정보시스템 관리세칙

제 정 2006. 2. 17
개 정(1) 2011. 4. 6
개 정(2) 2012. 4. 2
개 정(3) 2014. 8. 9
개 정(4) 2016. 10. 4
개 정(5) 2020. 9. 29
개 정(6) 2023. 3. 22

제1장 총칙

제1조(목적) 이 세칙은 컴퓨터에 의한 업무처리체계(H/W 및 S/W를 포함하는 개념으로 이하 “정보시스템”이라 한다)의 개발, 운영, 관리에 관한 사항을 정함을 목적으로 한다.

제2조(적용범위) ①정보시스템에 관한 사항은 법령 또는 다른 내규에 따로 정하는 경우 이외에는 이 세칙이 정하는 바에 의한다.
②이 세칙이 정하지 아니한 사항에 관하여는 정보시스템 주관부서장(이하 ‘주관부서장’이라 한다)이 정하는 바에 의한다.

제3조(용어의정의) ①이 세칙에서 사용하는 용어의 정의는 다음과 같다.
1. “정보시스템”이라 함은 컴퓨터에 의한 업무처리체계(H/W 및 S/W를 포함하는 개념)를 말한다.
2. “개발”이라 함은 업무를 정보시스템화 하는 일련의 과정을 말한다.
3. “운영”이라 함은 시스템의 조작 및 자료의 처리, 관리 등 정보시스템에 의해 업무를 처리하는데 수반되는 제반사항을 말한다.
4. “주관부서장”이라 함은 정보시스템 업무를 담당하는 부서장을 말한다.
5. “소관부서장”이라 함은 정보시스템화 대상 업무를 담당하는 부서장을 말한다.
6. “정보기기”라 함은 다음과 같다.
- 업무용 서버(Server)와 이에 연결 되어서 기능을 발휘하는 기기 및 탑재된 소프트웨어

- PC와 이에 연결 되어서 기능을 발휘하는 기기 및 탑재된 소프트웨어
- 데이터 통신설비와 이에 연결되어서 기능을 발휘하는 기기 및 탑재된 소프트웨어

7. “휴대용 저장매체”라 함은 디스켓, 외장형하드디스크(HDD), USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 등 자료를 저장하고 PC 등의 정보시스템과 분리할 수 있는 기억장치를 말한다.

8. “개인정보보호책임자“이라 함은 공사 내 처리되는 개인정보의 보호 및 관리를 담당하는 부서장을 말한다.

제2장 정보시스템 추진위원회

제4조(설치목적 및 기능) ①정보시스템업무 추진을 위한 중요사항을 심의·조정하기 위한 정보시스템추진위원회 (이하 “위원회”라 한다)를 설치·운영한다.

②위원회는 다음 각 호의 사항을 심의·조정한다.

1. 중장기 정보화계획의 수립
2. 기타 위원장이 필요하다고 인정하는 사항

제5조(구성) ①위원회는 다음과 같이 구성한다.

1. 위 원 장 : 경영관리부문장
2. 위　　원 : 관련 부서장, 기타 위원장이 필요하다고 인정하는 자

②위원회의 사무는 주관부서에서 담당한다.

제6조(운영방법) ①위원회 회의는 다음과 같이 소집한다.

1. 중장기 정보화계획 수립시
2. 공사의 경영에 영향을 미치는 정보시스템의 운영, 개발, 정보기기의 도입 등 위원장이 필요하다고 인정하는 때

②위원장은 필요시 관계있는 자를 출석시켜 그 의견을 청취할 수 있다.

제3장 계획

제7조(중장기 정보화계획) ①주관부서장은 정보기술 변화와 공사의 중장기 경영계

획에 맞추어 중장기 정보화계획을 수립한다.
②중장기 정보화계획은 사장 승인을 얻어 확정한다. 다만, 공사의 중장기 경영계획에 반영된 경우에는 그러하지 아니한다.
③주관부서장은 전략수립에 필요한 자료를 관련부서장에게 요청할 수 있다.
④중장기 정보화계획 중 공사의 중장기 경영계획 추진에 영향을 미치지 않는 경미한 사항은 주관부서장이 변경할 수 있다.

제8조(재해복구계획) ①주관부서장은 천재지변 등에 의한 전산재해 발생에 대비하여 백업, 복구절차, 인원 등에 대한 재해복구계획을 수립하고 이에 따라 재해복구시스템을 구축·운영한다.
②재해복구시스템의 점검을 위하여 필요시 주관부서장은 관련부서장에게 협조를 요청할 수 있다.

제4장 개발 및 운영

제9조(개발) ①업무별 소관부서장(이하 "소관부서장"이라 한다)은 정보시스템화 해야 할 대상업무에 대하여 타당성 검토 후 요건정의를 실시하고, 다음의 사항을 포함하여 주관부서장에게 개발을 의뢰한다.
1. 개발추진 배경
2. 정보시스템화 필요성, 효과분석
3. 업무처리개요(업무흐름도, 회계처리, 계산식, 보고서, 처리자격등급 등)
4. 업무량(사용자수 및 거래건수)
②정보시스템화 대상업무 소관부서장은 주관부서장이 요청하는 경우 다음의 사항을 적극 협조하여야 한다.
1. 정보시스템 개발자에게 개발업무 설명
2. 소관부서 직원의 파견 등 개발 참여
3. 기타 필요한 사항
③소관부서장이 독자적으로 정보시스템화 하고자 할 때에는 주관부서장의 합의를 거쳐 자체 개발할 수 있다. 이 경우 소관부서장은 정보기술체계, 개발자 선정 등에 관하여 주관부서장과 사전협의를 하여야 한다.
④개발방법론, 표준화 및 개발단계별 산출물은 주관부서장이 따로 정하는 바에 의한다.

제10조(개발절차) 업무를 정보시스템화 하고자 할 때에는 다음의 절차에 의한다. 다만, 개발규모가 작을 때에는 일부절차를 생략할 수 있다.

1. 분석
2. 설계
3. 프로그램 작성
4. 테스트
5. 이행(완료)

제11조(소관부서의 역할과 책임) 정보시스템의 개발 및 운영과 관련하여 소관부서의 역할과 책임은 다음 각호와 같다.

1. 정보시스템의 개발 및 변경 요청
2. 개발 및 변경대상 업무의 요건정의
3. 개발과정의 산출물 검증
4. 테스트 시나리오 작성 및 테스트 결과 확인
5. 개발시스템 및 데이터 이행 확인

제12조(주관부서의 역할과 책임) 정보시스템의 개발 및 운영과 관련하여 주관부서의 역할과 책임은 다음 각호와 같다.

1. 정보시스템의 개발 및 운영
2. 소관부서 업무의 정보시스템화 지원
3. 테스트 시나리오 작성 및 테스트
4. 데이터를 포함한 시스템 이행계획 수립 및 이행

제13조(운영) ①주관부서장은 이행된 업무의 유지보수 등 정보시스템을 운영·관리한다. 다만, 제9조 제3항에 의한 경우에는 주관부서장과 사전협의를 통하여 소관부서장이 운영·관리할 수 있다.

②소관부서장은 정보시스템의 안정적인 유지를 위하여 업무변경사항에 대하여 요건정의 및 테스트를 실시하여야 한다.

제14조(외주용역 및 업체선정) ①정보시스템의 개발 및 운영에 있어 필요하다고 판단하는 경우에는 이를 외주용역으로 할 수 있다.

②시스템 개발 및 유지보수를 위해 외부 전문업체의 용역이 필요할 경우, 용역업체의 선정은 계약세칙에 의한 절차를 따르는 것을 원칙으로 한다.

③제안평가는 “기술제안 평가표”를 작성하여 실시하며, 기술제안 평가표는

『기술제안서 평가항목 및 배점한도(정부고시 “소프트웨어기술성평가기준”)』을 기준으로 하여 작성하되 필요한 내용을 가감할 수 있다.

제15조(자료의 관리) ①공사의 업무에 대한 자료의 소유권한과 입력관리책임은 소관부서장이 갖는다.
②주관부서장은 정보시스템에 입력된 자료를 임의로 변경할 수 없다.

제16조(데이터 수정) ①데이터의 수정은 프로그램에 의하는 것을 원칙으로 하며, 소관부서의 정당한 요청 또는 프로그램 오류로 인하여 변경이 불가피한 경우 등 제한된 범위 내에서 수정한다.
②소관부서의 수정요청시 주요 데이터의 경우 적정성 여부 검증 후 수정토록 한다.

제17조(데이터의 수정요청) 소관부서는 데이터 수정이 불가피한 경우에 한하여 전자결재시스템의 “시스템 작업요청서”를 통해 데이터 수정을 요청한다.

제18조(정보기기의 관리) 정보기기를 설치·이용하고 있는 소관부서장과 주관부서장은 동 기기가 항상 정상적으로 가동될 수 있도록 유지 · 관리하여야 한다.

제19조(정보기기 배치요청) 정보기기에 대한 추가 수요가 발생한 경우 소관부서장은 전자결재시스템의 “정보기기 구입의뢰서”를 통해 주관부서장에게 해당 기기의 배치를 요청한다.

제20조(타당성 검토) 주관부서장은 요청내용에 대하여 검토를 실시하고 그 타당성이 인정될 경우 요청내용에 따라 처리한다.

제5장 정보보안

제21조(보안성 검토) ①주관부서장은 정보기기 도입 및 정보시스템의 개발과 운영시 정보보호를 위한 보안성을 검토한다.
②소관부서장이 정보시스템을 개발·운영하고자 할 경우에는 주관부서장에게 보안성 검토를 의뢰하여야 한다.

제22조(정보보안) ①주관부서장은 정보시스템 자료의 외부유출을 방지하거나 외부

침입자로부터 정보를 보호하기 위하여 통신의 차단 등 필요한 조치를 취할 수 있다.
②주관부서장은 정보자원의 보호를 위하여 필요한 모니터링을 실시하고 불법 소프트웨어의 삭제 등 필요한 조치를 취할 수 있다.

제23조(‘사이버보안진단의 날’ 운영) ①주관부서장은 매월 세번째 수요일을 ‘사이버보안진단의 날’로 지정·운영한다.
②주관부서장은 ‘사이버보안진단의 날’에 정보통신망을 대상으로 악성코드 감염여부와 정보통신시스템의 보안 취약 여부 등을 진단, 문제점을 발굴 개선한다.

제24조(PC 보안관리) ①PC사용자는 PC사용과 관련한 일체의 보안관리 책임을 가진다.
②PC사용자는 비인가자가 PC를 무단으로 접근하는 것을 통제하기 위하여 다음 각 호에 정한 보안대책을 강구하여야 한다.
1. 부팅, 화면보호 등 비밀번호 사용
2. 10분 이상 PC 작업 중단 시 화면보호 조치
3. 백신 및 PC용 침입차단시스템 등 운용
4. 운영체제 등 최신보안 패치 유지
5. P2P 등 업무와 무관하거나 보안에 취약한 프로그램의 사용 금지

③주관부서장은 PC반납시 하드디스크를 초기화 하여야한다.
④주관부서장은 PC고장으로 인하여 외부에 수리를 의뢰할 경우, 하드디스크에 수록된 자료는 백업 받은 후 복원이 불가능하도록 초기화 하여야 한다.
⑤PC사용자는 PC의 시스템 자원(폴더, 파일 등)에 대한 공유를 모두 제거하여야 한다. 다만, 필요에 의해 공유할 경우에는 암호설정 등의 보안대책을 수행하여야 한다.
⑥개인소유의 PC(노트북 PC 등)는 부서 내부로 반입 또는 반출하여 사용하여서는 아니 된다. 다만, 부득이한 경우에는 주관부서장의 승인을 받아 보안조치 한 후 반입 또는 반출 할 수 있다.
⑦인터넷 전용 PC의 경우, 문서 편집이 불가능하도록 읽기전용 소프트웨어를 설치·운용 하여야 한다.

제25조(보호구역 지정) 정보시스템과 관련하여 다음 구역을 보호구역으로 지정한다.
1. 컴퓨터실
2. 통신실

3. 백업센터
4. 기타 보안관리가 필요하다고 인정되는 정보시스템 설치장소

제26조(보호구역 출입자 통제) 주관부서장은 출입자격등급 보유자 이외의 보호구역 출입을 엄격히 통제한다.

제27조(보호구역 출입허가) 보호구역 출입자격등급 미 보유자가 보호구역을 출입하고자 하는 경우에는 출입구에 비치된 『보호구역 출입자 기록부』(양식1)에 출입시각 및 사유를 기술하고 주관부서장의 입회 하에 보호구역 내에 들어갈 수 있다.

제28조(사용자계정 관리) 사용자계정 관리방법은 다음과 같다.
1. 사용자별로 접근권한을 부여한다.
2. 외부사용자의 계정은 유효기간을 설정한다.
3. 비밀번호가 없는 계정은 폐기한다.
4. 일정기간 사용하지 않는 계정은 폐기한다.
5. 일정횟수이상 접속실패 시에는 사용을 중지한다.

제29조(사용자계정 신청) ①시스템을 사용하고자 하는 직원은 전자결재시스템의 “시스템 권한신청서”를 통해 시스템구분, 계정의 종류(시스템 계정, DB 계정)를 명시하여 신청한다.
②출장 등의 사유로 외부에서 공사 시스템(그룹웨어, 이메일 등) 접근이 필요한 경우, 전자결재시스템의 “시스템 작업요청서”를 통해 VPN 계정을 요청한다. 단, 기간은 한시적으로 적용한다.

제30조(사용자계정 부여) 주관부서장은 “시스템 작업요청서”에 명기된 사용자계정을 부여한다. 단, 그룹웨어 및 이메일 등의 시스템은 입사시 자동으로 부여한다.

제31조(사용자계정 삭제) ①임직원의 담당업무 변경 또는 이동 등의 인사발령 시 주관부서장은 해당 사용자계정을 삭제 한다.
②주관부서장은 장기간 사용하지 않는 계정이나, 시스템의 안정적 운영을 저해하는 사용자의 계정을 강제로 삭제할 수 있다.

제32조(비밀번호 초기화) ①계정사용자는 자신의 계정에 대한 비밀번호 초기화를

주관부서장에게 요청할 수 있다.
②주관부서장은 요청자의 사용자계정 비밀번호를 초기화하고 계정사용자는 초기화된 비밀번호를 변경하여 사용한다.

제33조(비밀번호 사용 및 관리) ①비밀번호 제정방법은 다음과 같다.
1. 추측할 수 있는 단어 사용 금지
2. 간단한 문자나 숫자의 연속사용 금지
3. 사전에 있는 단어 사용 금지
4. 숫자와 문자, 특수문자 등을 혼합하여 9자리 이상 사용
5. 사용자계정과 동일한 비밀번호 사용금지

②비밀번호는 화면에 나타나지 않도록 하는 등 타인이 알 수 없도록 관리하여야 한다.
③비밀번호 항목은 암호화하여 노출되지 않도록 관리하여야한다.
④비밀번호 변경내역(변경전 비밀번호, 변경일시 등)을 기록·유지하여 최근 3회 동안 변경 전 비밀번호 재사용을 방지하여야 한다.
⑤비밀번호는 90일 이내에 변경하여야 하며 변경되지 않은 경우 접근을 금지하여야 한다.
⑥정보시스템 접근시 비밀번호 저장기능 사용을 금하며, 반드시 비밀번호를 입력하여 사용하여야 한다.

제34조(사용자계정 재개) 장기간 미사용 등으로 사용허가가 중지된 계정의 사용재개를 주관부서장에게 요청할 수 있으며, 그 처리 절차는 비밀번호 초기화 절차에 준한다.

제35조(소프트웨어보안) ①모든 PC에는 정품 소프트웨어만이 설치되고 사용하여야 하며, 정품의 기준은 다음과 같다.
1. 원본의 저장매체를 보유하고 있는 경우
2. 해당 소프트웨어의 구입 또는 라이센스 계약서를 보유하고 있는 경우

②허가 없이 타인의 단말기에 접근하거나 자료를 취득할 수 있는 악의의 프로그램은 설치하거나 사용할 수 없다.

제36조(컴퓨터 바이러스 방지대책) ①바이러스 예방을 하기 위한 사항은 다음과 같다.
1. 휴대용 저장매체는 항상 쓰기 방지 기능을 적용하여 사용한다.

2. 저장매체를 이용한 자료 및 파일 복사시 반드시 바이러스 감염여부를 확인한다.
3. 휴대용 저장매체의 불법복사를 금지하여야 한다.
4. 개인용 컴퓨터 내에 항상 최신 버전의 바이러스 백신을 설치한다.
5. 컴퓨터바이러스로 인한 데이터 손상에 대비하여 수시 혹은 정기적으로 데이터의 백업을 실시하여야 한다.
6. 주관부서장은 바이러스 진단장치를 이용하여 서버의 바이러스 감염 여부를 수시로 확인한다.
7. 모든 프로그램은 사전에 바이러스 감염여부를 확인한 후 운영용 정보시스템에 설치한다.
② 바이러스 감염이 발견되었을 경우에 주관부서장은 다음의 조치를 하여야한다.
1. 바이러스 감염피해를 최소화하기 위하여 감염된 시스템 사용중지
2. 바이러스에 백신 프로그램을 이용하여 바이러스 퇴치
3. 바이러스 감염확산방지를 위해 사용자에게 관련 사실 및 보안조치사항을 즉시 전달
4. 바이러스 재발을 방지하기 위하여 원인 분석 및 예방 조치 수행

제37조(원격근무 보안관리) ①원격근무 지원자는 『원격근무 보안서약서』(양식2)를 작성하여 부서장에게 원격근무 승인을 득한 후, 주관부서장에게 제출하여야 한다.
②원격근무자는 원격근무 시 해킹을 통한 업무자료 유출을 방지하기 위하여 작업수행 전 최신 백신으로 원격근무용 PC를 점검하고 원격근무 PC에 업무자료 저장·보관을 금지한다.

제38조(전자우편 보안) ①전자우편 사용자는 보안조치 없이 전자우편을 이용한 비밀 및 중요자료 전송을 금지하고 출처가 불분명한 전자우편의 경우 열람하지 말고 삭제한다.
②주관부서장은 웜·바이러스, 스팸 메일 등으로부터 전자우편 시스템을 보호하기 위하여 백신 설치, 스팸 필터링 기능 도입 등 보안대책을 강구한다.

제39조(휴대용저장매체 사용제한) ①등록된 휴대용저장매체만 사용할 수 있으며 업무목적 이외 사적인 용도로 사용할 수 없다.
②주관부서장은 소속직원에게 공지 · 교육을 통하여 휴대용 저장매체의 임의 사용을 제한하여야 하고 이에 대하여 주기적인 점검을 실시한다.

제40조(휴대용저장매체 관리운영) ①휴대용저장매체는 각 부서장 책임 하에 관리하는 것을 원칙으로 한다.
②각 부서장은 소속직원의 휴대용저장매체 반 · 출입을 승인할 수 있으며 기간은 한 달 이내로 제한한다.
③휴대용저장매체의 분실, 고장, 또는 훼손 시 주관부서장에게 즉시 통보하고 주관부서장은 해당 휴대용저장매체의 사용을 중지시킨다.
④휴대용저장매체의 비밀번호 분실 시 주관부서장에게 통보하여 저장매체의 초기화 후 재등록하도록 한다.

제6장 개인정보보호

제41조(개인정보보호 조직 및 인력) 개인정보보호 업무를 총괄하여 수행할 수 있는 부서를 지정 · 운영하고, 개인정보보호 업무를 보다 원활하고 체계적으로 수행한다.

제42조(개인정보처리방침) 다음 각 호의 내용이 포함된 개인정보처리방침을 정하고 인터넷 홈페이지에 게재한다.
1. 개인정보보호책임자의 전화번호와 그 밖의 연락처
2. 개인정보의 수집, 처리, 파기 및 안전성 확보조치 등에 관한 사항
3. 그 밖에 개인정보의 보호를 위하여 필요한 사항

제43조(개인정보의 안전성확보) ①개인정보를 처리할 때에 개인정보가 분실·도난·누출·변조 또는 훼손되지 아니하도록 입출력자료·전산기기·전산실 등의 관리에 관하여 안정성확보에 필요한 조치를 강구한다.
②홈페이지를 구축 · 운영하는 과정에서 개인정보가 노출 또는 유출되지 아니하도록 관리적 · 기술적 조치를 취한다.

제44조(개인정보의 수집) ①채용 등의 개인정보 수집 시에 정보주체의 동의를 거친 후에 수집한다.
②개인정보를 수집하는 경우 개인정보 수집의 법적 근거, 목적 및 이용범위, 정보주체의 권리 등에 관하여 인터넷 홈페이지 등을 통하여 그 내용을 안내한다.

제45조(준용) 이 세칙에 명시되지 않은 사항은 다음 각 호의 정부규정 및 지침에 따른다.

1. 「국가정보보안 기본지침」
2. 「국가 사이버안전 관리규정」
3. 기타 관련법령

부 칙(1)

제1조(시행일) 이 세칙은 2006. 2.17 부터 시행한다.

부 칙(2)

제1조(시행일) 이 세칙은 2011. 4. 6 부터 시행한다.

부 칙(3)

제1조(시행일) 이 세칙은 2012. 4. 2 부터 시행한다.

부 칙(4)

제1조(시행일) 이 세칙은 2014. 8. 20 부터 시행한다.

부 칙(5)

제1조(시행일) 이 세칙은 2016. 10. 4 부터 시행한다.

부 칙(6)

제1조(시행일) 이 세칙은 2020. 9. 29 부터 시행한다.

부 칙(7)

제1조(시행일) 이 세칙은 2023. 3. 22 부터 시행한다.

(양식 1)

보호구역 출입자 기록부

일자	소 속	직위	성 명	날인	용 무	출 입 시 간		입 회 자	
						부 터	까 지	인	

(양식 2)

원격근무 보안서약서

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

1. 나는 부여받은 인증 관련 정보 및 매체를 타인에게 유출하지 아니 한다.
2. 나는 원격근무 중 작성·저장·열람·출력한 문서는 업무 목적에만 활용하고 타인에게 유출하지 아니한다.
3. 나는 원격근무용 소프트웨어 및 전산장비를 업무목적에만 활용하며 바이러스 백신 프로그램 및 기타 보안 프로그램을 설치하여 최신 상태로 유지한다.
4. 나는 여타 보안사항들을 성실히 준수하며 위반시 관련규정에 따라 처벌도 감수한다.

년 월 일

서약자 소속 직급 사번

☐ **제공동의**

성명 인

☐ **개인정보 취급동의**

※ 개인정보보호법 제15조 1항(개인정보의 수집·이용)에 의거하여 본인의 개인정보를 제공할 것을 동의 합니다