국립국어원 정보 보안 업무 처리 규정

제정 2013. 12. 26. 국립국어원 예규 제 95호
일부개정 2014. 3. 10. 국립국어원 예규 제111호

제1장 총 칙

제 1 조(목적) 이 규정은 국립국어원의 정보보안업무 수행에 필요한 사항을 규정함을 목적으로 한다.

제 2 조(정의) 이 규정에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. “부서”라 함은 국립국어원 각 과(실·팀을 포함)를 말한다.
2. “정보통신망”이라 함은 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송수신하는 정보통신체계를 말한다.
3. “인터넷서비스망”(이하 “인터넷망”이라 한다)이라 함은 기관의 네트워크 중에서 인터넷을 사용할 수 있도록 연결되어 있는 인터넷 전용망을 말한다.
4. “업무전산망”(이하 “업무망”이라 한다)이라 함은 기관의 네트워크 중에서 내부 업무를 수행할 수 있도록 연결되어 있는 전산망을 말한다.
5. “정보통신실”이라 함은 서버·PC 등 전산장비와 스위치·교환기·라우터 등 통신 및 전송장비 등이 설치 운용되는 장소를 말하며, 전산실·통신실 및 전자자료 및 전자기록물(전자정보) 보관실 등을 말한다.
6. “정보보안” 또는 “정보보호”라 함은 정보시스템 및 정보통신망을 통해 정보의 유출·위변조·훼손 등을 방지하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위로서 사이버안전을 포함한다.
7. “안전측정”이라 함은 정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 해킹·컴퓨터바이러스, 서비스방해, 도청 등으로부터 정보통신망과 정보를 보호하기 위하여 정보보안 취약점을 진단하는 제반활동을 말하며, 대도청(對盜聽) 측정활동을 포함한다.
8. “전자문서”라 함은 컴퓨터 등 정보처리 능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 정보를 말한다.
9. “전자기록물”이라 함은 정보처리능력을 가진 장치에 의하여 전자적인 형태로 송·수신 또는 저장되는 기록정보자료를 말한다.

10. “전자정보”라 함은 업무와 관련하여 취급하는 전자문서 및 전자기록물을 말한다.
11. “휴대용 저장매체”라 함은 디스켓・CD・하드디스크・USB 메모리 등 정보를 저장할 수 있는 것으로 PC 등의 정보통신망과 분리할 수 있는 기억장치를 말한다.
12. “정보시스템”이라 함은 PC・서버 등 단말기, 보조기억매체, 정보통신기기, 응용프로그램 등 정보의 수집・가공・저장・검색・송수신에 필요한 하드웨어 및 소프트웨어 일체를 말한다.
13. “정보보호시스템”이라 함은 정보의 수집・저장・검색・송신・수신시 정보의 유출, 위・변조, 훼손 등을 방지하기 위한 하드웨어 및 소프트웨어를 말한다.
14. “사이버공격”이라 함은 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스방해 등 전자적 수단에 의하여 정보통신망을 불법침입・교란・마비・파괴하거나 정보를 절취・훼손하는 공격 행위를 말한다.
15. “모바일 전자정부 공통기반”이라 함은 안전한 행정업무 모바일 서비스 제공을 위해 구비하여야할 모바일 기기관리, 구간암호화, 문서변환, 사용자 인증 등의 보안기능을 각급기관이 공동 활용할 수 있도록 제공하는 시스템을 말한다.
16. “모바일 기기”라 함은 각급기관의 업무 수행을 위해 기관 또는 기관 소속 공무원이 취득・관리・사용하는 스마트폰, 스마트패드, 태블릿PC 등의 휴대용 정보통신 단말기를 말한다.
17. “행정업무 모바일 서비스”라 함은 모바일 기기와 모바일 전자정부 공통기반을 이용하여 제공하는 행정업무 서비스를 말한다.
18. “행정업무 모바일 서비스 이용자”(이하 “이용자”라 한다)라 함은 행정업무 모바일 서비스를 이용하여 행정기관의 사무를 처리하고자 하는 행정기관 소속 공무원을 말한다.
19. “설치허용 앱목록(화이트리스트)”이라 함은 행정업무 모바일 서비스를 이용하는 모바일 기기에 설치할 수 있는 신뢰된 기관에서 검증한 모바일 애플리케이션의 목록을 말한다.
20. “모바일 전자정부 지원센터”라 함은「모바일 전자정부 서비스 관리지침」에 따라 공공기관의 모바일 서비스 등록・검증・배포 및 관리를 전담하는 조직을 말한다.

제 3 조(적용범위) 이 규정은 국립국어원에 적용한다.

제 2 장 정보보안업무의 체계

제 4 조(책무) 국립국어원장은 국가안보 및 국가이익 관련정보(전자정보를 포함한다. 이

하 같다)와 정보통신망을 보호하기 위한 보안대책을 마련하여야 하며 정보보안에 대한 책임을 진다.

제 5 조(정보보안담당관 지정 및 임무) ① 국립국어원장은 효율적인 정보보안업무를 수행하기 위하여 정보보안담당관을 임명하고 관련 조직을 구성 운영한다.

② 정보보안담당관을 임명한 경우에는 7일 이내에 소속・직책・직급・성명・연락처(전자우편 주소 포함) 등을 문화체육관광부장관을 경유하여 국정원장에게 통보하여야 하며, 정보보안담당관이 교체되었을 때에는 본부 정보보안담당관에게 통보하여야 한다.

③ 국립국어원장이 정보보안담당관에 부여하는 기본활동은 다음 각 호와 같다

1. 정보보안 정책 및 활동 세부계획 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. 정보통신실, 정보통신망 및 정보자료 등의 보안관리
6. 정보보안 관리실태 평가
7. 사이버공격 초동조치 및 대응
8. 사이버위협정보 수집・분석 및 보안관제
9. 정보보안 예산 및 전문인력 확보
10. 정보보안 사고 조사 결과 처리
11. 정보보안 교육 및 정보협력
12. 도청 위해 요소 측정・제거
13. 주요정보통신기반시설 보호활동
14. 국가용 보안시스템 및 암호키의 운용・보안관리
15. 행정업무 모바일 서비스 접속용 보안 소프트웨어 배포 및 설치 관리
16. 행정업무 모바일 서비스 이용자 등록 및 관리
17. 모바일 정보보안 정책 수립 및 검토
18. 모바일 악성코드 및 해킹 사고 발생 시 대응
19. 행정업무 모바일 서비스 이용자에 대한 주기적인 보안 교육 실시
20. 행정업무 모바일 서비스 이용 모바일 기기의 주기적인 보안 점검 실시
21. 기타 행정업무 모바일 서비스 보안 관련 제반 사항
22. 기타 행정업무 모바일 서비스 보안 관련 제반 사항
23. 기타 정보보안업무 수행 상 필요하다고 인정하는 사항

④ 정보보안담당관은 다음 각 호의 자가 되며, 보직 발령과 동시에 정보보안담당관

으로 임명된 것으로 본다.

1. 정보보안담당관 : 어문연구실장

2. 분임 정보보안담당관 : 각 부서의 장

⑤ 총괄 정보보안담당관은 행정업무 모바일 서비스 이용자의 근무지 위치, 업무특성 등에 따라 필요시 별도의 모바일 분임관리자를 지정할 수 있다.

⑥ 각 부서에서는 분임 정보보안담당관을 보좌하는 정보보안책임자를 둘 수 있으며, 부서별 분임 정보보안담당관이 지정하는 자가 된다.

제 6 조(분임 정보보안담당관의 지정 및 임무) ① 분임 정보보안담당관은 별도 발령 없이 보직과 동시에 분임 정보보안담당관이 된 것으로 본다.

② 분임정보보안담당관은 다음 각 호의 임무를 수행한다.

1. 정보보안담당관으로부터 지시 또는 위임을 받은 사항

2. 소속직원 및 위탁업체에 대한 정보보안 교육 및 점검

3. 소관의 업무에 대한 제반 정보보안 관리사항

제 7 조(정보보안 진단) ① 정보보안담당관은 정보보안업무 수행상의 모든 취약요소를 사전에 면밀히 파악・시정하고, 보안업무 관리체계를 확립하기 위하여 정기적으로 정보보안 진단을 실시하여야 하며, 정보보안 진단반은 다음 각 호와 같이 편성한다.

1. 반장 : 정보보안담당관(또는 언어정보과장)

2. 반원 : 정보보안 진단반장이 지명하는 자

② 제1항의 정보보안진단은 매월 셋째 주 수요일에 실시하며, 이 날을 “사이버・보안진단의 날”로 한다. 다만, 보안진단의 날이 공휴일인 경우에는 그 익일로 한다.

③ “사이버・보안진단의 날”에 실시할 보안진단의 내용은 다음 각 호와 같다.

1. 정보통신망의 악성코드 감염여부, 정보시스템의 보안취약 여부 등 정보보안업무 전반에 대하여 체계적이고 종합적인 보안진단

2. 기타 정보보안업무 전반에 대한 사항

④ 정보보안진단 실시결과 중대한 위반자에 대하여는 관계규정에 의한 행정조치를 취하여야 하며, 경미한 사항에 대하여는 즉각 시정을 명하여야 한다.

⑤국립국어원장은 정보보안진단 결과를 제8조에 규정한 정보보안업무 심사분석에 포함하여 문화체육관광부장관을 경유하여 국정원장에게 통보하여야 한다.

제 3 장 정보보안 기본활동

제 8 조(활동계획 수립 및 심사분석) ① 국립국어원장은 정보보안업무 세부추진계획(「국가사이버안전관리규정」제9조에 따른 사이버안전대책을 포함한다)을 수립·시행하고, 그 추진결과를 심사분석·평가하여야 한다.

② 제1항의 경우 국립국어원장은 세부추진계획 및 심사분석을 작성하여 문화체육관광부장관에게 제출한다.

제 9 조(정보보안 내규 제·개정) ① 국립국어원장은 정보 및 정보통신망 보호를 위한 자체 정보보안 내규(지침·시행세칙 등)를 이 지침에 저촉되지 아니하는 범위에서 작성 운용한다.

② 제1항의 경우 국립국어원장은 문화체육관광부장관과 사전 협의한다.

제10조(재난방지) ① 국립국어원장은 인위적이거나 자연적인 원인으로 인한 정보통신시스템의 장애 발생에 대비하여 시스템 이원화, 백업관리, 복구 등 종합적인 재난방지대책을 수립·시행하여야 한다.

② 국립국어원장은 재난방지 대책을 정기적으로 시험하고 검토해야 하며 업무 연속성에 대한 영향평가를 실시하여야 한다.

③ 국립국어원장은 정보시스템 장애에 대비한 백업시설을 확보하고 정기적으로 백업을 수행하여야 한다.

④ 국립국어원장은 제3항에 의거 백업시설을 설치할 경우에는 정보통신실과 물리적으로 일정거리 이상 위치한 안전한 장소에 설치하여야 하며 전력공급원 분리 등 정보시스템의 가용성을 최대화 할 수 있도록 하여야 한다.

제11조(정보보안위규) ① 정보보안 위규사항은 별표 1와 같다.

② 국립국어원장은 국가안보 및 국가이익에 중대한 영향을 미칠 수 있다고 판단되는 정보보안 위규에 대해서는 가장 신속한 방법으로 문화체육관광부장관을 경유하여 국정원장에게 통보하여야 한다.

③ 국립국어원장은 제2항의 경우 위규자, 위규 내용 및 조치 사항을 문화체육관광부장관을 경유하여 국정원장에게 통보하여야 한다.

제12조(보안사고 처리 및 조사) ① 국립국어원장은 별표 2의 정보 보안사고가 발생한 때에는 즉시 피해확산 방지를 위한 조치를 취하고 다음 각 호의 사항을 문화체육관광부장관을 경유하여 국정원장에게 통보하여야 한다.

1. 일시 및 장소
2. 사고원인, 피해현황 등 개요
3. 사고자 및 관계자의 인적사항
4. 조치내용 등

② 국립국어원장은 규정에 의한 관련자 징계, 재발방지를 위한 보안대책의 수립·시행

등 사고조사 결과에 따라 필요한 조치를 하여야 한다.

제13조(정보보안 기술 적용) ① 국립국어원장은 정보보안 대책을 강구하는 경우 제1항의 규정에 따라 국정원장이 제정한 표준을 우선 적용하여야 한다.

② 국립국어원장은 공공분야의 정보보안 관련 기술의 확보를 위하여 국정원장이 지정한 전문 연구기관으로 하여금 관련 연구개발을 수행하게 할 수 있다.

제 4 장 정보 및 정보통신망 보안

제14조(정보통신망 보안성 검토) ① 국립국어원장은「전자정부법 시행령」제35조에 따라 다음 각 호의 경우에 대하여는 자체 보안대책을 강구하고 문화체육관광부장관을 경유하여 국정원장의 보안성 검토를 받아야 한다. 다만, 사안이 경미할 경우 국정원장과 사전협의만으로 보안성 검토를 생략할 수 있다.

1. 유·무선 네트워크를 신·증설하거나 주전산기 등 정보통신시스템을 교체하는 경우(정보화 용역개발을 추진하고자 하는 사업계획 포함)
2. 내부 정보통신망을 외부망과 연결하고자 할 경우
3. 국정원장이 개발하거나 안전성을 검증한 암호장비·보안자재·암호논리·암호모듈·정보보호시스템을 도입 운용하고자 할 경우. 단, 암호장비·보안자재·암호논리·암호모듈·정보보호시스템 자체에 대한 검증은 '국가정보보안 기본지침' 제21조, 제22조, 제54조제2항, 제89조에 따른다.
4. 원격근무 지원 등을 위해 시스템을 도입하는 경우
5. 외부기관 및 업체에 정보통신망 보안감리 또는 보안컨설팅(보안취약성 분석·평가 포함)을 의뢰하거나 정보처리·보안관제 등 정보화·정보보호사업 업무를 위탁하는 경우
6. 기타 정보통신 운용환경 변화로 인하여 별도의 보안대책 수립이 필요하다고 인정되는 경우

② 국립국어원장은 당해년도 정보통신망 보안성 검토 대상사업 현황을 1.25한 국정원장에게 제출한다. 이 경우 제77조의 규정에 의한 시행계획을 활용하거나 별도로 제출할 수 있다.

③ 정보통신망 보안성 검토 업무절차는 다음과 같다.

1. 국립국어원장은 자체적으로 수립한 보안대책에 대하여 문화체육관광부를 경유하여 국정원에 보안성 검토를 요청한다.
2. 정보통신망 보안성 검토는 서면 검토를 원칙으로 하며, 국정원장이 필요하다고 판단하는 경우에는 현장 확인을 병행 실시할 수 있다.

④ 정보통신망 보안성 검토를 요청할 경우에는 다음 각 호의 서류를 제출 하여야 한

다.

1. 사업 목적 및 추진계획
2. 사업계획서
3. 기술제안요구서(RFP)
4. 정보통신망 구성도
5. 자체 보안대책 강구사항

⑤ 제6항 제5호 자체 보안대책 강구사항에는 다음 각 호를 포함하여야 한다.

1. 보안관리 수행체계(조직, 인원) 등 관리적 보안대책
2. 정보시스템 설치장소에 대한 보안관리 방안 등 물리적 보안대책
3. 국가용 보안시스템 및 국정원장이 개발하거나 안전성을 검증한 암호모듈·정보보호시스템 도입 운용 계획
4. 국가기관 간 망 연동 시 당해 기관간 보안관리 협의사항
5. 서버, 단말기, 보조기억매체, 네트워크 등 정보통신망의 요소별 기술적 보안대책
6. 재난복구 계획 또는 상시 운용계획

제15조(보안 적합성 검증) ①『전자정부법 시행령』제35조 제2항에 따라 국정원장이 개발한 것 이외의 정보보호시스템에 대한 안전성을 검증하기 위해 보안적합성 검증을 수행할 경우에는 문화체육관광부를 경유하여 국정원장에게 신청한다.

② 보안적합성 검증업무에 관한 세부사항은 제138조 내지 제144조의 규정에 따른다.

제16조(안전측정) ① 국립국어원장은 다음 각 호의 경우에 문화체육관광부를 경유하여 국정원장에게 안전측정을 요청할 수 있다.

1.「전자정부법」제27조 및「공공기록물 관리에 관한 법률」시행령 제5조의 규정에 따른 전자정보 보안조치(국정원장이 안전성을 확인한 암호장비·보안자재·암호논리·암호모듈·정보보호시스템 등의 도입 운용 및 정보통신망 보안대책의 시행)의 이행여부를 확인하고자 하는 경우
2.「국가사이버안전관리규정」제9조의 규정에 따른 사이버안전대책의 이행여부 등 정보통신망에 대한 안전성을 확인하고자 하는 경우
3.「보안업무규정」제35조에 따라 보안측정을 실시하는 경우
4. 정보보안 사고가 발생하여 정보통신망의 보안취약성 진단이 요구되는 경우
5. 국가 중요 정보통신시설에 대한 사이버공격이나 도청(盜聽) 등으로부터의 보호대책이 필요한 경우
6. 정보통신수단에 의하여 국가기밀 유출 및 암호체계의 누설 우려가 있는 경우
7. 국립국어원장이 정보통신망에 대한 보안취약성 점검 또는 종합진단이 필요 하다

고 판단하여 요청할 경우

8. 기타 국가안보상 필요하다고 판단하는 경우

② 국정원장은 안전측정을 실시하는 경우 사전에 측정항목・세부일정・준비사항 등이 포함된 안전측정 계획을 국립국어원장에게 통보하여야 한다.

③ 국정원장은 안전측정 결과 신속한 시정이 필요하다고 판단하는 경우에는 국립국어원장에게 필요한 조치를 요청할 수 있다. 이 경우 국립국어원장은 특별한 사유가 없는 한 이에 따라야 한다.

제17조(전자정보 보안대책) 국립국어원장은『전자정부법』제27조와 동법 시행령 제35조 및『공공기록물 관리에 관한 법률 시행령』제5조에 따라 전자정보에 대한 보안대책을 수립・시행하여야 한다.

제18조(전자정보 보안조치) ① 국립국어원장은 정보통신망을 통하여 보관・유통되는 전자정보의 보안을 위하여 다음 각 호의 조치를 이행하여야 한다.

1.『국가 정보보안 기본지침』제6조의 규정에 의한 정보보안 기본활동 수행

2.『국가 정보보안 기본지침』제27조 내지 제31조의 규정에 의한 전자정보 보안대책 이행

3.『국가 정보보안 기본지침』제3장의 규정에 의한 국가용 보안시스템의 사용

4.『국가 정보보안 기본지침』제4장의 규정에 의한 정보보호시스템의 도입 운용

5. 정보통신망 보안대책의 수립・시행

6. 국정원장이 발행한 지침・매뉴얼 및 각종 권고사항의 이행

7. 기타 전자정보 보안을 위하여 필요하다고 인정되는 보안대책의 이행

② 국정원장은 제1항제5호의 규정에 의한 정보통신망 보안대책 수립・시행에 필요한 별도의 지침・매뉴얼을 작성 배포할 수 있다.

제19조(일반전자정보 보호등급 분류) ①국립국어원장은 비밀이 아닌 중요 전자정보의 효율적인 보호를 위하여 다음 각 호에 해당하는 경우에는 자체 실정에 맞는 보호등급을 분류하여야 한다.

1. 최초로 정보통신망을 신설하여 전자정보의 보호등급 구분이 필요한 경우

2. 현재 운용중인 정보통신망을 재구성할 경우

3. 국립국어원장이 필요하다고 인정하는 경우

② 제1항의 규정에 의한 전자정보의 보호등급 분류는 다음 각 호와 같이 구분한다.

1. '가'급

유출 또는 손상되는 경우에 각급 기관의 업무수행에 중대한 장애를 초래하거나 개인신상에 심각한 영향을 줄 수 있는 전자정보

2. '나'급

유출 또는 손상되는 경우에 각급 기관의 업무수행에 장애를 초래하거나 개인신상

에 영향을 줄 수 있는 전자정보

3. '다'급

유출 또는 손상되는 경우에 각급 기관의 업무수행 및 기관의 이미지에 경미한 영향을 줄 수 있는 전자정보

제20조(일반 전자정보 보안대책) 국립국어원장은 제85조 제2항에 규정에 의하여 분류된 전자정보를 보호하기 위해서 EAL2 등급 이상의 인증을 받은 제품 중에서 선택하여 국정원장에게 보안적합성 검증을 신청하여야 한다.

제21조(비밀 전자정보 보안대책) ① 비밀 등 중요 전자자료를 정보통신망을 이용하여 생산·보관·분류·열람·출력·송수신·이관하는 등 전자적으로 처리하기 위해서는 국가용 보안시스템을 사용하여 암호화하는 등 국정원장이 안전성을 확인한 보안조치를 수행하여야 한다.

② 비밀을 전자적으로 생산하고자 할 때에는 해당 비밀등급과 예고문을 입력하여 열람 또는 출력시 비밀등급이 자동으로 표시되도록 하여야 한다.

③ 비밀을 전자적으로 생산·열람·출력·송수신·이관시에는 작업내용을 전자적으로 기록 유지하여야 하며 송수신시에는 정당성 확인 및 부인을 방지하기 위하여 전자적으로 생성된 영수증을 사용하여야 한다

④ 비밀 생산을 완료한 경우에는 PC에 입력된 비밀내용을 삭제하여야 한다. 만약 업무상 계속 보관이 필요한 경우에는 비밀 저장용 보조기억매체를 별도로 지정 사용하거나 PC 내에 독립된 폴더를 지정, 국가용 보안시스템으로 암호화하여 보관하여야 한다.

⑤ 국방·외교 관련 사항 등 비밀을 주로 취급하는 정보통신망은 인터넷 등 상용망과 분리 운용함을 원칙으로 한다. 다만, 국정원장이 승인한 경우에는 그러하지 아니할 수 있다

⑥ 전자적으로 처리된 비밀을 종이문서로 출력한 이후의 취급 관리는「보안업무규정」을 따른다.

제22조(비밀관리시스템) ① 국정원장은 비밀을 전자적으로 안전하게 처리하기 위하여 접근제어, 기밀성, 무결성, 식별, 부인방지 및 인증 등 보안기능을 제공하며 이 과정에서 발생하는 모든 정보를 기록 관리하는 기능을 가지는 정보시스템(이하 "비밀관리시스템"이라 한다)을 개발하여 각급기관에 보급할 수 있다.

② 제1항의 규정에도 불구하고 국립국어원장이 비밀관리시스템을 자체 개발하여 운용하고자 하는 경우에는 국정원장이 별도로 정한 규격을 준수하여야 한다.

③ 국립국어원장은 비밀관리시스템을 국가용 보안시스템으로 관리하여야 하며, 국정원장은 비밀관리시스템의 안전한 운영관리를 위해 필요한 사항을 정하여 국립국

어원장에게 배포할 수 있다.

제23조(비밀의 전자적 처리규격) 비밀을 전자적으로 안전하게 처리하는데 필요한 다음 각호의 사항에 대하여 별도의 규격으로 정한다.

1. 비밀의 생산, 등록, 보관, 사용, 유통 및 재분류, 이관, 파기 등 전 처리과정에서 요구되는 보안기능
2. 비밀의 관리를 위한 기능
3. 비밀을 표시하기 위한 양식 및 외형 정의
4. 비밀을 전자적으로 처리하면서 발생하는 각종 이벤트 기록·관리 기능
5. 비밀을 관리하기 위한 각종 대장 및 카드 정의
6. 사용자 및 시스템 관리 기능
7. 기타 비밀을 전자적으로 처리하는데 필요한 보안·관리 기능

제24조(대도청 측정) ① 국립국어원장은 청사(해외 포함)를 신설·이전 또는 증·개축하고자 할 때에는 도청방지 대책을 강구하여야 한다.

② 국정원장은 전자파 방출 또는 도청장치에 의한 정보유출을 방지하기 위하여 다음 각 호를 대상으로 대도청(對盜聽)측정 계획을 수립·시행할 수 있다.

1. 각급기관의 시설·지역·네트워크·정보시스템
2. 해외공관 및 해외무역관
3. 방위산업체 등

③ 국립국어원장은 도청징후를 포착하였거나 중요한 협상이나 회의 또는 회담을 개최하는 장소 및 공사가 진행중인 주요시설 등에 대하여 국정원장에게 대도청측정을 요청할 수 있다.

④ 국립국어원장은 디지털·레이저 등 첨단도청장치에 의한 불법도청을 방어하기 위한 시스템 도입·운용할 경우에는 국정원장과 사전 협의하여야 한다.

⑤ 국립국어원장은 비의도적인 전자파 발생 또는 침입 전자파에 의한 기밀유출 방지를 위하여 관련 장비를 도입·운용하고자 할 경우에는 국정원장과 사전협의하여야 한다.

⑥ 국립국어원장은 전자파 차폐실을 구축할 경우에는 국정원장이 제정한 「전자파 차폐실 구축 및 측정기준」에 따른다.

⑦ 국립국어원장은 주요 사무실에 차폐유리·도료 등 차폐재료 설치를 권장하고 전자파장애(EMI)·전자파적합성(EMC) 검증을 받은 제품을 사용하여야 한다.

제25조(대도청측정 결과조치) ① 국정원장은 대도청(對盜聽)측정결과를 당해 기관의 장에게 통보하여야 하며, 국립국어원장은 도출된 문제점에 대하여 국정원장과 협의하여 필요한 보안방책을 수립·시행하여야 한다.

② 국립국어원장은 대도청측정 계획 및 결과에 관한 내용을 외부에 공개하여서는 아니 된다.

제26조(인적 보안) ① 국립국어원장은 소관 정보통신망(정보시스템 포함) 사용과 관련하여 사용자의 직위·임무별 정보통신망 접근 자격부여 등 인적보안에 관한 절차 및 방법을 마련하고, 정보통신망을 통하여 비밀 등 중요정보를 취급하는 사용자에 대해서는 비밀취급인가, 보안서약서 징구 등의 보안조치를 하여야 한다.

② 국립국어원장은 외부 인력을 활용하여 정보시스템의 개발, 운용, 정비 등을 수행할 경우에는 해당 인력의 고의 또는 실수로 인한 정보유출이나 파괴를 방지하기 위하여 보안조치를 수행하여야 한다. 용역사업에 관련된 세부사항은 제30조(용역사업 보안관리) 또는 국가 정보보안 기본지침 「외부 용역업체 보안관리방안」(부록 7)을 따른다.

제27조(정보시스템 보안) ① 국립국어원장은 정보시스템(PC·서버·네트워크 장비, 정보통신기기 등 포함)을 도입·사용할 경우, 사용자와 해당 시스템의 관리자 및 관리책임자를 지정 운용하여야 한다.

② 사용자는 개인PC 등 소관 정보시스템을 사용하거나 본인 계정으로 정보통신망에 접속하는 것과 관련한 보안책임을 가진다.

③ 시스템관리자는 서버·네트워크 장비 등 부서 공통으로 사용하는 정보시스템의 운용과 관련한 보안책임을 진다.

④ 제1항부터 제3항까지와 관련하여 정보시스템을 실제 운용하는 부서의 장이 정보시스템 '관리책임자'가 되며, 관리책임자는 정보시스템 관리대장(별지 제7호 서식)을 수기 또는 전자적으로 운용 관리하여야 한다.

⑤ 관리책임자는 해당 부서의 정보시스템 관리대장에 정보시스템의 변경 최종 현황을 유지하여야 한다.

⑥ 정보보안담당관은 제1항부터 제5항까지에 명시된 정보시스템 운용과 관련한 보안취약점을 발견하거나 보안대책 강구가 필요하다고 판단할 경우, 사용자·시스템 관리자 및 관리책임자에게 시정을 요구할 수 있다,

제28조(중요 정보통신시설 보안관리) ① 국립국어원장은 다음 각 호의 중요 정보통신시설 및 장소를 「보안업무규정」에 따른 보호구역으로 설정 관리하여야 한다.

1. 암호실·통신실
2. 정보통신실
3. 국가용 보안시스템 개발·설치 장소
4. 백업센터 및 중요한 정보통신시설을 집중 제어하는 국소
5. 기타 보안관리가 필요하다고 인정되는 정보시스템 설치 장소

② 국립국어원장은 제1항에서 지정된 보호구역에 대한 보안 대책을 강구할 경우 다음 각 호 사항을 참고하여야 한다.

1. 방재대책 및 외부로부터의 위해(危害) 방지대책
2. 상시 이용하는 출입문은 한 곳으로 정하고 이중 잠금장치 설치
3. 출입문 보안장치 설치 및 주야간 감시대책
4. 보조기억매체를 보관할 수 있는 용기 비치
5. 정보시스템 안전지출 및 긴급파기 계획 수립
6. 관리책임자 및 자료·장비별 취급자 지정 운용
7. 정전에 대비한 비상전원 공급, 시스템의 안정적 중단 등 전력관리 대책
8. 비상조명 장치 등 비상탈출 대책
9. 전자파 누설 방지 대책
10. 카메라 장착 휴대폰 등을 이용한 불법 촬영 방지 대책 등

제29조(정보통신망 현황·자료 관리) ① 국립국어원장은 다음 각 호에 해당하는 정보통신망 관련 현황·자료 관리에 유의하여야 한다.

1. 정보통신시스템 운용현황
2. 정보통신망 구성현황
3. IP 할당현황
4. 주요 정보화사업 추진현황

② 국립국어원장은 다음 각 호의 자료를 대외비로 분류하여 관리하여야 한다. 다만, 국가안보와 직결되는 중요한 정보통신망 관련 세부자료는 해당 등급의 비밀로 분류 관리하여야 한다.

1. 정보통신망 세부 구성현황(IP 세부 할당현황 포함)
2. 국가용 보안시스템 운용 현황
3. 보안취약점 분석·평가 결과물
4. 정보시스템 관리대장 (별지 제 7호 서식)
5. 기타 보호할 필요가 있는 정보통신망 관련자료

③ 정보통신망에 비밀번호를 저장하고자 할 경우에는 암호화하여 보관하여야 하고, 서버 등 주요 정보시스템의 비밀번호를 종합기록 관리하고자 할 경우에는 정보시스템 관리대장(별지 제 7호 서식)에 등재하여 관리하여야 한다.

④ 제 2항에 명시되지 않은 정보통신망 관련 대외비 및 비밀의 분류는 국정원장이 제정한「비밀 세부분류지침」(대외비)을 따른다.

제30조(용역사업 보안관리) ① 국립국어원장은 정보화·정보보호사업 및 보안감리·보안컨설팅 수행 등을 외부 용역으로 추진할 경우, 국정원장의 사전 보안성 검토를

거친 보안대책을 수립·시행하여야 한다.

② 국립국어원장은 제1항 관련 용역사업 계약시 계약서에 용역사업 참여직원의 보안준수 사항과 위반시 손해배상 책임 등을 명시하여야 한다.

③ 국립국어원장은 비밀 관련 용역사업을 수행할 경우, 외부인원에 대한 비밀 취급인가 보안교육 등 보안조치를 수행하고 그 이행실태를 점검하여야 한다.

④ 정보통신망도·IP현황 등 용역업체에 제공할 자료는 자료 인계인수대장을 비치, 보안조치 후 인계·인수하고 무단 복사·외부반출을 금지한다.

⑤ 정보보안담당관은 용역업체의 노트북 등 관련 장비를 반입·반출시마다 악성코드 감염여부, 자료 무단반출 여부를 확인하는 등 보안조치를 확 행하여야 한다.

⑥ 용역사업 종료시 외부업체의 노트북·보조기억매체 등을 통해 기관 내부자료 및 용역 결과물이 유출되는 것을 방지하기 위하여 복구가 불가능하도록 완전 삭제·포맷 및 필요시 자성소거 등 보안조치를 확행하여야 한다.

⑦ 국립국어원장은 용역업체로부터 용역 결과물을 전량 회수하고 비인가자에게 제공·대여·열람을 금지하는 등 관리를 철저히 하여야 한다.

제31조(원격근무 보안관리) ① 국립국어원장은 재택·파견·이동근무 등 원격근무를 지원하기 위한 정보시스템을 도입·운영할 경우 기술적·관리적·물리적 보안대책을 수립하고 국정원장의 보안성 검토를 거쳐 시행하여야 한다.

② 국립국어원장은 원격근무 가능 업무 및 공개·비공개 선정기중을 수립 운영하고 대외비 이상 비밀자료를 취급하는 업무는 원격근무 대상에서 원칙적으로 제외하되 대외비 이상의 업무를 필히 수행해야 하는 경우 국정원장과 협의한 후 수행여부를 결정한다.

③ 국립국어원장은 모든 원격근무자에게 보안서약서를 징구하고 원격근무자의 업무변경·인사이동·퇴직 등 상황 발생시 이용권한 재설정 및 삭제, 정보시스템 회수 등 절차를 마련 시행하여야 한다.

④ 국립국어원장은 정보통신망에 대한 접근통제를 위하여 침입차단시스템 등을 설치하고 원격 근무자가 필요한 서비스만 사용하도록 접근권한을 설정하여야 한다.

⑤ 원격근무자는 정보시스템 고장시 정보유출 방지등 보안대책을 강구한 후 정보보안담당관과 협의하여 정비·반납 등 조치를 취하여야 한다.

⑥ 비공개 원격업무인 경우에는 국가용 보안시스템을 사용하여 소통자료를 암호화하고 행정전자서명처계를 이용하여 인증하며 인증강화를 위해 일회용 비밀번호·생체인증 등 보안기술을 사용하여야 한다.

⑦ 정보보안담당관은 주기적인 보안점검을 실시하여 원격근무 보안대책의 이행여부를 확인하여야 한다.

제32조(무선통신 보안관리) ① 국가 무선통신망(이하 '무선망'이라 한다)운용에 따른 보안관리 방침은 다음과 같다.

1. 보안상 취약한 무선망의 신설 또는 증설 억제
2. 도서·내륙지역 취약 무선망의 유선화 및 다원화 연차적 추진 등 보안대책 수립 추진
3. 국가 및 공공기관에서 운용하고 있는 무선망으로 비밀 등 중요자료를 소통하고자 하는 경우 국가용 보안시스템 사용
4. 무선망을 신규 도입하거나 운용환경을 변경하고자 할 때에는 국가용 보안시스템을 개발 적용할 수 있도록 입찰조건에 명시

② 무선망을 운용하거나 무선망 사업자를 관할하는 기관의 장은 다음사항을 주관 시행하여야 한다.

1. 전파월경 방지대책 강구
2. 무선망에 국가용 보안시스템 설치 운용
3. 무선국의 현황 관리와 보안지도 점검
4. 정보보안 위규 및 보안취약성 근절을 위한 전파감시 및 전파측정
5. 공중통신망 이용시 국가용 보안시스템 활용

제33조(무선랜 보안관리) ① 국립국어원장은 무선랜(와이파이 등)을 사용하여 업무자료를 소통하고자 할 경우 자체 보안대책을 수립하여 관련 사업 계획단계(사업 공고 전)에서 국가정보원장에게 보안성 검토를 의뢰하여야 한다.

② 시스템관리자는 제1항의 보안대책 수립시, 다음 각 호의 사항을 포함하여야 한다.

1. 네트워크 이름(SSID, Service Set Identifier) 브로드캐스팅 중지
2. 추측이 어려운 복잡한 SSID 사용
3. WPA2 이상(256비트 이상)의 암호체계를 사용하여 소통자료 암호화(국가정보원장이 승인한 암호논리 사용)
4. MAC 주소 및 IP 필터링 설정, DHCP 사용 금지
5. RADIUS(Remote Authentication Dial-In User Service) 인증 사용
6. 그 밖에 무선단말기·중계기(AP) 등 무선랜 구성요소별 분실·탈취·훼손·오용 등에 대비한 관리적·물리적 보안대책

③ 정보보안담당관은 제1항 및 제2항과 관련한 보안대책의 적절성을 수시로 점검하고 보완하여야 한다.

제34조(무선 인터넷 보안관리) ① 국립국어원장은 무선인터넷(WiBro, HSDPA 등) 시스템을 구축하여 업무자료를 소통하고자 할 경우 자체 보안대책을 수립하여 관련 사

업 계획단계(사업 공고 전)에서 국가정보원장에게 보안성 검토를 의뢰하여야 한다.

② 시스템관리자는 청사 전역에 무선인터넷 사용을 제한하고 민원실 등 특별히 무선인터넷 사용이 필요한 구역에 한해 기관장 책임하에 운용한다.

③ 시스템관리자는 업무용PC에서 무선인터넷 접속장치(USB형 등)가 작동되지 않도록 관련 프로그램 설치 금지 등 기술적 보안대책을 강구하여야 한다.

④ 정보보안담당관은 개인 휴대폰을 제외한 무선인터넷 단말기의 사무실 무단 반입·사용을 금지하는 한편 제1항부터 제2항까지와 관련한 보안대책의 적절성을 수시로 점검하고 보완하여야 한다.

제35조(RFID 보안관리) ① 국립국어원장은 RFID 시스템을 구축하여 중요자료 등 보호할 필요가 있는 정보를 소통하고자 할 경우 자체 보안대책을 수립하여 사업계획 단계(사업공고 전)에서 국가정보원장에게 보안성 검토를 의뢰하여야 한다.

② 시스템관리자는 제1항의 보안대책 수립시, 다음 각 호의 사항을 포함하여야 한다.

1. RFID시스템의 분실·탈취 대비 보안대책 및 백업대책
2. 태그정보의 최소화 대책
3. 장치 인증, 사용자 인증 및 기밀 등 중요정보의 암호화 대책

③ 정보보안담당관은 제1항 및 제2항과 관련한 보안대책의 적절성을 수시로 점검하고 보완하여야 한다.

④ RFID 보안관리에 관한 구체적인 사항은 국가 정보보안 기본지침「RFID 보안관리지침」(부록 8)을 따른다.

제36조(인터넷전화 보안관리) ① 국립국어원장은 인터넷전화 시스템을 구축하거나 민간 인터넷 전화 사업자망(070)을 사용하고자 할 경우에는 사업 계획단계에서 자체 보안대책을 수립 시행하여야 한다

② 시스템관리자는 제1항의 보안대책 수립시, 다음 각 호의 사항을 포함하여야 한다.

1. 인터넷전화기에 대한 장치 인증 및 사용자 인증
2. 제어신호 및 통화내용의 암호화
3. 인터넷전화망(음성 네트워크)과 일반 전산망(데이터 네트워크)의 분리
4. 인터넷전화 전용 방화벽 등 정보보호시스템
5. 백업체제 구축

③ 시스템관리자는 인터넷전화 시스템 구축을 위하여 민간 사업자망을 이용할 경우, 해당 사업자로 하여금 서비스 제공 구간에 대한 보안대책을 강구하도록 하여야 한다.

④ 인터넷전화 구축시 보안관리에 관련된 구체적인 사항은 국가 정보보안 기본지침 「인터넷전화 구축시 보안준수사항」(부록 9)을 따른다.

제37조(CCTV시스템 보안관리) ① 국립국어원장은 CCTV 운용에 필요한 카메라, 중계·관제서버, 관리용PC 등 관련 시스템을 비인가자의 임의 조작이 물리적으로 불가능하도록 설치하여야 한다.

② CCTV 상황실은 보호구역으로 지정 관리하고 출입통제장치를 도입하여야 한다.

③ 시스템관리자는 CCTV 카메라, 비디오서버, 관제서버 및 관련 전산망 설치시 업무망 및 인터넷망과 분리 운영하는 것을 원칙으로 한다. 다만, 부득이하게 인터넷망을 이용할 경우에는 전송내용을 암호화하여야 한다.

④ CCTV 시스템 일체는 사용자계정·비밀번호 등 시스템 인증대책을 강구하고 허용된 특정 IP에서만 접속 허용하는 등 비인가자의 침입 통제대책을 강구하여야 한다.

⑤ 정보보안담당관은 제1항부터 제4항까지와 관련하여 보안대책의 적절성을 수시로 점검하고 보완하여야 한다.

⑥ CCTV 시스템의 보안관리에 관련된 구체적인 사항은 국가 정보보안 기본지침 「CCTV 시스템 보안관리 방안」(부록 10)을 따른다.

제38조(디지털복사기 보안관리) ① 국립국어원장은 디지털복사기(”이하 “복사기”라 한다)를 도입하고자 할 경우 복사기 저장매체에 보관된 자료유출 방지를 위하여 자료의 완전삭제 기능이 탑재된 제품을 도입하여야 한다.”

② 시스템관리자는 다음 각 호의 경우에 복사기 저장매체의 저장자료를 완전 삭제하여야 한다.

1. 복사기의 사용연한이 경과하여 폐기·양여할 경우
2. 복사기의 무상 보증기간중 저장매체 또는 복사기 전체를 교체할 경우
3. 고장수리를 위한 외부반출 등 해당 기관이 복사기의 저장매체를 보안통제할 수 없는 환경으로 이동할 경우
4. 그 밖에 해당 기관에서 저장자료 삭제가 필요하다고 판단하는 경우

③ 시스템관리자는 복사기의 소모품 등을 교체하기 위한 유지보수시 정보보안담당관 입회·감독하에 작업을 실시하여 저장매체 무단 교체 등을 예방하여야 한다.

④ 정보보안담당관은 저장매체 내장 복사기 현황을 파악하고 복사기의 유지보수 및 불용처리시 저장매체에 대한 보안조치를 수행하여야 한다.

⑤ 복사기의 저장자료 삭제방법 등에 관련한 구체적인 사항은 국가 정보보안 기본지침 「정보시스템 저장매체 불용처리지침」(부록 6)을 따른다.

제39조(첨단 정보통신기기 보안관리) ① 국립국어원장은 개인휴대단말기(PDA)·스

마트폰, 전자제어장비 등 첨단 정보통신기기를 활용하여 업무자료 등 중요정보를 소통·관리하고자 할 경우에는 자체 보안대책을 수립하여 관련 사업 계획단계(사업 공고 전)에서 국가정보원장에게 보안성 검토를 의뢰하여야 한다.

② 시스템관리자는 제1항의 보안대책 수립시, 다음 각 호의 사항을 포함하여야 한다.

1. 첨단 정보통신기기에 대한 장치 인증 및 사용자 인증
2. 제어신호, 통화내용 등 데이터의 암호화
3. 업무자료의 무단 저장 금지 및 업무용·인터넷 PC에 무단 연동 금지
4. 시스템의 분실·훼손·탈취 등에 대비한 관리적·물리적·기술적 보안대책

③ 정보보안담당관은 개인이 소지한 첨단 정보통신기기가 업무와 무관하더라도 업무자료 유출에 직·간접 악용될 소지가 있다고 판단될 경우, 반출·반입 통제 등 관련 대책을 강구할 수 있다.

④ 국립국어원장은 제2항과 관련한 보안대책 수립·시행을 위하여 국가정보원장에게 해당 첨단 정보통신기기 도입에 따른 보안취약점과 대책 등 기술지원을 요청할 수 있다.

⑤ 국립국어원장은 제2항과 관련한 정보통신기기 사용자를 대상으로 인증 및 암호화에 필요한 전자정보를 발급할 수 없는 경우, 「정보통신기기 암호기술 적용지침」(2010.8, 국가정보원)을 준수하여야 한다.

⑥ 국립국어원장은 스마트폰을 업무에 안전하게 활용하고자 할 경우, 보안 요구사항을 명시한 「국가기관 업무용 스마트폰 보안규격」(2010.6, 국가정보원)을 준수하여야 한다.

제40조(국제협상 보안관리) ① 국립국어원장은 국제 협상을 위해 노트북 PC 등 정보시스템을 현지에서 사용하고자 하는 경우 중요협상정보가 유출되지 않도록 다음 각 호의 보안대책을 수립·시행하여야 한다.

1. 정보시스템 설치장소에 대한 물리적 접근통제 대책
2. 정보시스템 등 보안관리 대책
3. 암호화 등 정보시스템 저장정보 보안대책
4. 전화·팩스 등 통신시설에 대한 도청 방지 대책
5. 기타 협상정보 보호를 위해 필요하다고 인정되는 대책

② 국립국어원장이 제1항의 보안대책을 수립한 경우 미리 국정원장에게 보안성검토를 요청하여야 한다.

③ 국제협상 참가자는 협상 대상국이 제공한 정보시스템을 이용하여 중요 협상 정보를 작성하거나 저장 또는 송·수신하여서는 아니 된다. 다만, 불가피한 경우에는 보안대책을 수립, 국정원장의 보안성 검토를 거쳐 시행하여야 한다.

제41조(사이버공격 초동조치) ① 국립국어원장은 소관 정보통신망에 대하여 해킹, 웜·바이러스 유포 등 사이버공격 인지시 피해실태를 파악하고 관련 로그자료 보존 및 필요시 정보통신망 분리 등 초동조치를 하여야 한다.

② 단순 웜·바이러스 감염 등 경미한 사항은 자체 처리 후 문화체육관광부를 경우하여 국정원장에게 관련사항을 통보하여야 한다.

③ 홈페이지 변조, 정보통신망 기능장애, 마비 또는 자료 유출 등 중대사고 발생시에는 초동조치 후 즉시 국정원장에게 통보하여 지원을 받아야 한다.

④ 제3항과 관련하여 피해시스템은 사고원인 규명시까지 증거보전을 의무화하고 임의 자료삭제 또는 포맷을 금지한다.

제42조(사이버공격 대응) ① 국립국어원장은 소관분야의 사이버공격 대응절차를 수립·시행하고 이행실태를 지속 확인 점검하여야 한다.

② 국립국어원장은 국정원장이 경보 발령시 소관분야 직원을 대상으로 관련사항을 전파하고 대응조치를 이행하며 진행상황을 예의주시하는 등 대응절차에 따라 신속하게 대처하여야 한다.

③ 국립국어원장은 제2항에 따른 경보 단계별 조치사항을 본문화체육관광부장관을 경유하여 국정원장에게 통보하여야 한다.

④ 국정원장은 제1항 및 제2항과 관련하여 정보통신망에 대한 안전성을 확인할 수 있다.

⑤ 제1항 내지 제4항에 구체적으로 명시되지 않은 사항은「국가사이버안전관리규정」과「국가사이버안전매뉴얼」에 따른다.

제 5 장 보안적합성 검증

제43조(검증신청) 국립국어원장은 정보보호시스템을 도입·운용하고자 하는 경우 문화체육관광부장관을 경유하여 국정원장에게 안전성 확보를 위한 보안적합성 검증을 신청하여야 한다.

제44조(검증대상 제품) 보안적합성 검증대상제품은 다음과 같다

1. 국제공통평가기준(CC)에 따라 인증한 제품이나 국정원장이 그와 동등 한 효력이 있다고 인정한 제품
2. 국립국어원장이 자체 개발하거나 외부업체 등에 의뢰하여 개발한 제품

제45조(제품선정) ① 국립국어원장은 정보보호제품을 도입할 경우에는 사전에 별지 제10호 서식을 참조하여 보안기능 구현여부 및 업체 기술지원 가능 여부들을 점검하여야 한다.

② 국립국어원장은 정보보호제품의 안정적인 운용을 위해 도입시점부터 최소 1년이상 유지보수가 가능한 업체의 제품을 선정하여야 한다.

제46조(제출문서) ① 보안적합성 검증 신청에 필요한 제출문서는 다음과 같다.

1. 국제공통평가기준(CC) 인증제품
   가. 별지 제10호 서식의 정보보호제품 자체 점검결과 1부
   나. 별지 제8호 서식의 보안적합성 검증 신청서 1부
   다. 기술제안요청서 사본 1부
2. 자체 개발하거나 외부업체 등에 의뢰하여 개발한 제품
   가. 별지 제10호 서식의 정보보호제품 자체 점검결과 1부
   나. 별지 제8호 서식의 보안적합성 검증 신청서 1부
   다. 기술제안요청서 사본 1부
   라. 상세설계서 1부
   마. 개발완료 보고서 1부
   바. 제품사용설명서 1부

② 국정원장은 제1항의 제출문서 이외에 보안적합성 검증에 필요하다고 판단될 경우 추가 자료를 요청할 수 있다.

③ 제2항에 의거 추가 자료제출 요청을 받은 기관의 장은 특별한 사유가 없는 한 15일 이내에 제출하여야 한다.

④ 제1항 내지 제2항의 제출문서는 한글로 작성하여야 하다.

제47조(제품의 취약점 보완) ① 국립국어원장은 국정원장이 통보한 보안적합성 검증결과를 반영하여 도출된 취약점을 제거한 후 제품을 운용하여야 한다.

② 국립국어원장은 도입제품의 보안기능 및 보증등급 등이 전자정보 보안대책으로 적절치 않다고 검증된 경우 유사기능의 타 제품으로 대체하거나 지적된 사항을 보완하는 등의 조치를 하여야 한다.

제48조(제품의 활용범위) 보안적합성 검증이 완료된 제품은 비밀 및 대외비를 제외한 모든 전자정보를 보호하는데 사용할 수 있다.

제49조(목적이외 사용제한) 국립국어원장은 보안적합성 검증이 완료된 정보보호시스템에 대해 보안기능을 임의로 변경하거나 도입 목적이외의 용도로 운용하여서는 아니 된다.

제 6 장 안전성 확인

제50조(보안성 검토 신청) ① 국립국어원장은 다음 각 호의 정보화사업을 추진할 경우에 대하여 자체 보안대책을 강구하고 안전성을 확인하기 위하여 사업 계획단계(사업 공고 전)에서 국정원장에게 보안성 검토를 의뢰하여야 한다.

1. 비밀 등 중요자료의 생산, 등록, 보관, 사용, 유통 및 재분류, 이관, 파기 등 비 밀 업무와 관련된 정보시스템 및 네트워크 구축
2. 국가용 보안시스템과 상용 암호모듈·정보보호시스템을 도입 운용하고자 할 경우
3. 국방·외교 등 국가안보상 중요한 정보통신망 및 정보시스템의 구축
4. 대규모 정보시스템(10억 이상 사업) 또는 다량의 개인정보(100만명 이상)를 처리하는 정보시스템 구축
5. 전력·교통 등 국민생활과 밀접한 정보통신기반시설의 중요 제어시스템 구축
6. 내부 정보통신망을 인터넷이나 타 기관 전산망 등 외부망과 연동하는 경우
7. 업무망과 연결되는 무선 네트워크 시스템 구축
8. 와이브로·스마트폰 등 첨단 IT기술을 업무에 활용하는 시스템 구축
9. 원격근무시스템 구축
10. 정보통신망의 신·증설, 업무망과 인터넷 분리 사업
11. 그 밖에 국립국어원장 또는 국정원장이 보안성 검토가 필요하다고 판단하는 정보화사업

② 보안성 검토 대상 정보화사업에 관련된 구체적인 사항은 국가 정보보안 기본지침 부록2(정보화사업 보안성 검토 처리기준)을 참조한다.

③ 국립국어원장은 제1항에 명시된 보안성 검토 대상 사업의 경우에도 국정원장의 승인을 받아 보안성 검토를 생략할 수 있다.

제51조(보안성 검토 절차) ① 국립국어원장은 자체적으로 수립한 보안대책에 대하여 문화체육관광부장관을 경유하여 국정원장에게 보안성 검토를 요청한다.

② 정보통신망 보안성 검토는 서면 검토를 원칙으로 하며, 국정원장이 필요하다고 판단하는 경우에는 현장 확인을 병행 실시할 수 있다.

제52조(제출 문서) ① 국립국어원장은 정보통신망 보안성 검토를 요청할 경우에는 다음 각 호의 문서를 제출하여야 한다.

1. 사업계획서(사업목적 및 추진계획 포함)
2. 기술제안요청서(RFP)
3. 정보통신망 구성도(필요시, IP주소체계 추가)
4. 자체 보안대책 강구사항

② 제1항제4호의 자체 보안대책 강구사항에는 다음 각 호를 포함한다.

1. 보안관리 수행체계(조직, 인원) 등 관리적 보안대책

2. 정보시스템 설치장소에 대한 보안관리방안 등 물리적 보안대책
3. 국가용 보안시스템 및 국정원장이 개발하거나 안전성을 검증한 암호모듈· 정보보호시스템 도입 운용 계획
4. 국가기관간 망 연동시 해당 기관간 보안관리 협의사항
5. 서버, 휴대용 저장매체, 네트워크 등 정보통신망의 요소별 기술적 보안대책
6. 재난복구 계획 또는 상시 운용계획

제53조(결과 조치) ① 국립국어원장은 국정원장의 보안성 검토 결과를 준수하여 보안대책을 보완하여야 한다. 이 경우, 국정원장이 보안성 검토 결과 신속한 시정이 필요하다고 판단하는 경우에는 필요한 조치를 요청할 수 있으며 해당 기관의 장은 특별한 사유가 없는 한 이에 따라야 한다.

② 국정원장은 정보통신망 보안대책이 적절히 수립되었는지 등 이행여부 확인을 위하여 현장점검을 실시할 수 있다.

제54조(정보보호시스템의 도입 등) ① 국립국어원장은 정보 및 정보통신망 등을 보호하기 위해 정보보호시스템을 도입할 수 있다. 다만, 국가 정보보안 기본지침 별표3에 규정된 유형의 시스템에 대해서는 해당 도입요건을 만족하는 경우로 한정한다.

② 국정원장은 국가 정보보안 기본지침 별표3의 정보보호시스템 유형별 도입요건을 변경할 경우, 국립국어원장에게 관련 사항을 통보하여야 한다.

③ 제1항의 정보보호시스템에 중요자료 저장·소통을 위한 암호기능이 포함될 경우 아래와 같은 알고리즘 및 보호함수가 포함된 검증필 암호모듈을 탑재하여야 하며 구체적인 사항은 국정원장이 별도로 정한다.

1. 암호검증기준(KS X ISO/IEC 19790)에서 제시하는 보호함수
2. 그 밖에 국정원장이 사용을 허용한 암호 알고리즘

제55조(보안적합성 검증 신청) ① 국립국어원장은 정보보호시스템을 도입할 경우 문화체육관광부장관을 경유하여 국정원장에게 안전성 확보를 위한 보안적합성 검증을 신청하여야 한다.

② 보안적합성 검증대상은 다음 각 호와 같다.

1. 상용 정보보호시스템
2. 국립국어원장이 자체 개발하거나 외부업체 등에 의뢰하여 개발한 정보보호시스템
3. 보안성 검토 결과 세부 검증이 필요하다고 판단된 보안기능이 있는 정보시스템 및 제어시스템 등

③ 제3항에도 불구하고, 다음 각 호의 경우에는 검증을 생략할 수 있다.

1. 국정원장이 정한 국내용 CC 인증제도에 따라 인증을 받은 정보보호시스템

2. 국정원장이 안전성을 확인한 암호제품

3. 그 밖에 국정원장이 보안적합성 검증이 불필요하다고 인정한 시스템

제56조(제출문서) ① 보안적합성 검증 신청에 필요한 제출문서는 다음과 같다.

1. 상용 정보보호시스템

가. 국가 정보보안 기본지침 별지 제18호 서식의 정보보호시스템 도입시 확인사항 1부

나. 별지 국가 정보보안 기본지침 제19호 서식의 보안적합성 검증 신청서 1부

2. 개발 정보보호시스템

가. 1호 상용 정보보호시스템의 제출문서(가~다)

나. 상세설계서 1부

다. 개발완료 보고서 1부

라. 제품사용설명서 1부

② 국정원장은 제1항의 제출문서 이외에 보안적합성 검증에 필요하다고 판단될 경우 추가 자료를 요청할 수 있으며 이 경우, 국립국어원장은 특별한 사유가 없는 한 15일 이내에 추가 자료를 제출하여야 한다.

제57조(검증시험 및 결과조치) ① 국정원장은 각급기관으로부터 제출받은 문서에 대하여 타당성 및 적절성을 검토하고 시스템의 보안기능 정상동작 여부 등 안전성을 시험한다.

② 국정원장은 국가정보보안기술 연구개발을 수행하는 정부출연 연구기관의 장 등에게 안전성 시험을 의뢰할 수 있다.

③ 국립국어원장은 국정원장이 시스템 개발업체의 개발환경에 대한 보안관리 실태 점검을 요청할 경우 특별한 사유가 없는 한 협조하여야 한다.

④ 국정원장은 보안적합성 검증결과 취약점이 발견될 경우에는 이를 해당 기관에 통보한다.

⑤ 국립국어원장은 취약점을 통보받았을 때에는 30일 이내에 보완대책을 수립하여 조치하고 그 결과를 국정원장에게 통보하여야 한다.

제58조(사후 관리) ① 국립국어원장은 보안적합성 검증 완료 이후 시스템에 새로운 취약점이 발견될 경우에는 즉시 제거한 후 그 결과를 국정원장에게 통보하고 제거가 불가능할 경우에는 그 사실을 국정원장에게 통보하여 조치를 받아야 한다.

② 국정원장은 신규 취약점이 발견된 시스템에 대해 국립국어원장에게 취약점 제거를 요청할 수 있다.

③ 취약점 제거를 요청받은 국립국어원장은 특별한 사유가 없는 한 30일 이내에 이를 제거하고 그 결과를 국정원장에게 통보하여야 한다.

제59조(무단변경 및 오용금지) 국립국어원장은 보안적합성 검증이 완료된 정보보호시

스템에 대해 형상을 무단 변경하거나 도입 목적이외의 용도로 운용하여서는 아니된다.

제 7 장 정보시스템 보안관리

제60조(PC 등 단말기 보안관리) ① 단말기 사용자는 PC · 노트북 · PDA 등 단말기(이하 "PC 등"이라 한다) 사용과 관련된 일체의 보안관리 책임을 가진다.

② 정보보안담당관은 비인가자가 PC 등을 무단으로 조작하여 전산자료를 절취, 위 · 변조 및 훼손시키지 못하도록 다음 각 호의 보안대책을 단말기 사용자에게 지원하며, 사용자는 이를 준수하여야 한다.

1. 장비(CMOS 비밀번호) · 자료(문서자료 암호화 비밀번호) · 사용자(로그온 비밀번호)별 비밀번호를 주기적으로 변경 사용하고 지문인식 등 생체인식 기술 적용 권고
2. 10분 이상 PC 등의 작업 중단시 비밀번호 등이 적용된 화면보호 조치
3. PC용 최신 백신 운용 · 점검, 침입차단 · 탐지시스템 등을 운용하고 운영체제(OS) 및 응용프로그램(아래아한글, MS Office, Acrobat 등)의 최신 보안패치 유지
4. 업무상 불필요한 응용프로그램 설치 금지 및 공유 폴더 제한
5. 그 밖에 국가정보원장이 안정성을 확인하여 배포 승인한 프로그램의 운용 및 보안권고문

③ 사용자는 PC 등을 교체 · 반납 · 폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 정보보안담당관과 협의하여 하드디스크에 수록된 자료가 유출, 훼손되지 않도록 보안조치 하여야 한다.

④ 관리책임자는 사용자가 PC 등을 기관 외부로 반출하거나 내부로 반입할 경우에 최신 백신 등을 활용하여 해킹프로그램 감염 여부를 점검하여야 한다.

⑤ 개인 소유의 PC 등을 무단 반입하여 사용하여서는 아니된다. 다만, 부득이한 경우에는 정보보안담당관의 승인을 받아 사용할 수 있다.

제61조(서버 보안관리) ① 서버 관리자는 서버를 도입 운용할 경우, 정보보안담당관과 협의하여 해킹을 이용한 자료 절취, 위 · 변조 등에 대비한 보안대책을 수립 · 시행하여야 한다.

② 서버 관리자는 서버 내 저장자료에 대해 업무별 · 자료별 중요도에 따라 사용자의 접근권한을 차등 부여하여야 한다.

③ 서버 관리자는 사용자별 자료의 접근범위를 서버에 등록하여 인가여부를 식별토록 하고 인가된 범위 이외의 자료접근을 통제하여야 한다.

④ 서버 관리자는 서버의 운용에 필요한 서비스 포트 외에 불필요한 서비스 포트를 제거하며 관리용 서비스와 사용자용 서비스를 분리 운용하여야 한다.

⑤ 서버 관리자는 서버의 관리용 서비스 접속시 특정 IP와 MAC 주소가 부여된 관리용 단말을 지정 운용하여야 한다.

⑥ 서버 관리자는 서버 설정 정보 및 서버에 저장된 자료에 대해서는 정기적으로 백업을 실시하여 복구 및 침해행위에 대비하여야 한다.

⑦ 서버 관리자는 데이터베이스에 대하여 사용자의 직접적인 접속을 차단하고 개인정보 등 중요 정보를 암호화하는 등 데이터베이스별 보안조치를 실시하여야 한다.

⑧ 정보보안담당관은 제1항부터 제7항까지에서 수립한 보안대책의 적절성을 수시 확인하되, 연1회 이상 보안도구를 이용하여 서버 설정 정보 및 저장자료의 절취, 위·변조 가능성 등 보안취약점을 점검하여야 한다.

제62조(웹서버 등 공개서버 보안관리) ① 서버 관리자는 외부인에게 공개할 목적으로 설치되는 웹서버 등 공개서버를 내부망과 분리된 영역(DMZ)에 설치·운용하여야 한다.

② 국립국어원장은 비인가자의 서버 저장자료 절취, 위·변조 및 분산서비스거부(DDoS) 공격 등에 대비하기 위하여 국가정보원장이 안전성을 검증한 침입차단·탐지시스템 및 DDoS 공격대응시스템을 설치하는 등 보안대책을 강구하여야 한다.

③ 서버 관리자는 비인가자의 공개서버 비공개 정보에 대한 무단 접근을 방지하기 위하여 서버 접근 사용자를 제한하고 불필요한 계정을 삭제하여야 한다.

④ 공개서버의 서비스에 필요한 프로그램을 개발하고 시험하기 위하여 사용된 모든 도구(컴파일러 등)는 개발 완료 후 삭제를 원칙으로 한다.

⑤ 공개서버의 보안관리에 관련한 그 밖의 사항에 대해서는 제61조(서버 보안관리)에 따른다.

제63조(홈페이지 게시자료 보안관리) ① 국립국원장은 개인정보를 포함한 중요 업무자료가 홈페이지에 무단 게시되지 않도록 홈페이지 게시자료의 범위·방법 등을 명시한 자체 홈페이지 정보공개 보안지침을 수립 시행한다.

② 사용자는 개인정보, 비공개 공문서 및 민감내용 등이 포함된 자료를 홈페이지에 공개하여서는 아니된다.

③ 홈페이지에 중요 정보를 게시하고자 하는 부서의 장은 비밀 등 비공개 자료가 게시되지 않도록 하여야 한다.

④ 사용자는 인터넷 블로그·카페·게시판·개인 홈페이지 또는 소셜네트워크 서비스 등 일반에 공개된 전산망에 업무관련 자료를 무단 게재하여서는 아니된다.

⑤ 정보보안담당관은 홈페이지 등에 비공개 내용이 게시되었는지 여부를 주기적으

로 확인하고 개인정보를 포함한 비공개 자료가 홈페이지에 공개되지 않도록 보안교육을 주기적으로 실시하여야 한다.

⑥ 국립국어원장은 홈페이지에 중요 정보가 공개된 것을 인지할 경우 이를 즉시 차단하는 등의 보안조치를 강구 시행하여야 한다.

제64조(사용자계정 관리) ① 시스템관리자는 사용자에게 정보시스템 접속에 필요한 사용자계정(ID) 부여시 비인가자 도용 및 정보통신시스템 불법 접속에 대비하여 다음 각 호의 사항을 반영하여야 한다.

1. 사용자별 또는 그룹별로 접근권한 부여
2. 외부인에게 계정 부여는 불허하되 업무상 불가피시 기관장 책임하에 필요업무에 한해 특정기간 동안 접속토록 하는 등 보안조치 강구 후 허용
3. 비밀번호 등 사용자 식별 및 인증 수단이 없는 사용자계정 사용 금지

② 시스템관리자는 사용자가 5회 이상에 걸쳐 로그인 실패시 정보시스템 접속을 중단시키도록 시스템을 설정하고 비인가자의 침입 여부를 확인 점검하여야 한다.

③ 시스템관리자는 직원의 퇴직 또는 보직변경 발생시 사용하지 않는 사용자계정을 신속히 삭제하고, 특별한 사안이 없는 한 유지보수 등을 위한 외부업체 직원에게 관리자계정 제공을 금지하여야 한다.

④ 정보보안담당관은 사용자계정의 부여 및 관리가 적절한 지 연 2회 이상 점검하여 결과를 시스템관리자에게 통보하여야 한다.

제65조(비밀번호 관리) ① 사용자는 비밀번호 설정 사용시 정보시스템의 무단사용 방지를 위하여 다음 각 호와 같이 구분하여야 한다.

1. 비인가자의 정보통신시스템 접근방지를 위한 장비 접근용 비밀번호(1차)
2. 정보시스템 사용자가 서버 등 정보통신망에 접속 인가된 인원인지 여부를 확인하는 사용자인증 비밀번호(2차)
3. 문서에 대한 열람・수정 및 출력 등 사용권한을 제한할 수 있는 자료별 비밀번호(3차)

② 비밀이나 중요자료에는 자료별 비밀번호를 반드시 부여하되, 공개 또는 열람 자료에 대해서는 부여하지 아니할 수 있다.

③ 비밀번호는 다음 각 호의 사항을 반영하여 숫자와 영문자, 특수문자 등을 혼합하여 9자리 이상으로 정하고, 분기별로 1회 이상 주기적으로 변경 사용하여야 한다.

1. 사용자계정(ID)과 동이랗지 않은 것
2. 개인 신상 및 부서명칭 등과 관계가 없는 것
3. 일반 사전에 등록된 단어는 사용을 피할 것
4. 동일단어 또는 숫자를 반복하여 사용하지 말 것

5. 사용된 비밀번호는 재사용하지 말 것

6. 동일 비밀번호를 여러 사람이 공유하여 사용하지 말 것

7. 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지

④ 서버에 등록된 비밀번호는 암호화하여 저장하여야 한다.

제66조(네트워크장비 보안관리) ① 시스템관리자는 라우터, 스위치 등 네트워크 장비 운용과 관련하여 다음 각 호의 보안조치를 강구해야 한다.

1. 네트워크 장비에 대한 원격접속은 원칙적으로 금지하되, 불가피할 경우 장비 관리용 목적으로 내부 특정 IP・MAC 주소에서의 접속은 허용

2. 물리적으로 안전한 장소에 설치하여 비인가자의 무단접근 통제

3. 최초 설치시 보안취약점을 점검하여 제거하고 주기적으로 보안패치 실시

4. 불필요한 서비스 포트 제거

② 시스템관리자는 네트워크장비의 접속기록을 6개월 이상 유지하여야 하고 비인가자의 침투 여부를 주기적으로 점검하여 정보보안담당관에게 관련결과를 제출하여야 한다.

제67조(전자우편 보안대책) ① 시스템관리자는 웜・바이러스 등 악성코드로부터 사용자 PC 등 전자우편 시스템 일체를 보호하기 위하여 국가정보원장이 안전성을 확인한 백신, 바이러스 월, 해킹메일 차단시스템을 구축하는 등 보안대책을 강구하여야 한다.

② 사용자는 상용 전자우편을 이용한 업무자료 송・수신을 금지하며 기관 전자우편으로 송・수신한 업무자료는 열람 등 활용 후 메일함에서 즉시 삭제하여야 한다.

③ 사용자는 메일에 포함된 첨부파일이 자동 실행되지 않도록 설정하고 첨부파일 다운로드시 반드시 최신 백신으로 악성코드 은닉여부를 검사하여야 한다.

④ 사용자는 출처가 불분명하거나 의심되는 제목의 전자우편은 열람을 금지하고 해킹메일로 의심되는 메일 수신시에는 즉시 정보보안담당자를 경유하여 국가사이버안전센터에 신고하여야 한다.(신고메일 : cert@ncsc.go.kr)

⑤ 사용자는 전자우편을 사용하는 PC에 대하여 제60조(PC 등 단말기 보안관리) 및 제65조(비밀번호 관리)에 명시된 보안조치 사항을 따른다.

제68조(휴대용 저장매체 보안대책) ① 휴대용 저장매체 관리책임자는 휴대용 저장매체를 사용하여 업무자료를 보관할 필요가 있을 때에는 위변조, 훼손, 분실 등에 대비한 보안대책을 강구하여 정보보안담당관의 승인을 받아야 한다.

② 휴대용 저장매체 관리책임자는 휴대용 저장매체를 비밀용, 일반용으로 구분하고 주기적으로 수량 및 보관 상태를 점검하며 반출・입을 통제하여야 한다.

③ 휴대용 저장매체 관리책임자는 USB 관리시스템을 도입할 경우 국가정보원장이

안정성을 확인한 제품을 도입하여야 한다.

④ 휴대용 저장매체 관리책임자는 사용자가 USB메모리를 PC 등에 연결시 자동 실행되지 않도록 하고 최신 백신으로 악성코드 감염여부를 자동 검사하도록 보안설정한다.

⑤ 비밀자료가 저장된 휴대용 저장매체는 매체별로 비밀등급 및 관리번호를 부여하고 비밀관리기록부에 등재 관리하여야 한다. 이 경우에는 매체 전면에 비밀등급 및 관리번호가 표시되도록 하여야 한다. 다만, 휴대용 저장매체가 국가용 보안시스템에 해당될 경우에는 해당 보안시스템의 운용·관리체계에 따라 관리하여야 한다.

⑥ 휴대용 저장매체를 파기 등 불용처리하거나 비밀용을 일반용 또는 다른 등급의 비밀용으로 전환하여 사용할 경우 저장되어 있는 정보의 복구가 불가능하도록 완전삭제 프로그램을 사용하여야 한다.

⑦ 정보보안담당관은 사용자의 휴대용 저장매체 무단 반출 및 미등록 휴대용 저장매체 사용 여부 등 보안관리실태를 주기적으로 점검하여야 한다.

⑧ 그 밖에 휴대용 저장매체의 보안관리에 관련된 사항은 국가 정보보안 기본지침의 「USB메모리 등 휴대용 저장매체 보안관리지침」(부록 5)을 따른다.

제69조(악성코드 감염 방지대책) ① 국립국어원장은 웜·바이러스, 해킹 프로그램, 스파이웨어 등 악성코드 감염을 방지하기 위하여 다음 각 호와 같은 대책을 수립·시행하여야 한다.

1. 사용자는 개인PC에서 작성하는 문서·데이터베이스 작성기 등 응용프로그램을 보안패치하고 백신은 최신상태로 업데이트·상시 감시상태로 설정 및 주기적인 점검을 실시하여야 한다.
2. 사용자는 출처, 유통경로 및 제작자가 명확하지 않은 응용프로그램 사용을 금지하고 인터넷 등 상용망으로 자료 입수시 신뢰할 수 있는 인터넷 사이트를 활용하되 최신 백신으로 진단후 사용하여야 한다.
3. 사용자는 인터넷 파일공유 프로그램과 메신저·대화방 프로그램 등 업무상 불필요한 프로그램을 사용 금지하고 시스템관리자는 인터넷 연동구간의 침입차단시스템 등에서 관련 사이트 접속을 차단하도록 보안설정 하여야 한다.
4. 사용자는 웹브라우저를 통해 서명되지 않은(Unsigned) Active-X 등이 PC내에 불법 다운로드 되고 실행되지 않도록 보안설정 하여야 한다.
5. 제1호부터 제4호까지의 보안대책과 관련하여 시스템관리자는 정보보안담당관과 협조하여 사용자가 적용할 수 있는 보안기술을 지원하여야 한다.

② 시스템관리자 또는 PC 등의 사용자는 시스템에 악성코드가 설치되거나 감염된 사실을 발견하였을 경우에 다음 각 호의 조치를 하여야 한다.

1. 악성코드 감염원인 규명 등을 위하여 파일 임의삭제 등 감염 시스템 사용을 중지하고 전산망과의 접속을 분리한다.
2. 악성코드의 감염확산 방지를 위하여 정보보안담당관에게 관련 사실을 즉시 통보한다.

③ 제2항의 조치가 완료된 후 제12조제3항에 따라 정보보안 사고 조사권한이 국립국어원장(정보보안담당관)에게 위임되었을 경우, 정보보안담당관은 감염 PC 등에 대하여 다음 각 호의 조치를 하여야 한다.

1. 최신 백신 등 악성코드 제거 프로그램을 이용하여 악성코드를 삭제한다.
2. 감염이 심각한 경우 포맷 프로그램을 사용하여 하드디스크를 포맷한다.
3. 악성코드 감염의 확산 및 재발을 방지하기 위하여 원인을 분석하고 예방조치를 수행한다.

④ 국립국어원장은 악성코드가 신종이거나 감염피해가 심각하다고 판단할 경우에는 관련 사항을 국가정보원장에게 신속히 통보하여야 한다.

⑤ 국립국어원장은 국가정보원장이 기관에 악성코드 감염사실을 확인하여 조치를 권고할 경우, 즉시 이를 이행하여야 한다.

⑥ 그 밖에 정보보안 사고 조사와 관련한 사항에 대해서는 제12조(보안사고 처리 및 조사)를 따른다.

제70조(접근기록 관리) ① 시스템관리자는 정보시스템의 효율적인 통제·관리, 사고발생시 추적 등을 위하여 사용자의 정보시스템 접근기록을 유지 관리하여야 한다.

② 제1항의 접근기록에는 다음 각 호의 내용이 포함되어야 한다

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

③ 시스템관리자는 접근기록을 분석한 결과, 비인가자의 접속 시도, 정보 위변조 및 무단 삭제 등의 의심스러운 활동이나 위반 혐의가 발생한 사실을 발견한 경우 정보보안담당관에게 즉시 보고하여야 한다.

④ 접근기록은 정보보안 사고 발생시 확인 등을 위하여 최소 6개월 이상 보관하여야 하며 접근기록 위·변조 및 외부유출 방지 대책을 강구하여야 한다.

제71조(정보시스템 개발보안) ① 시스템 개발사업 담당자는 정보시스템을 자체적으로 개발하고자 하는 경우에는 다음 각 호의 사항을 고려하여 보안대책을 수립하고 정보보안담당관의 승인을 받아야 한다.

1. 독립된 개발시설을 확보하고 비인가자의 접근 통제

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

② 시스템 개발사업 담당자는 외부용역 업체와 계약하여 정보시스템을 개발하고자 하는 경우에는 다음 각 호의 사항을 고려하여 보안대책을 수립하고 정보보안담당관의 승인을 득하여야 한다.

1. 외부인력 대상 신원확인, 보안서약서 징구, 보안교육 및 점검
2. 외부인력의 보안준수 사항 확인 및 위반시 배상책임의 계약서 명시
3. 외부인력의 정보시스템 접근권한 및 제공자료 보안대책
4. 외부인력에 의한 장비 반입·반출 및 자료 무단반출 여부 확인
5. 제1항제1호부터 제3호까지의 사항

③ 정보보안담당관은 제1항 및 제2항과 관련하여 보안대책의 적절성을 수시로 점검하고 정보시스템 개발을 완료한 경우에는 정보보안 요구사항을 충족하는지 시험 및 평가를 수행하여야 한다.

제72조(정보시스템 유지보수) ① 국어정보원장은 정보시스템 유지보수와 관련한 절차, 주기, 문서화 등에 관련된 사항을 자체 규정에 포함하여야 한다. 유지보수 절차 및 문서화 수립시 고려사항은 아래의 각 호와 같다.

1. 유지보수 인력에 대해 보안서약서 집행, 보안교육 등을 포함한 유지보수 인가 절차를 마련하고 인가된 유지보수 인력만 유지보수에 참여한다.
2. 결함이 의심되거나 발생한 결함, 예방 및 유지보수에 대한 기록을 보관한다.
3. 유지보수를 위하여 원래 설치장소 외 다른 장소로 정보시스템을 이동할 경우, 통제수단을 강구한다.
4. 정보시스템의 유지보수시에는 일시, 담당자 인적사항, 출입 통제조치, 정비내용 등을 기록·유지하여야 한다.

② 시스템관리자는 자체 유지보수 절차에 따라 정기적으로 정보시스템 정비를 실시하고 관련 기록을 보관하여야 한다.

③ 시스템관리자는 정보시스템의 변경이 발생한 경우, 정보보안담당관과 협조하여 정보시스템의 설계·코딩·테스트·구현과정에서의 보안대책을 강구하며 정보보안담당관은 관련 적절성을 주기적으로 확인하여야 한다.

④ 정보보안담당관은 시스템관리자 등이 유지보수와 관련된 장비·도구 등을 반출입할 경우, 악성코드 감염여부, 자료 무단반출 여부를 확인하는 등 보안조치 하여야 한다.

⑤ 시스템관리자는 외부에서 원격으로 정보시스템을 유지보수하는 것을 원칙적으로 금지하여야 하며 부득이한 경우에는 정보보안담당관과 협의하여 자체 보안대책을 강구한 후 한시적으로 허용할 수 있다.

제73조(전자정보 저장매체 불용처리) ① 사용자 및 시스템관리자는 하드디스크 등 전자정보 저장매체를 불용처리(교체・반납・양여・폐기 등) 하고자 할 경우에는 정보보안담당관의 승인하에 저장매체에 수록된 자료가 유출되지 않도록 보안조치 하여야 한다.

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

③ 국립국어원에서 정보시스템의 사용자가 변경된 경우, 비밀처리용 정보시스템은 완전포맷 3회 이상, 그 외의 정보시스템은 완전포맷 1회 이상으로 저장자료를 삭제하여야 한다.

④ 전자정보 저장매체의 불용처리에 관련된 구체적인 사항은 국가 정보보안 기본지침 「정보시스템 저장매체 불용처리지침」(부록 6)을 따른다.

제 8 장 행정업무 모바일 서비스 보안관리

제74조(서비스 운영시 준수사항) ① 국립국어원장은 행정업무 모바일 서비스의 구축・운영 시 다음 각 호의 지침 및 가이드라인 등을 준수하여야 한다.

1. 모바일 전자정부 서비스 관리 지침
2. 모바일 전자정부 서비스 사용자 인터페이스 설계 지침
3. 대국민 모바일 서비스 구축 가이드라인
4. 행정업무 모바일 서비스 구축 가이드라인
5. 모바일 전자정부 서비스 공통기반 및 지원센터 활용 가이드라인
6. 모바일 전자정부 표준 프레임워크 활용 가이드라인
7. 국가・공공기관 업무용 스마트폰 보안 규격(국가정보원)

제75조(모바일 기기의 보안관리) ① 국립국어원장은 행정업무 모바일 서비스를 이용하려는 자에게 보안서약서를 징구 하여야 한다.

② 각급기관의 모바일 정보보안 담당관은 행정업무 모바일 서비스를 이용하려는 자의 모바일 기기에 설치된 모든 모바일 애플리케이션이 설치허용앱목록에 포함되어 있는지 여부를 확인한 후 행정업무 모바일 서비스 접속용 보안 소프트웨어를 설치하여야 한다.

③ 행정업무 모바일 서비스 이용자는 모바일 기기를 분실하였을 경우에는 지체 없이 모바일 정보보안 담당관에게 신고하여야 하며, 모바일 정보보안 담당관은 해당 모바일 기기 관리자의 동의를 받아 원격 모바일 기기 잠금, 모바일 기기 초기화 등의 필요한 조치를 수행하여야 한다.

④ 모바일 행정업무 서비스 이용자가 모바일 기기를 교체 또는 폐기 할 경우 모바일 정보보안 담당관에게 신고하여야 하며, 모바일 정보보안 담당관은 행정업무 모바일 서비스 접속용 보안 소프트웨어의 비활성화, 삭제 등의 필요한 조치를 수행하여야 한다.

⑤ 각급기관의 모바일 정보보안 담당관은 제1항부터 제4항까지의 효율적인 업무 수행을 위하여 행정업무 모바일 서비스 이용자의 근무지 위치, 업무특성 등에 따라 필요시 별도의 모바일 분임관리자를 지정할 수 있다.

⑥ 제5항에 따라 모바일 분임관리자를 지정한 경우, 각급기관의 모바일 정보보안 담당관은 모바일 분임관리자가 행정업무 모바일 서비스 접속용 보안소프트웨어의 배포 및 설치를 안전하게 수행하도록 보안관리를 하여야 한다.

⑦ 행정업무 모바일 서비스 이용자는 다음의 사항을 준수하여야 한다.

1. 모바일 기기의 설치허용앱목록 검사 및 허용되지 않는 앱의 삭제
2. 모바일 기기의 운영체계 임의 변조 금지
3. 행정업무 모바일 서비스 접속용 소프트웨어 및 업무관련 자료를 모바일 기기 내부에 복사하거나 외부에 유출 금지
4. 비밀번호 설정 기능을 이용하고 정기적인 비밀번호 변경 관리
5. 운영체제 및 백신 프로그램을 최신 버전으로 유지
6. 발신인이 불명확하거나 의심스러운 메시지 또는 메일 열람 금지
7. 모바일 기기의 이상 동작 탐지시 악성코드 감염여부 등 확인・조치
8. 작성자/배포처가 불분명한 앱(App) 설치 금지 및 신뢰할 수 없는 웹 사이트 접속 금지
9. 행정업무 모바일 서비스 접속 시 해당 용도 이외의 모바일 애플리케이션 및 무선랜, 테더링, 카메라, 화면캡처, 블루투스, 마이크 등 타 프로세스 실행 금지)

제 9 장　보안조사

제76조(보안사고) ① 보안사고가 발생하였을 때에는 지체 없이 본부 정보보안담당관에게 보고하여야 하며, 정보보안담당관은 사고전말을 신속히 조사하여 국립국어원장에게 보고한 후 즉시 보안사고의 통보를 하여야 한다.

② 보안사고의 범위는 다음 각 호와 같다.

1. 비밀의 누설 또는 분실
2. 공무원의 행방불명, 납치 및 피살

3. 시설물에 대한 방화 및 파괴
4. 보안관련 주요장비 및 기재의 도난
5. 기타 제1호 내지 제4호의 규정에 준하는 사고

③ 비밀의 누설 또는 분실시에는 그 비밀의 발행기관 및 배포기관에도 통보하여야 하며, 보안사고의 내용은 발생경위 및 이에 대한 전말조사가 종결될 때까지 공개하여서는 안된다.

④보안사고를 발생하게 한 자, 사고를 은폐한 자 또는 발생을 인지하고도 보고하지 아니한 자에 대하여는 문책하여야 한다.

제10장 정보보안업무 세부시행계획 및 정보보안교육 등

제77조(보안업무 세부시행계획 수립 및 심사분석) ① 국립국어원장은 매년 초에 문화체육관광부 보안업무 세부시행계획에 의거 구체적이고 실현가능성 있게 자체 보안업무 세부시행계획을 수립·시행한다

② 국립국어원장은 자체 보안업무 세부시행계획에 대한 심사분석을 실시하고, 그 결과를 매년 10월 10일까지 본부 정보보안담당관에게 제출한다.

③ 제2항의 규정에 의한 심사분석은 자체세부시행계획에 의한 보안업무 수행과정에서 도출된 문제점과 부진사항에 대한 원인을 정밀분석, 그에 대한 개선대책을 구체적으로 강구한다.

제78조(보안교육) ① 정보보안담당관은 자체보안업무의 향상 발전을 위하여 연간 보안교육계획을 수립하여 시행하고, 소속 전 직원을 대상으로 년 2회 이상의 보안교육을 실시한다.

② 직무교육(전 직원 또는 신규 채용자 대상)을 실시할 때에는 보안업무 기초개념에 대한 보안교육과정을 포함한다.

③ 신규임용자, 전입자 및 비밀취급인가 예정자, 공무 해외출장자, 퇴직예정자에 대하여는 사전에 필요한 기본 보안교육을 충분히 실시하여야 한다.

④ 제1항의 규정에 의한 연간 보안교육계획에는 다음 각호의 사항이 포함되어야 한다.

1. 세부교육시간계획
2. 교육대상
3. 교육방법
4. 교육내용(보안관계법규 규정 해설, 정보통신보안, 보안실무 및 기타 국가보안 전반에 관한 사항)

⑤ 국립국어원장은 정보보안 관련 전문기관 교육 및 기술 세미나 참석을 장려하는 등 정보보안 담당자의 업무 전문성을 제고하기 위하여 노력하여야 한다.

제79조(준용) 동 규정에서 명시되지 않은 사항은 '국가 정보보안 기본지침', '국가사이버안전 매뉴얼' 및 '문화체육관광부 보안업무규정 시행세칙'을 준용한다.

부 칙 <2013. 12. 26.>

이 규정은 발령한 날부터 시행한다.

부 칙 <2014. 3. 10.>

이 규정은 발령한 날부터 시행한다.

[별표 1]

정보보안 위규사항

조	내 용	항	세 부 내 용
1	불온통신에 관한 사항	(1) (2) (3) (4)	북한 통신소와의 불법교신 국내침투 간첩과의 교신 적성국(또는 반국가단체) 통신소와의 불법교신 기타 반국가적인 불온통신
2	군사상 기밀의 누설	(1) (2) (3) (4) (5) (6) (7) (8)	군사전략, 작전계획 및 진행사항 군 편제·임무·시설 및 기타 부대현황 병력(군·경·예비군) 현황 및 이동 상황 경찰 및 특수기관의 장비(작전·정보·수사용) 현황과 집행사항 특수기관·군사시설의 위치 및 이동상황 군사장비의 구성·성능 및 발명개량 연구사항 군사장비(군수품 등) 생산 및 공급사항 기타 국가방위에 영향을 초래하는 사항
3	외교상 기밀의 누설	(1) (2) (3) (4)	국가 외교방침, 기본계획 및 재외공관에 발하는 훈령 공개할 수 없는 외교조약 또는 협약 특수임무를 수행하는 해외주재원의 활동(계획· 지시·보고) 및 신원정보에 관한 사항 기타 국가외교에 영향을 초래하는 사항
4	국가정보활동에 관한 사항 누설	(1) (2) (3) (4)	대공업무와 관련된 사항 정보(첩보) 수집활동에 관한 사항 간첩 또는 대공용의자 발견과 수사활동 정보 및 특수수사기관의 기구 또는 임무기능에 관한 사항

조	내 용	항	세 부 내 용
4	국가정보활동에 관한 사항 누설	(5) (6) (7) (8) (9) (10)	국가원수 및 기타 요인의 비공개행사 불명선박의 발견 및 처리 중요물자 수송활동 테러·마약·밀수 및 국제범죄조직에 관한 정보·수사활동 적 또는 경쟁국에 유리한 과학기술 및 산업에 관한 정보 기타 국가안보 및 공안유지에 불리한 영향을 초래하는 사항
5	국가용 보안시스템에 관한 사항 누설	(1) (2) (3) (4) (5) (6) (7) (8)	국가용 보안시스템의 연구개발 및 제작에 관한 사항 암호전문을 허위로 조립하여 송신 암호를 부정한 목적에 사용하였을 때 암호문과 평문의 혼용 및 이중사용 암호문 작성시 동일 난수를 2회이상 반복사용 사용기간이 경과된 보안자재를 계속 사용 암호문에 평문을 삽입하여 송신 기타 국가용 보안시스템 보호체계를 손상시킬 우려가 있는 사항
6	비인가 통신시설 및 통신제원 사용에 관한 사항 누설	(1) (2) (3) (4) (5)	비인가된 무선시설의 설치운용 비인가된 무선시설과 교신 비인가된 호출부호 및 주파수 사용 비인가된 전파형식 사용 지정출력의 초과사용
7	허가목적외 방법으로 사용하는 경우	(1) (2) (3)	허가목적 업무와 관련이 없는 통신 군 통신망에서 군사업무와 관련이 없는 통신 기타 사회질서를 해하는 통신

[별표 2]

정보보안사고 유형

조	내 용	항	세 부 내 용
1	정보시스템 및 정보통신실	(1) (2) (3) (4)	정보통신망에 대한 해킹·악성코드의 유포 비밀이 저장된 PC, 보조기억매체 등 분실 정보시스템 및 정보통신실 파괴 중요 정보시스템 기능 장애 및 정지
2	암호장비	(1) (2) (3) (4) (5) (6)	암호장비 분실 및 피탈 암호장비 파손 및 임의파기 암호장비 복제·복사 비인가 암호장비 사용 암호장비 비닉체계 특성 및 제원 노출 암호장비 키 운용체계 노출
3	보안자재	(1) (2) (3) (4)	암호·음어·약호자재의 분실 및 누설 암호·음어·약호자재의 파손 및 임의파기 암호·음어·약호자재의 임의제작 사용 세부 암호체계 노출
4	전자정보 (전자문서 및 전자기록물)	(1) (2) (3)	주전산기(주요 서버 등)·대용량 전자기록(DB) 손괴 전자정보의 위조·변조·훼손 및 유출 비밀의 평문 보관 및 유통

<별지 제1호서식>

신원조사 대상자 명단

요청기관 :

연번	성 명	생년월일	직위 및 직급	조사목적	본적 및 주소	비고
					본적 : 주소 :	
					본적 : 주소 :	
					본적 : 주소 :	
					본적 : 주소 :	
					본적 : 주소 :	
					본적 : 주소 :	
					본적 : 주소 :	

<별지 제2호서식>

PERSONAL BACKGROUND(소개서)

※ THIS INFORMATION IS ONLY FOR OFFICIAL USE

FULL NAME (성명)		DATE OF BIRTH (생년월일)		NATIONALITY (국적)		PHOTO	
ADDRESS (주소)							
OCCUPATION (직업)	WORKPLACE(직장명) : LOCATION (소재지) :			TELEPHONE NUMBER (전화)	WORK(직장) : HOME (집) :		
RELIGION (종교)		BLOOD TYPE (혈액형)		WEIGHT (체중)	kg	HEIGHT (신장)	cm

EDUCATION (학력)	SCHOOL (학교명)	PERIOD (MONTH/YEAR-MONTH/YEAR) (기간)	SPECIALTY (전공)	DEGREE (학위)	LOCATION (소재지)
		-			
		-			
		-			
		-			

CAREER (경력)	WORKPLACE (직장명)		PERIOD (MONTH/YEAR - MONTH/YEAR) (기간)			TITLE (지위)
			-			
			-			
			-			
			-			
FAMILY (가족 사항)	RELATION (관계)	FULL NAME (성명)	DATA OF BIRTH (생년월일)	EDUCATION (학력)	OCCUPATION (직업)	ADDRESS(CITY, COUNTRY) (주소)
					DATE (작성일) : SIGNATURE (서명) :	

<별지 제3호서식>

서 약 서

본인은 년 월 일부로 으로 근무함에 있어 다음 사항을 준수할 것을 엄숙히 서약한다.

1. 본인은 비밀로 분류될 성질의 업무를 수행함에 있어 이에 관련된 소관업무가 국가안전보장에 관한 기밀임을 인정한다.
2. 본인은 이 기밀을 누설함이 이적행위가 됨을 자각하고 보안관계 제규정을 시간과 지역에 제한없이 성실히 이행하며 재직중은 물론 퇴직후에도 직무상 지득한 제반 비밀사항을 일체 누설하지 않을 것을 서약한다.
3. 본인이 기밀을 누설한 때에는 동기 여하를 막론하고 그 결과가 반국가적 행위임을 자인하고 아래 제법규에 의거하여 엄중한 처벌을 받을 것을 서약한다.

가. 국가보안법 제4조제1항제2호 및 제5호(국가기밀누설등)
나. 형법 제99조(일반이적)
다. 형법 제127조(공무상 비밀의 누설)
라. 군형법 제14조제8호(일반이적)
마. 군형법 제80조(군사기밀 누설)
바. 군사기밀보호법 제8조(업무상 누설)
사. 군사기밀보호법 제9조(과실 누설)

년 월 일

서 약 자	소속	직급 직위	생년월일 성 명	(인)
서약집행자	소속	직급 직위	생년월일 성 명	(인)

<별지 제4호서식>

통 제 구 역 출 입 자 명 부

년·월·일 시 간	용 무	출 입 자		입 회 (피면회) 자			비 고
		연 락 처	성 명	직 급	성 명	인	

<별지 제5호 서식>

정보보안업무 세부 추진계획

< 작성 요령 >

1. 활동 목표
2. 기본 방침
3. 세부 추진계획

분야별	사업명	세부 추진계획	주관・관련부서	비고

* 보안성 검토 대상여부 표기

4. 전년도 보안감사・지도방문시 도출내용과 조치내역

도 출 내 용	조 치 내 역	담당부서

* 형식위주의 계획수립을 지양하고 소속 및 산하기관의 추진계획을 종합, 자체 실정에 맞게 작성

<별지 제6호 서식>

정보보안업무 심사분석

1. 총　　평
2. 주요 성과 및 추진사항
3. 세부 사업별 실적 분석

추진계획	추진실적	문제점	개선대책

* 추진실적은 목표량과 대비하여 성과달성도를 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 제7호 서식>

정보시스템 관리대장

연번	소속	취급자 (성명)	관리번호	종류 (서버・PC 등)	비밀번호 (필요시 장비용・사용자인증용・ 자료용으로 구분)	인증번호	인증 부여 일자	인증 해제 일자

<별지 제8호 서식>

보안적합성 검증 신청서

<table>
<tr><td rowspan="7">신청기관</td><td>기관명</td><td colspan="3"></td><td>운용부서</td><td colspan="2"></td></tr>
<tr><td>도입목적</td><td colspan="6"></td></tr>
<tr><td rowspan="2">운용환경</td><td>사용자 수</td><td colspan="2"></td><td>망 구성</td><td colspan="2">□유선 □무선</td></tr>
<tr><td>속도(대역폭)</td><td colspan="5"></td></tr>
<tr><td>운용형태</td><td colspan="6">□ 단독 설치·운용 □타 보안제품과 연동 □대 국민 배포용</td></tr>
<tr><td>연동
시스템</td><td colspan="6">□ ERP □ KMS □ CRM □ 전자결재 □ 기타 그룹웨어</td></tr>
<tr><td>사업명</td><td colspan="6"></td></tr>
<tr><td rowspan="9">신청제품</td><td>업체명</td><td colspan="3"></td><td>대표자</td><td colspan="2"></td></tr>
<tr><td>주소</td><td colspan="3"></td><td>전화번호</td><td colspan="2"></td></tr>
<tr><td rowspan="3">제품명</td><td colspan="3" rowspan="3">* 신청제품이 2種 이상인 경우, 추가기재</td><td>CC
인증번호</td><td colspan="2"></td></tr>
<tr><td>암호
검증번호</td><td colspan="2"></td></tr>
<tr><td>용역개발
여부</td><td colspan="2">□ 예 □ 아니오</td></tr>
<tr><td>평가기관</td><td></td><td>인증기관</td><td></td><td>등급</td><td colspan="2"></td></tr>
<tr><td rowspan="3">담당자</td><td>전화번호</td><td colspan="5"></td></tr>
<tr><td>휴대폰번호</td><td colspan="5"></td></tr>
<tr><td>E-mail</td><td colspan="5"></td></tr>
<tr><td>암호모듈</td><td colspan="6">□없음 □있음 (□검증 □미검증)</td></tr>
</table>

<별지 제9호 서식>

대 외 비 관 리 기 록 부

관리 번호	수발			문서 번호	형태	건 명	사본 번호	예고문	처리 담당	보관 장소	재분류				참조	
	년월일	발행처	수신처								등급 변경	파기	파기 확인	근거	영수증	수령자(인)

※ 삭제 방법 형태부터 사본번호까지 두줄로 삭제 (_____)

<별지 제10호 서식>

정보보호제품 자체 점검결과

항목명	점검 항목	결과
인증여부	EAL 2 이상 CC인증서 획득 여부	
	CC 미인증의 경우, 검증필 제품목록 등재 여부(09.5.31限)	
	국정원장이 검증한 암호모듈 탑재 여부	
일치성	CC 인증보고서와 도입제품 보안기능 일치성 여부	
	기술제안서(RFP)에서 요구하는 보안기능 구현 여부	
운용환경	운용환경 설치에 따른 제품기능 등 형상변경 가능 여부	
	도입기관의 시스템 관리자 지정여부	
	감사기능 지원 여부	
	도입기관 주요업무 및 최대사용자 등에 대한 가용성 보장 여부	
유지보수	보안적합성 검증결과 반영 가능 여부	
	업체 기술지원 전담조직 운영 여부	
	작동중단 등 긴급상황에 대비한 지원절차 구비 여부	
	업체 유지보수 매뉴얼 제공 여부	
	한글 관리자 설치·운영 매뉴얼 제공 여부	
	업체의 제품운용교육 제공 여부	
	신규취약성에 대한 통보 및 처리절차 구비 여부	

※ 점검결과는 O, X로 표기

<별지 제11호 서식>

「사이버 · 보안 진단의 날」 실시 결과

번호	구분	단 순 점 검 항 목	(○ / X)
1	보안 진단 실시	「사이버 · 보안 진단의 날」 자체 시행계획을 수립하였는가?	
2		진단의 날 행사 관련 1주前 자체 업무망에 공지하였는가?	
3	상용 메일	상용메일 사용이 차단되어 있는가?	
4	국가 보안	자체 보안업무 시행세칙에 진단의 날 시행내용을 포함, 개정을 완료 또는 추진중인가?	
5		보유비밀에 대한 전수조사 및 안전지출을 실시하였는가? (매회 2~3개 과단위 윤번제 실시)	
6		비밀취급은 현 보직에 적절하게 인가되어 있는가?	
7		사무실 복도, 복사기 · 팩스 사용후 문건방치 여부를 점검하였는가?	
8		폐휴지 처리시에 비밀 · 중요문건 무단 유기 여부를 점검하였는가?	

번호	구분	상 세 점 검 항 목	PC 대수
1	PC 진단 실시	자체 보유중인 PC는 모두 몇 대입니까? *** 망분리 완료된 기관에서는 인터넷PC 수**	전체 PC ( )
2		PC진단프로그램(내PC지키미)이 설치된 PC는 몇 대입니까?	설치 PC ( )
3		진단의 날 기간중 내PC지키미를 실행한 PC는 몇 대입니까?	실행 PC ( )
4	내PC 지키미 진단 결과 보완	바이러스 백신이 설치된 PC는 모두 몇 대입니까?	백신이 설치된 전체 PC ( )
5		진단의 날 기간중 새로 백신을 설치한 PC는 몇 대입니까?	신규 설치 PC ( )
6		진단의 날 기간중 바이러스를 치료한 PC는 몇 대입니까?	웜 · 바이러스를 치료한 PC ( )
7		진단의 날 기간중 백신을 업데이트한 PC는 몇 대입니까?	신규 백신 업데이트 PC ( )
8		운영체제 · MS Office의 최신 보안패치가 설치된 PC는 모두 몇 대입니까?	OS · Office 보안패치 설치 전체 PC ( )
9		진단의 날 기간중 운영체제 · MS Office 최신 보안패치를 새로 설치한 PC는 몇 대입니까?	신규 OS · Office 보안패치 PC ( )

<별지 제 12호 서식>

행정업무 모바일 서비스 이용 보안 서약서

본인은 ____년____월____일부로 행정업무 모바일 서비스를 이용함에 있어 다음 사항을 준수할 것을 엄숙히 서약하며 위반 시 관련규정에 따라 책임을 질 것을 서약합니다.

1. 본인은 업무용 모바일 서비스 접속을 위해 설치된 보안소프트웨어 등을 임의로 삭제하거나 변경하지 아니한다.
2. 본인은 미 인가된 사용자 접속 또는 모바일 기기 잠김 등을 미연에 방지하기 위하여 모바일 기기의 USIM을 임의로 변경하여 아니한다.
3. 본인은 모바일 기기에 설치허용앱목록에 포함된 모바일 서비스만 이용하고, 운영체제를 변경하거나, 임의로 공장초기화를 하지 아니한다.
4. 본인은 행정업무 모바일 서비스 사용을 위해 부여된 ID, 비밀번호, 인증서 등이 외부로 유출되지 않도록 철저히 관리한다.
5. 본인은 모바일 기기 분실 및 도난 시 모바일 정보보안 담당관에게 즉시 통보하여 모바일 기기 잠금, 중요데이터 삭제 등을 통해 정보 유출 방지에 적극 참여한다.
6. 본인은 모바일 기기 교체 또는 폐기 시 사전에 모바일 정보보안 담당관에게 신고하여 모바일 기기에 설치된 보안소프트웨어, 행정업무 모바일 서비스를 삭제한다.
7. 본인은 모바일 서비스를 이용함에 있어 국가정보원 및 모바일 전자정부지원센터 관련 규정 및 지침을 준수한다.

년 월 일

개인정보취급

○ 개인정보보호법 제15조 ①항(개인정보의 수집·이용)에 의거, 고유식별번호를 제공할 것을 동의합니다.

☐ 동의합니다. ☐ 동의하지 않습니다.

서 약 자	소 속 :	
	직 급 :	
	성 명 :	(서명)