 각 호의 보안대책을 수립하여 시행하여야 한다.

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 정보보안관리자는 공개서버의 보안취약점을 수시로 점검하고, 홈페이지 위변조, 분산서비스거부(DDoS)공격, 악성코드, 민감정보의 위·변조 및 훼손 여부를 확인하여야 한다.

제16조(홈페이지 게시자료 보안관리) ① 정보보안책임자는 개인정보를 포함한 중요 업무자료가 홈페이지에 무단 게시되지 않도록 별지 제2호에 따라 정보등록절차를 마련하여 시행하여야 한다.

② 정보시스템 운영책임자는 개인정보, 비공개 문서, 민감정보 등이 포함된 자료를 홈페이지에 공개하여서는 아니 된다.

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

④ 정보보안관리자는 홈페이지 등에 비공개 내용이 게시되었는지 여부를 주기적으로 확인하여야 한다.

⑤ 정보보안관리자는 홈페이지에 중요정보가 공개된 것을 인지할 경우 이를 즉시 삭제하는 등의 보안조치를 강구하여야 한다.

제17조(사용자계정 관리) ① 시스템관리자 및 정보시스템 운영자는 사용자계정(ID)의 비인가자 도용 및 정보시스템 불법접속 등을 방지하기 위해 다음 각 호의 사항을 조치하여야 한다.

1. 직무변경, 퇴직 등 인사이동이 있을 경우 별지 제3호에 따라 관련 정보시스템 접근권한을 조정
2. 사용자별·그룹별 접근권한 부여 및 사용자계정 공용 금지
3. 장기간 사용하지 않는 휴면계정을 점검하여 불필요시 삭제
4. 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 정보시스템별 관리자계정은 별지 제4호에 따라 계정발급 현황을 관리하여야 한다.

제18조(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

② 서버에 등록된 비밀번호는 암호화하여 저장하여야 한다.

제19조(네트워크장비 보안관리) ① 시스템관리자는 라우터, 스위치 등 네트워크 장비 운용과 관련하여 다음 각 호의 보안조치를 강구하여야 한다.

1. 네트워크 장비에 대한 원격접속은 원칙적으로 금지하되 불가피할 경우 장비 관리용 목적으로 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 네트워크장비 접속기록은 6개월 이상 유지하고 비인가자의 침투 여부를 주기적으로 점검하여야 한다.

제20조(전자우편 보안대책) ① 정보보안관리자는 웜·바이러스 등 악성코드로부터 사용자의 전자우편 시스템 일체를 보호하기 위하여 백신, 바이러스 월, 악성메일 차단시스템 등의 보안대책을 강구하여야 한다.

② 사용자는 출처가 불분명하거나 의심되는 제목의 전자우편은 열람하지 않고 악성메일로 의심되는 전자우편은 즉시 정보보안관리자에게 신고하여야 한다.

제21조(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 프로그램 사용 금지

② 시스템관리자 또는 사용자는 악성코드가 설치되거나 감염된 사실을 발견하였을 경우에 다음 각 호의 조치를 취하여야 한다.

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

③ 정보보안책임자는 정보시스템 및 PC내 악성코드에 감염되어 피해가 심각한 경우 국가정보원, 중소기업청 등 유관기관에게 통보하여야 한다.

제22조(접속기록 관리) ① 정보시스템의 효율적인 통제·관리, 사고 발생 시 추적 등을 위하여 접속기록을 유지·관리하여야 한다.

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 분석시, 비인가자의 접속 시도, 정보 위변조 및 무단 삭제 등의 의심스러운 활동 사실을 발견한 경우 정보보안관리자에게 즉시 보고하여야 한다.

④ 접속기록은 최소 6개월 이상 보관하여야 하며 위·변조 및 외부유출 방지 대책을 강구하여야 한다.

제23조(데이터베이스 보안) ① 데이터베이스의 추가, 변경, 삭제 권한은 최소한의 인가자로만 제한되도록 운영하여야 한다.
② 정보의 중요도에 따라 사용자 접근권한을 부여하고, 모니터링하여야 한다.
③ 사용자별 접속기록을 관리하여야 하며 제22조에 따라 보안대책을 강구하여야 한다.

제24조(정보시스템 유지보수) ① 정보시스템 유지보수 수행업체에 대하여 다음 각 호의 보안대책을 강구하여야 한다.
1. 투입인력 보안관리, 보안서약서 징구(별지 제5호), 교육 등
2. 물리적 출입통제
3. 정보시스템 접근통제
4. 주기적인 정보보안 점검(별지 제6호) 등
② 시스템관리자는 유지보수 절차에 따라 정기점검을 수행하고 기록하여야 한다.
③ 시스템관리자는 유지보수와 관련된 장비·도구 등을 반·출입할 경우, 악성코드 감염여부, 자료 무단반출 여부를 확인하는 등의 보안조치를 하여야 한다.

제25조(전자정보 저장매체 불용처리) ① 전자정보 저장매체를 불용처리(교체・반납・양여・폐기 등)할 경우 저장매체에 수록된 자료가 유출되지 않도록 자산관리 담당부서와 협의하여 보안대책을 강구하여야 한다.
② 자료의 삭제는 해당 정보가 복구될 수 없도록 국가 정보보안 기본지침에 따라 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

제26조(보안 프로그램 설치·운영) 정보보안책임자는 사용자 PC 등의 보안환경을 강화하기 위하여 다음 각 호의 보안프로그램 설치 및 운용방안을 강구할 수 있다.
1. 바이러스백신 소프트웨어
2. 보안취약점 점검 소프트웨어
3. 자료유출방지 소프트웨어

제27조(무선랜 보안관리) ① 시스템관리자는 무선랜을 사용할 경우 보안대책을 수립하고 설치 사실을 정보보안관리자에게 통보하여야 한다.
② 시스템관리자는 제1항의 보안대책 수립시, 다음 각 호의 사항을 포함하여야 한다.
1. 복잡한 SSID 사용
2. SSID 브로드캐스팅 금지
3. WPA2 이상(256비트 이상)의 암호체계를 사용하여 통신 암호화
4. 무선단말기, 중계기(AP) 등 무선랜 구성요소별 분실·탈취·훼손·오용 등에 대비한 기술적·관리적·물리적 보안대책
5. 제19조에 따라 비밀번호 설정 및 관리
③ 정보보안관리자는 제1항 및 제2항과 관련한 보안대책의 적절성을 점검하여야 한다.

제28조(정보시스템 위탁운영 보안관리) ① 정보시스템 위탁운영시 관리적·물리적·기술적 보안대책을 수립하여 시행하여야 한다.
② 정보화용역사업 보안대책에 대한 이행실태를 주기적으로 점검하고 미비점 발견시 보완 조치하여야 한다.

부 칙(2014. 7. 23)

제1조(시행일) 이 요령은 원장의 승인을 받은 날부터 시행한다.

제2조(경과조치) 이 요령의 시행과 동시에 정보보안지침은 폐지하며, 이 요령 시행 당시 종전의 정보보안지침에 의하여 시행된 사항에 대해서는 이 요령에 의하여 시행된 것으로 본다.

[별지 제1호]

정보보안 실태조사 점검표

정보보안 관리자	정보보안 책임자

1. 정보보안 기본활동

순번	세부 점검사항	점검 결과	비 고 (부적정사유, 개선사항 등)
1	기관 자체 실정에 맞는 정보보안업무 내규를 수립하고 있는가? - 증빙자료 : 기관의 직제 규정(지침)		
2	매년 정보보안업무 활동계획을 수립·시행하고 심사분석 하는가? - 증빙자료 : 정보보안업무 세부추진계획 및 심사분석·평가 자료		
3	정보보안업무 전담 조직 및 직원(정보보안담당관)이 지정되어 있는가? - 증빙자료 : 기관의 직제 규정(지침) 및 조직도, 업무분장 관련 문서, 전담조직 임무·기능, 직원 명단		
4	사이버보안진단의 날을 내실 있게 수행하는가? - 증빙자료 : 사이버보안진단의 날 수행 실적, 월별 중점점검사항		
5	정보보안 위규·사고, 정보통신망 장애 발생시 보고체계 및 조치절차가 있는가? - 증빙자료 : 기관의 직제 규정(지침)		
6	정보시스템 사용자에 대한 심사 등 인적보안 절차·방법을 강구중인가? - 증빙자료 : 기관의 직제 규정(지침)		
7	보직변경 등 인사이동시 정보시스템 접근권한을 신속하게 조정하는가? - 증빙자료 : 정보시스템 접근권한 조정 내역		
8	서버·PC 등 정보시스템 현황을 제대로 파악하는가? - 증빙자료 : 정보시스템 현황 자료		
9	정보통신장비(노트북 등) 반출입 통제를 철저히 하는가? - 증빙자료 : 정보통신장비 반출입 대장		
10	업무자료를 상용 전자우편으로 전송하고 있지 않는가? - 증빙자료 : 접속 차단 설정, 내부 공지사항 등 근거자료		
11	정보통신망 구축 및 유지보수 업무를 수행하는 외부인력에 대한 신원확인 및 보안서약서 징구 등 충분한 보안조치를 하고 있는가? - 증빙자료 : 보안서약서 및 용역업체 보안대책 점검표		
12	용역업체 직원의 내부 정보시스템 접근을 통제하고 있는가? - 증빙자료 : 정보시스템별 접근권한 현황		
13	홈페이지에 자료 게재시 자체 보안성검토를 시행하고 있는가? - 증빙자료 : 홈페이지 정보공개 보안지침		
14	중요 정보화사업에 대하여 국정원에 보안성검토를 의뢰하는가? - 증빙자료 : 국가정보원 보안성 검토 결과		
15	정보보호시스템(암호모듈 포함) 도입시 보안적합성 검증절차를 준수하는가? - 증빙자료 : 암호제품 도입 현황, 검증필 암호모듈 사용 여부 입증 자료		

2. PC 및 서버 보안관리

순번	세부 점검사항	점검 결과	비 고 (부적정사유, 개선사항 등)
1	PC·서버에 설치된 운영체제 및 응용프로그램을 최신 보안업데이트 하였는가? - 증빙자료 : 사용자 PC 점검 결과, 서버 점검 결과		
2	백신프로그램이 자동 업데이트되고 실시간 감시기능이 설정되어 있는가? - 증빙자료 : 사용자 PC 점검 결과		
3	인터넷 PC에 업무관련 자료(비밀 포함)를 보관하고 있는가? - 증빙자료 : 사용자 PC 점검 결과		
4	P2P, 웹하드, 메신저 등 업무에 무관한 서비스가 허용되거나 비인가 프로그램을 사용하지 않도록 보안조치 하는가? - 증빙자료 : 비인가 사이트 차단 목록 갱신 증빙 자료, 보안 점검결과		
5	비인가자 접근방지를 위해 PC 부팅 비밀번호를 설정했는가? - 증빙자료 : 사용자 PC 점검 결과		
6	서버내 저장자료는 중요도에 따라 권한설정이 되어 있는가? - 증빙자료 : 서버별 권한설정 증빙 자료		
7	공개서버가 DMZ 구간에 위치하는 등 정보통신망 구성측면에서 PC 및 서버 등의 위치가 적정한가? - 증빙자료 : 정보통신망 세부 구성 현황 자료		
8	인가받지 않은 휴대용 저장매체(USB, 이동형 하드디스크, 메모리카드 등)를 반입·휴대하고 있는가? - 증빙자료 : 휴대용 저장매체 관리대장		
9	전자우편 비밀번호 설정시 특수문자 포함, 9자리 이상으로 설정하고 주기적으로 변경 사용하는가? - 증빙자료 : 내부 공지사항 등 근거자료		
10	비밀은 비밀용 보안USB를 별도 지정하여 저장하고 비밀관리기록부에 등재하여 사용하고 있는가? - 증빙자료 : 보안USB 관리기록부		
11	서버 등 정보시스템 접근기록을 유지 관리하는가? - 증빙자료 : 정보시스템 접근기록 대장		
12	PC·서버에 비인가 USB 등 비인가 정보통신기기 연결시 작동되지 않도록 보안 설정되어 있는가? - 증빙자료 : 사용자 PC 점검 결과		
13	PC·노트북 등 저장매체가 있는 기기의 고장시 저장된 자료의 완전 삭제를 확인하고 외부에 수리를 의뢰하는가? - 증빙자료 : 완전삭제 제품, 국가기관 도입가능 제품 여부, 정보시스템 수리현황		
14	중요정보가 저장된 매체 불용처리 시 전용 소자장치로 삭제하거나 파쇄·용해 등 물리적으로 완전 파기하고 있는가? - 증빙자료 : 불용PC처리대장, 하드포멧 증빙서류 등 확인		

3. 네트워크 보안관리

순번	세부 점검사항	점검 결과	비 고 (부적정사유, 개선사항 등)
1	정보시스템 세부 구성도(IP 포함)를 최신으로 유지하면서 대외비 이상 비밀로 관리하고 있는가? - 증빙자료 : 정보통신망 세부 구성 현황 자료, 대외비 관리기록부		
2	업무자료를 소통하기 위한 내부망 구축시 사설주소체계(NAT)를 적용하는가? - 증빙자료 : 업무망 IP 현황 및 NAT 적용 증빙 자료		
3	국가정보원장이 안전성을 검증한 정보보호시스템을 운용하고 있는가? - 증빙자료 : 정보보호시스템 목록(인증 및 보안적합성 검증여부 표기)		
4	네트워크를 통한 파일공유를 제한하고 있는가? - 증빙자료 : 사용자 PC 점검 결과		
5	스위치·라우터 등 네트워크 장비와 서버는 비인가자가 접속 못하도록 IP·MAC 통제 등 보안설정하고 불필요한 서비스포트를 제거하는가? - 증빙자료 : 네트워크 장비별 접근통제목록(ACL) 설정 출력물		
6	와이브로, 무선랜 등 허가받지 않은 인터넷 접속경로가 존재하는가? - 증빙자료 : 비인가 무선랜 점검 결과		
7	첨단 정보통신기기에 의한 내부 업무자료 유출방지 대책이 충분한가? - 증빙자료 : 정보 유출 방지시스템(문서보안제품 등) 구축 현황, 내부 업무자료 유출방지 대책		
8	시스템 최초 설치 시 등록된 관리자계정(회사명 등)·패스워드를 변경하였는가? - 증빙자료 : 관련 기록		
9	장비 신규 도입, IP할당내역 등 전산망 구성 변동시 관련사항을 기록하는가? - 증빙자료 : 정보시스템 현황자료 및 변경이력		
10	중요업무 처리 PC는 인터넷 연결을 금지하고 이상 유무를 수시로 점검하는가? - 증빙자료 : 사용자 PC 점검 결과		
11	무선네트워크 구축 시 사전에 국정원의 보안성검토를 받았는가? - 증빙자료 : 국가정보원 보안성 검토 결과		
12	홈페이지에 대한 보안취약점을 주기적으로 점검하는가? - 증빙자료 : 홈페이지 보안취약점 점검 및 조치결과		
13	불가피한 사정상 무선중계기를 설치하였을 경우 WPA2이상 보안설정을 하였는가? - 증빙자료 : WPA2 이상 보안설정 화면 출력물		
14	직원의 재택·파견·이동근무 등 원격근무 시 보안관리 절차가 충분한가? - 증빙자료 : 원격근무에 대한 보안관리 규정(지침)		

4. 정보통신시설보안 및 대도청 활동

순번	세부 점검사항	점검 결과	비 고 (부적정사유, 개선사항 등)
1	인위적·자연적 원인에 의한 정보통신망 장애 대비 백업 등 재난방지 대책을 강구하였는가? - 증빙자료 : 기관자체 재해복구 계획		
2	통합전산센터, 정보통신실 등 중요 정보통신시설을 보호구역으로 관리하는가? - 증빙자료 : 보호구역 지정현황, 보안조치 현황		
3	사무실 책상서랍 등에 비밀문건이나 비인가 정보통신기기가 방치되어 있는지 주기적으로 확인하는가? - 증빙자료 : 보안 관리·실태 점검표		
4	외부인의 정보통신실 출입이 통제되고 관련기록이 관리되는가? - 증빙자료 : 전산실(또는 정보통신실) 출입 관리대장		
5	무정전 전원공급장치 설치 등 비상시 전력장애에 대한 대책을 강구하고 있는가? - 증빙자료 : 전력장애에 대한 대책방안		
6	침입자동 경보장치, CCTV 등 보안장비와 방화장비(하론소화기 등) 정상동작 여부를 정기적으로 점검하고 있는가? - 증빙자료 : 월별 점검 결과 증빙자료		
7	정보통신시설에 관련시스템 긴급 파기를 위한 장비(해머 등)를 비치하였는가? - 증빙자료 : 증빙자료		
8	정보통신시설에 대한 접근권한을 업무목적에 따라 차등 적용하고 있는가? - 증빙자료 : 정보통신시설에 대한 접근통제목록(ACL) 설정 출력물, 정보통신시설 접근권한 차등적용 화면출력 자료 및 관련 근거		
9	외부인이 전사내 출입할 경우 출입통제를 실시하고 있는가? - 증빙자료 : 전산실(또는 정보통신실) 출입 관리대장		
10	통신(전화 등)단자함에 시건장치를 하여 비인가자가 무단 접근할 수 없도록 조치되어 있는가? - 증빙자료 : 통신(전화 등)단자함 시건장치 자료		
11	정보통신장비 수리·점검시 정보보안담당관이 입회하고 있는가? - 증빙자료 : 장비 수리·점검 결과서		

5. 보안관제 등 해킹 대응활동

순번	세부 점검사항	점검 결과	비 고 (부적정사유, 개선사항 등)
1	사이버공격에 대응하기 위한 관제센터를 운영하거나 同 업무를 他기관에 위탁 하였는가? - 증빙자료 : 관제센터 운영 보고서 및 위탁운영 현황 자료		
2	보안관제센터 운영을 총괄 관리하는 전담 공무원이 있는가? - 증빙자료 : 업무분장표		
3	사이버공격 탐지·대응 매뉴얼이 구비되어 있는가? - 증빙자료 : 사이버침해사고 대응체계, 담당자별 수행업무 명시자료		
4	해킹사고 조사결과, 보안위규자에 대한 처벌이 제대로 이루어지고 있는가? - 증빙자료 : 보안위규자에 대한 규정(지침) 또는 처리 내역		
5	보안시스템 및 정보시스템에 대한 로그를 일정기간 유지하고 있는가? - 증빙자료 : 로그관리 규정(지침) 또는 관리근거 자료		
6	보안관제 용역업체 직원에 대한 보안대책이 있는가? - 증빙자료 : 용역업체 보안점검 계획 및 결과		
7	자체 DDoS공격 대응매뉴얼을 구비하였는가? - 증빙자료 : 기관의 직제 DDoS공격 대응메뉴얼		
8	자체 사이버위기 대응 모의훈련을 주기적으로 실시하는가? - 증빙자료 : 사이버침해사고 대응훈련 계획, 훈련결과 보고서		
9	DDoS공격 등 침해사고 발생시 국가정보원 등 유관기관에 즉시 연락하는가? - 증빙자료 : 사이버침해사고 대응반 및 비상연락망 운영 현황		
10	시스템 장애시 유지보수 업체에 연락할 수 있는 비상연락체계가 구비되어 있는가? - 증빙자료 : 사이버침해사고 대응반 및 비상연락망 운영 현황		
11	보안관제시스템에 대한 물리적인 보안대책을 준수하고 있는가? - 증빙자료 : CCTV설치 및 생체인증 방식의 보안통제 입증 자료		
12	침해사고 발생시 사고조사내역 등 관련 문서(전자문서 포함)를 저장하고 있는가? - 증빙자료 : 처리결과 문서 및 통보기록		
13	해킹메일 대응방안 등 침해사고 대응절차 등을 보안교육을 수행하는가? - 증빙자료 : 교육계획 및 교육자료, 교육결과 보고서		
14	보안취약점 발표 시, 대상기관이나 담당직원에게 즉시 배포하는가? - 증빙자료 : 내부 공지사항 및 배포기록대장		
15	국가사이버안전센터 등과 사이버위협정보, 탐지기술 등 정보를 공유하고 있는가? - 증빙자료 : 정보공유 근거자료(공문, 이메일, 팩스 등)		
16	사이버공격 발생 시 소속·산하기관에 전파할 수 있는 체계가 구비되었는가? - 증빙자료 : 사이버침해사고 대응반 및 비상연락망 운영 현황		

[별지 제2호]

홈페이지 자료등록 신청서

(추가, 변경, 삭제)

신청부서	담당	부/팀장

신청일 :　　년　　월　　일

신청부서(팀)명			
신 청 자		연락처	Tel :
등록자료 위치		분량	페이지(A4)
등록자료 제목			
첨부 파일			
등록자료 내용요약*			
희망 등록일	년　　월　　일		
등록 처리일**	년　　월　　일		

정보보안관리자	* 등록자료 상세내용 및 첨부파일은 메일 전송 ** 등록 처리일은 정보보안 담당부서에서 기록	정보보안책임자

중소기업기술정보진흥원

[별지 제3호]

정보시스템 접근권한 변경내역서

정보보안 관리자	정보보안 책임자

아래와 같이 인사발령에 의거, 정보시스템 접근권한을 변경합니다.

20 년 월 일

<table>
<tr><td rowspan="2">담당자 정보</td><td>성명</td><td>직급</td><td>부서</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>접근권한 변경
(√)</td><td>등록(√)</td><td>수정( )</td><td>삭제( )</td></tr>
<tr><td rowspan="3">변경대상
정보시스템
(√)</td><td>그룹웨어
( )</td><td>인사관리시스템
( )</td><td>경영정보시스템
( )</td></tr>
<tr><td rowspan="2">웹메일
( )</td><td rowspan="2">홈페이지
( )</td><td>기타
( )</td></tr>
<tr><td></td></tr>
<tr><td>변경사유</td><td colspan="3"></td></tr>
</table>

[별지 제4호]

정보시스템 관리자계정 관리대장

정보보안 관리자	정보보안 책임자

No.	시스템명	분류	위치	ID	Password	관리자(성명)

[별지 제5호]

보안 서약서

성명 :

주민등록번호 :

소속 :

주소 :

상기 본인은 년 월 일 부로 중소기업기술정보진흥원(이하 :기정원“이라 한다)의 용역업무를 수행함에 있어 다음의 사항들을 준수할 것을 서약합니다.

1. 본인은 기정원의 보안규정에서 제시하는 사항들에 대해 성실히 수행할 것을 서약합니다.

2. 본인은 기정원으로부터 제공받은 각종 정보 및 자료에 대해 업무이외의 목적으로 사용하지 않을 것을 서약합니다.

3. 본인은 계약사항이 완료된 경우 기정원으로부터 습득한 관련 자료를 반납하며, 또한 비밀유지 의무를 다할 것을 서약합니다.

본인은 상기 사항들에 대해 성실하게 준수할 것을 서약하며, 만일 이를 위반했을 경우에는 대한민국 법이 정한 바에 따라 민/형사상의 책임을 감수할 것임을 서약합니다.

년 월 일

서약인 : (인/서명)

중소기업기술정보진흥원장 귀중

[별지 제6호]

정보화용역 정보보안 점검표

정보보안 관리자	정보보안 책임자

기관(업체) 명: 점검 일자: 20 년 월 일

순번	점검항목	관리 실태	이행여부
1	위탁 기관(업체)는 정보보안에 관련된 자체 규정이 마련되어 있는가?		
2	위탁 정보시스템의 보안사고에 대한 보고 및 대응절차를 마련하고 있는가?		
3	위탁 정보시스템의 보안사고에 대비한 비상연락망을 보유하고 있는가?		
4	위탁 정보시스템에 대한 자체 보안대책을 수립하고 정기적으로 이행하고 있는가?		
5	위탁 정보시스템 운영인력에 대하여 자체 보안 서약서를 징구하여 관리하고 있는가?		
6	위탁 정보시스템 출입통제를 실시하고 있는가?		
7	위탁 정보시스템에 대한 접근권한을 제한하고 있는가?		
8	위탁 정보시스템에 대한 접근기록 등의 보안로그를 설정하여 운영하고 있는가?		
9	사용자 계정 부여원칙을 준수하고 있는가?		
10	사용자 계정에 대한 패스워드 부여원칙을 준수하고 있는가?		
11	외부 위탁 정보시스템에 대한 불필요한 서비스포트를 제거하여 운영하고 있는가?		
12	외부 위탁 정보시스템에 대한 보안패치를 주기적으로 수행하여 최신 보안상태를 유지하는가?		
13	외부 위탁 정보시스템에 대한 악성코드 보안대책이 적용되어 운영하고 있는가?		
14	외부 위탁 정보시스템에 대한 정보보호시스템을 설치하여 보안을 강화하고 있는가?		
15	외부 위탁 정보시스템에 대한 모니터링 등으로 보안사고에 대한 대책을 수립하고 있는가?		
16	외부 위탁 정보시스템 장애 및 침해사고 시 해당 기록을 관리하고 재발방지대책을 수립하고 있는가?		

[별지 제7호]

정보시스템 관리대장

정보보안 관리자	정보보안 책임자

No.	시스템명	주요기능(용도)	설치일자	관리책임자	비 고

[별지 제8호]

방화벽 오픈 신청서

정보보안 관리자	정보보안 책임자

① 신 청 내 용(사용자 정보)			
성 명	(인)	직 급	
소 속		e-mail	
전화번호		휴대폰번호	
사용기간 (최대 30일)	20 . . . ~ 20 . . .		
사용목적 (상세히)			

② 방화벽 OPEN 정보 ※별지첨부가능

*구분	*IP주소 (Soruce IP)	*장비정보	*IP주소 (Destination IP)	*장비정보	*포트번호	*포트정보
1						
2						
3						
4						
5						
6						

처리내용			
처리일시			
처리자 성명	서명	전화번호	
비고			