목 차 Contents

제1편 보안 실무 편람

제2편 보안업무 관계 규정

관련규정은 이하 다음과 같이 약칭한다.

- 보안업무규정(대통령령)
- 농림수산식품부보안업무시행세칙(훈령)
- 농림수산식품부정보보안지침(훈령)
- 보안업무규정시행규칙(대통령훈령)
- 국가 정보보안 기본지침(국정원)

보안 실무 편람

제1편

I 보안일반

Ⅰ 보 안 일 반

❶ 보안의 중요성

외부로 누출, 누설될 경우 국가안보에 영향을 미침
⇒ 따라서 규정과 방침, 규칙을 벗어난 재량과 융통성에 제한이 따름

Point
- 보안활동은 그 성격이 비능률적·비경제적인 것이라 하더라도, 보호할 가치가 있기 때문에 보호하는 것임

❷ 보안의 개요

가. 보안의 의의

어느 개인이나 조직 또는 국가가 그 존립을 확보하거나 경쟁에서 승리하는 데 필요한 요소를 찾아 그것을 보호하기 위해 취하는 총체적 방위수단 및 활동

나. 보안의 목적

– 보안의 궁극적 목적은 국가안보 및 현대국가의 존립을 위한 국가 이익 확보
- 각종 위해행위로부터 국민의 생명을 보호하고
- 각종 파괴행위로부터 국가재산 보호 및 국가의 안전 도모하며
- 국내·외적으로 국가의 지위 및 이익을 유리하게 하는데 있음

다. 보안의 주체

보안의 주체는 국가이며, 보안업무의 실제 수행은 국가기관, 공공단체 또는 국가로부터 위임받은 개인, 법인임

Point
- 보안은 비밀을 취급하는 사람만이 하는 업무다 (×)

라. 보안의 대상

– 일반대상 : 비밀, 인원, 문서, 자재, 시설, 지역, 장비통신 등의 정적 보호
– 특별대상 : 간행물, 공연물, 우편물, 출·입국자 등의 동적 보호

Point
- 보안은 비밀의 보호가 전부다 (×)

마. 보안의 책임(규정 제3조)

국가안전보장에 관련되는 인원, 문서, 자재, 시설 및 지역을 관리하는 자와 관계기관의 장은 이에 대한 보안책임을 짐

Point

- 보안사고 유발시 인사상 불이익을 받게됨
- 국가안전보장에 위해를 가져온 경우 관계 직원은 행정(징계) 및 형사상의 책임을 져야하며, 기관장은 행정적 책임을 지게 됨

바. 보안의 종류

① 인원보안 ② 문서보안
③ 시설보안 ④ 정보보안(전산분야, 통신분야)

① 인원보안 : 적정한 자격이 있는 자로 하여금 보안업무를 수행토록 사전에 심사하고, 신분·자격을 취득한 자에 대하여는 사후 관리감독을 하는 것
⇒ 신원조사, 보안교육, 보안조치 등

② 문서보안 : 국가기밀이 수록된 문서에 대하여 그 수록된 기밀이 누설되지 않도록 취해지는 일체의 수단과 방법
⇒ 비밀의 생산, 취급, 관리, 파기 등에 있어 엄격한 절차 및 방법 규정

③ 시설보안 : 불순분자의 각종 침해행위 또는 재난으로부터 대상시설을 보호하기 위해 취해지는 보호대책
⇒ 보호구역(제한지역, 제한구역, 통제구역으로 구분) 및 방법 규정

④ 정보보안 : 각종 전기통신수단에 의해 발신되는 내용을 적국 또는 비인가자로부터 보호하기 위해 취해지는 각종 수단과 방법
⇒ 방화벽, 침입탐지시스템 등 다양한 방법이 도입되고 있음

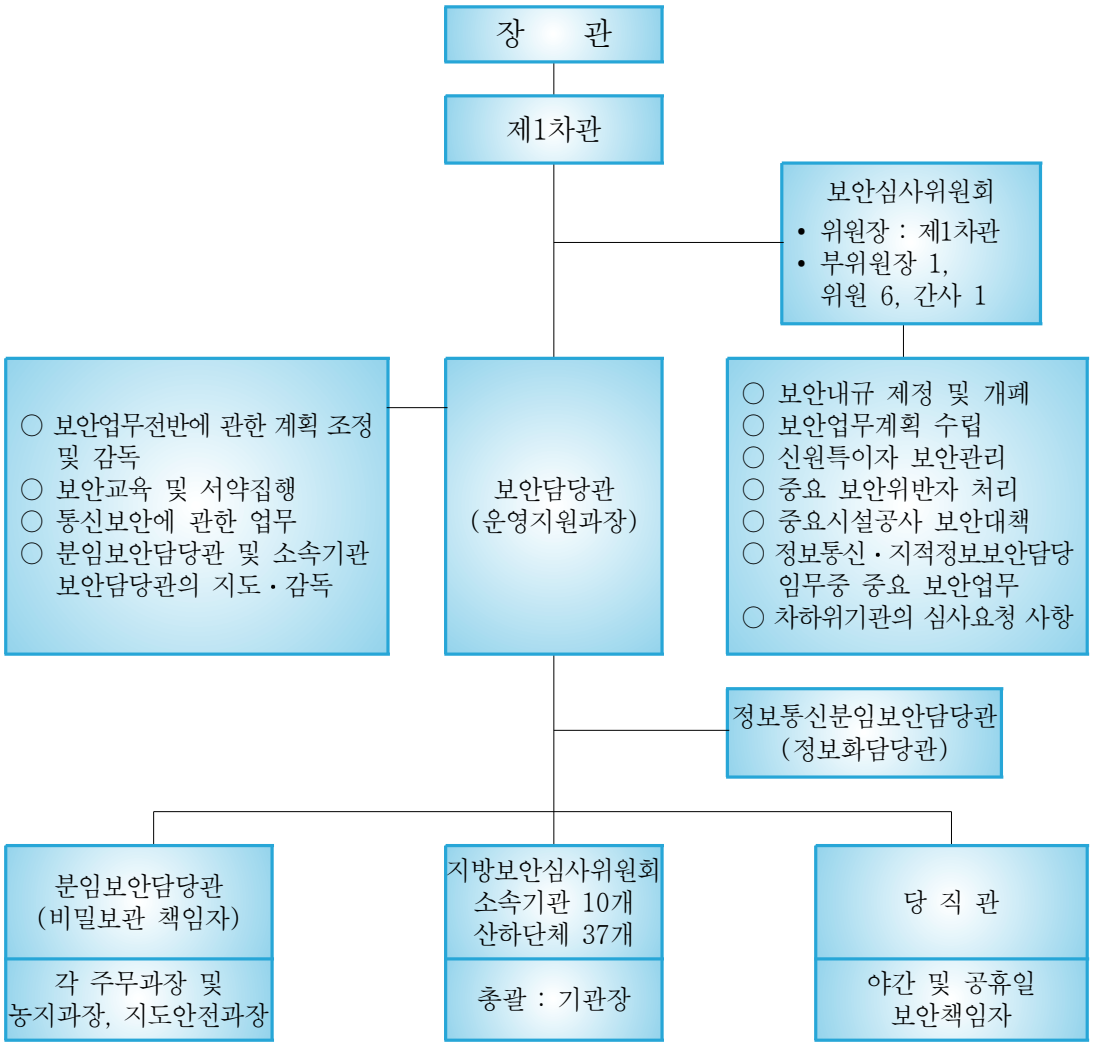
사. 보안의 취약성

① 무지와 몰이해 ② 속단 및 습관
③ 무관심과 타인 신뢰 ④ 과시욕과 자만

아. 보안업무관계 법규

- 정부조직법(2008. 2. 29. 법률 제8867호)
- 국가정보원법(2007. 1. 1. 법률 제8050호)
- 국가보안법(1998. 1. 1. 법률 제5454호)
- 정보 및 보안업무 기획 조정규정(2008. 12. 31. 대통령령 제21214호)
- 보안업무규정(2006. 3. 29. 대통령령 제19431호)
- 보안업무규정시행규칙(2005. 6 25. 대통령훈령 제149호)
- 국가 사이버 안전 관리규정(2005. 1. 31. 대통령훈령 제141호)
- 농림수산식품부보안업무시행세칙(2009. 4. 3. 훈령 제83호)
- 신원조사업무지침(2008. 9. 1. 국가정보원)
- 전자문서 보안조치 수행지침(2002. 9. 국가정보원.)
- 전자정부구현을 위한 행정업무등의 전자화촉진에 관한 법률
- 전자정부구현을 위한 행정업무등의 전자화축진에 관한 법률 시행령
- 사무관리규정
- 남북교류협력에 관한 법률
- 남북교류협력에 관한 법률 시행령
- 특수자료취급지침(1970.2.16.제정, 1998.9.1. 제4차 개정, 국가정보원)
- 정부비밀문서 발간 관리 지침(조달청 자재 43161-58463, 2003. 10. 2)
- 정보통신기반보호법
- 정보통신기반보호법 시행령
- 공공기관의기록물관리에 관한 법률
- 공공기관의기록물관리에 관한 법률 시행령
- 공공기관의기록물관리에 관한 법률 시행규칙

❸ 보안관리 체계



❹ 보안담당관, 분임보안담당관 지정 및 임무

가. 보안담당관의 지정(농식품부보안업무시행세칙 제25조, 농식품부정보보안지침 제7조)

① 보안담당관

○ 본　　부 : 운영지원과장

○ 소속기관 : 서무담당과장 또는 각 기관의 차하위자

○ 산하기관 : 기관장이 지정하는 실(처)장급 책임자(1차소속 이하는 기관장 지정자)

② 분임보안담당관

○ 본　　부 : 각 실·국의 주무과장(담당관), 정보통신 보안분야는 정보화담당관(정보통신분임보안담당관⇒정보보안담당관), 국가지리정보 보안분야는 농지과장, 어업통신분야는 지도안전과장

○ 소속기관 : 각 기관의 장이 지정

Point

• 보안담당관 및 분임보안담당관은 보안업무의 수행의 원활을 위해 당해 직위에 임용과 동시에 지정(별도의 지정절차 불필요)

나. 보안담당관의 임무

① 자체보안업무 수행에 관한 계획조정 및 감독
② 보안교육 및 서약의 집행
③ 비밀소유 현황 조사
④ 정보통신보안에 관한 사무
⑤ 보안진단 및 보안업무 심사분석에 관한 사항
⑥ 보안감사 및 보안점검
⑦ 분임보안담당관 및 소속기관 보안담당관의 지휘·감독
⑧ 기타 보안업무 전반에 관한 지도조정 및 감독에 관한 사항

Point

• 보안담당관 : 각각의 관리책임자별로 분담되어 있는 보안업무를 효과적으로 조정하고 지휘·감독하기 위한 최고관리자의 참모

다. 보안담당관 교체시의 조치(세칙 제27조)

• 보안담당관 교체 후 3일 이내 인계·인수 후 관계기관(국정원) 통보
• 근　　거 : 국가정보원 지시문서로 시달된 내용이므로 관계규정에서 찾을 수 없음
• 본　　부 : 국가정보원
• 소속기관 : 국가정보원 지부

Point

• 첨부 서류 : 인사기록카드 사본 1부, 신원진술서 1부, 사진(명함판) 1매

라. 분임보안담당관의 임무

보안담당관 임무에 준한다.

① 자체보안업무 수행에 관한 계획·조정 및 감독
② 실·과(팀) 자체 보안교육
③ 일일보안점검 및 월별 보안진단 실시
④ 자체 정보보안에 관한 사무
⑤ 비밀소유 현황 및 비밀취급인가자 현황 파악
⑥ 비밀 재분류 및 불필요 비밀의 정리

마. 정보보안담당관의 임무

- 정보통신보안 활동계획의 수립 및 정보통신보안업무 심사분석
- 정보통신망 신·증설시 보안대책 수립
- 정보통신실, 정보통신망 및 정보자료 등의 보안관리
- 정보통신보안업무 지도·감독 및 교육
- 정보통신보안 감사·지도점검 실시 및 사고조사·처리
- 정보보호시스템의 보안관리
- 정보통신보안관련 규정·지침 등 제·개정
- 기타 정보통신보안 관련 업무

5 보안심사위원회(세칙 제4조)

가. 설치 대상기관

- 본 부
- 고위공무원단(단, 동·서해어업지도사무소 제외)에 속하는 일반직 공무원이 기관장인 1차 소속기관 및 산하단체는 중앙 및 도 단위 단체와 이에 준하는 단체

나. 구성

- 위 원 장 : 본부는 제1차관, 소속기관은 기관장, 산하단체는 부책임자
- 부위원장 : 본부는 기획조정실장, 소속기관 및 산하단체는 상위자 순
- 위　　원 : 본부는 비밀취급이 많은 국장, 소속기관 및 산하단체는 상위자 순
- 간　　사 : 본부는 운영지원과장, 소속기관 및 산하단체는 보안관련 부서장

다. 보안심사위원회 심의·결정 사항

- 보안업내규의 제정 및 개폐에 관한 사항

- 보안업무계획 수립에 관한 사항
- 신원특이자 보안관리에 관한 사항
- 중요 보안위반자의 처리에 관한 사항
- 중요시설공사에 대한 보안대책
- 정보통신·지적정보보안담당관 임무중 중요 보안업무에 관한 사항
- 차하위 기관에서 심의 요청하는 사항
- 기타 보안업무 수행상 위원장이 필요하다고 인정하는 사항

6 보안사고(세칙 제64조)

가. 보안사고의 범위

비밀의 누설, 분실 및 비밀보관용기(보관시설)의 파기와 시설 내 불법침입자에 의한 시설 파기를 말함.

나. 보안사고 보고

- 보고주체 : 보안사고 발생 기관장, 사고를 범하였거나 이를 인지한 자
- 보고사항 : 사고의 일시, 장소, 사고내용, 현재 취하고 있는 조치사항
- 보고절차 : 본부 경유 국정원 보고

Point

- 보안사고는 전말조사가 종결될 때까지 공개할 수 없음

7 보안감사(세칙 제69조)

- 보안감사의 주관 : 보안담당관
- 보안감사의 종류
  - 정기감사 : 보안업무 전반에 관하여 연 1회
  - 수시감사 : 보안담당관이 필요하다고 인정한 때
- 감사반 편성
  - 반장 : 보안담당
  - 반원 : 일반보안 담당자, 통신보안담당자, 정보보안 담당자
- 결과조치
  - 감사결과에 중대한 위반사실이 지적되었을 때에는 관계공무원과 감독직에 있는 공무원에 대하여 응분의 조치 강구

♣ 보안감사와 보안점검의 차이점?

① 공 통 점 : 보안규정, 보안업무추진계획, 지적사항 등의 이행상태를 확인 및 감독하고 관리상의 취약점을 찾아 이를 개선하는 행위

② 보안감사 : 사전통보-공개-비교적 장시간에 걸쳐 취약점 발굴 및 보안대책의 적절성 여부 확인에 중점

③ 보안점검 : 불시-비공개-비교적 단시간에 걸쳐 보안대책의 평상시 이행상태 확인에 중점

8 보안감사시 착안사항

가. 보안감사 착안사항

① 일반보안 분야

- 보안관리체제구축실태, 보안환경 변화에 따른 대처능력
- 신원조사·비밀취급인가 등 인원보안 대책
- 비밀 및 중요정책 연구용역에 따른 보안대책, 중요정책 및 대북·국제협상 보안대책
- 외국인 채용·교류 및 접촉시 보안대책
- 기록물관리법시행에 따른 보안대책
- 대테러·보안장비 보호대책, 행정정보공개에 따른 보안대책
- 국가지리정보보안대책, 폐기문서 및 불용 PC·디스켓 처리관련 보안대책,

② 정보 보안분야

- 정보보안업무 수행 및 관리체계 적절성 여부, 정보화사업 추진시 안전성 확보를 위한 보안절차 준수여부
- 사이버 침해사고 대응체계 구축
- 암호장비 등 보안시스템 보안관리 실태, 정보통신실 보안대책
- 네트워크 보안대책, 정보보호시스템 보안관리 대책,
- 웹서버 등 공개서버 보안대책, 전자우편 보안대책
- PC등 정보통신기기 운용관리 보안대책

Ⅱ 보안실무

❶ 인원보안

1-1. 신원조사

가. 신원조사(규정 제31조, 세칙 제10조)

국가보안을 위하여 국가에 대한 충성심, 성실성 및 신뢰성을 조사하기 위하여 행하며, 임용 전 또는 인가 전에 실시하고 회보 결과는 임용, 승진, 인가, 허가 등에 영향을 미침.

Point

- 신원 특이자는 보안심사위원회의 심의 필요

나. 신원조사 대상자(규정 제31조제2항, 세칙 제10조)

- 공무원 임용 예정자
- 공무원이 아닌 자의 비밀취급인가 예정자
- 정부청사출입규정에 의한 상시출입증 발급대상자
- 국가 중요시설, 장비 및 자재 등의 관리자와 기타 각급 기관의 장이 국가보안상 필요하다고 인정하는 자

Point

- 임시직이나 단순고용직으로 임용되는 사람 중 국가중요시설·지역의 통제·출입 및 중요 문서·자재의 취급자로서 당해기관의 장이 보안상 필요로 하는 사람 외에는 신원조사 생략

다. 상시출입증 발급 대상자

- 본부에 파견되어 근무하는 소속 공무원
- 산하단체의 부장급 이상인자
- 유관업체의 임원급 이상인자
- 각 실·국의 연구개발 사업등에 참여하는 외부인중 6개월 이상 청사를 출입하기로 된 자
- 문서사송을 위한 상시출입자

라. 신원조사 대상자별 조사·요청기관

조 사 대 상 자	조사기관	요청자
• 3급(상당)이상 공무원 임용예정자(고위공무원단 포함) • 국가보안상 필요하다고 인정하여 요청하는 자 (국가중요시설, 장비 및 자재 관리자 등) • 외국인으로서 공무원 임용예정자 • 정부의 승인이나 동의를 요하는 법인의 임원 및 직원 • 해외주재공무원 및 국게기구 파견 공무원	국가정보원장	장 관
• 공무원 임용예정자(국가정보원장에게 요청하는 자 제외) • 공무원이 아닌 자의 비밀취급인가예정자 • 상시출입증발급대상자 • 국가보안상 신원조사가 필요하다고 인정하는 자	관할 경찰청장	임용권자 비밀취급인가권자 각급 기관장

마. 신원조사 요청시 구비서류(규칙 제55조, 세칙 제23조)

- 대상자 명단(국정원, 신원조사업무지침 별지 제1호 서식) 1부
- 신원진술서(국정원, 신원조사업무지침 별지 제2호 서식) 1부
- 최근 3개월이내 촬영한 상반신 반명함판 사진 1매

☞ 외국인에 대한 신원조사의 경우는?

- 자기소개서 (규칙 별지 제21호 서식) 1부
- 여권 사본, 자국 공안기관 발행 범죄기록증명원 각 1부
- 최근 3개월 이내 촬용한 상반신 반명함판 사진 1매

바. 신원특이자 관리

- 신원회보 결과 특이사항이 있는 자는 신규임용, 해외여행시 보안심사위원회의 심의를 요함
- 신원조사 결과 특이자라 할지라도, 신원조사 회보서는 개인별 인사기록카드에 합철 보관
- 신원특이자의 안보분야, 비밀수발부서 및 주요보직 임용시는 보안심사위원회의 의결을 거쳐야 함

사. 신원조사회보서 관리(세칙 제24조)

- 개인별로 인사기록서류와 함께 관리하되 타기관 전출자는 인사기록서류와 함께 이송
- 퇴직자는 퇴직자 인사기록서류와 함께 관리
- 신원특이자의 신원조사회보서는 사본을 당해 직원이 소속된 기관의 보안담당관에게 이송

1-2. 임시용원의 관리(세칙 제15조)

가. 임시용원이란

▶ 국가공무원법의 적용을 받지 아니하고 예산서에 일용임금으로 계상된 잡급 및 임시사역원(기관에서 임용하여 기관업무를 보조하는 직원 및 6개월 이상의 일용직을 포함)을 말함

- 특수분야 종사자(비밀업무취급자, 통제구역근무자, 경비근무자)와 기타 기관장이 필요하다고 인정하는 자의 신원조사는 규정 제31조의 규정 적용
  단, 단순업무 종사자에 대해서는 신원조사를 생략
- 임시용원에게 비밀취급 담당 및 통제구역 근무 등 보안상 책임있는 주요업무를 부여하여서는 안되며, 부득이한 사유로 공안상 특수분야(비밀업무취급자, 통제구역 근무자, 경비근무자)에 근무를 시키고자 할 경우에는 취업의 필요성, 보안감독 방안, 수행할 업무내용을 기록하고 보안담당관의 승인을 얻은 후 채용해야 함.(이 경우 신원조회로 우선 승인을 받아 채용하고 임용한 날부터 15일 이내에 신원조사를 요청하여 신원조사회보서 사본 첨부 결과 통보)
- 임시용원의 채용과 동시에 보안각서를 징구하고, 보안교육을 실시하여야 함.
- 임시용원의 보안사고에 대한 감독책임은 그 소속과장이 짐(세칙 제16조)

1-3. 비밀취급인가

가. 비밀취급인가권자, 범위, 한계(세칙 제17조 내지 제18조)

① 비밀취급

- 비밀의 취급이란 비밀을 생산, 접수, 분류, 보관, 열람 및 파기하는 일체의 행위를 말함
- 비밀을 취급할 수 있는 자는 당해등급의 비밀취급 인가를 받은 자와 비밀취급 인가권이 있는 직위에 임명된 자가 됨

Point

- 대외비는 비밀취급인가 여부와 관계없이 당해 업무에 관련된 내부 직원은 열람 가능

② 소속 직원에 대한 비밀취급 인가권

- Ⅰ급이하 비밀취급 인가권 : 장관

- Ⅱ급이하 비밀취급 인가권 : 장관, 1차 소속기관장, 농협협동조합중앙회장, 한국농촌공사사장, 농수산물유통공사사장, 한국마사회장, 수산업협동조합중앙회장, 한국원양산업협회장

③ 비밀취급인가 범위

- 1급 비밀 취급 : 본부 국장급 이상 공무원, 본부 보안담당관
- Ⅱ·Ⅲ급 비밀 취급
  - 본부 및 소속 공무원중 부서별 비밀보관 정·부 책임 공무원
  - 본부 및 각 과의 서무(보안업무) 담당공무원과 직책상 비밀을 항상 사무적으로 취급하는 공무원
  - 장·차관 비서관, 수행비서 및 장·차관 수행기사
  - 문서수발 담당공무원
  - 산하기관의 경우 직접 비밀업무와 관련 있는 소속 임직원 (비밀 수발계통, 비밀 보관담당, 비밀 열람권자)
- 기타 인가권자가 필요하다고 인정한 자

④ 비밀취급 한계

- 비밀취급인가자 : 관계업무 범위 내
- 비인가자 : 비밀입수 시 지체 없이 해당 비밀취급인가자에게 인도
- 비인가자의 범위
  - 비밀취급 미 인가자
  - 인가받은 등급보다 상위등급의 비밀을 취급한 자
  - 동급 비밀이라 할지라도 업무상 무관한 비밀을 취급한 자

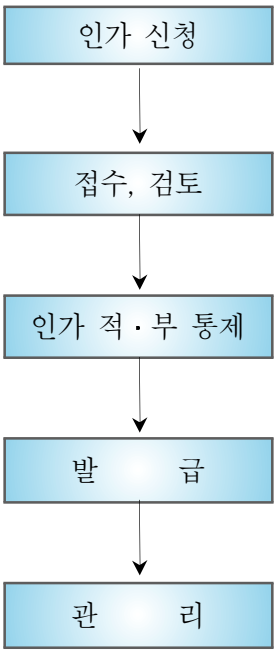
나. 비밀취급인가 요령 및 절차(세칙 제19조)

① 비밀취급 인가 요령

- 비밀을 취급 또는 비밀에 접근하는 직원은 해당등급의 비밀취급인가 대상자의 직책에 따라 필요 최소한의 인원으로 제한
- 신원조사는 임용당시의 신원조사회보서에 의거 인가 가능

※ 국가비상훈련(을지연습)을 실시하기 위하여 동원되는 자가 비밀사항 취급시는 비밀취급인가를 대신하여 서약서로 갈음할 수 있음(세칙 제24조 제5항)

② 비밀취급 인가 절차



보안업무담당과에 문서로 신청

신청서류 — 비밀취급인가조서
신원조사회보서 사본

보안업무담당과

보안업무담당과(보안담당관)

보안교육 실시
비밀취급인가증 발급, 수령증 교부

비밀취급인가자명부 작성
전보, 전출, 업무변경 등에 따른 해제, 갱신 조치

다. 비밀취급인가 해제(세칙 제20조)

① 당연해제 ⇒ 별도의 서면발령 없이 인가증 회수, 반납
- 인가권을 달리하는 타기관으로 전출, 전보 시
- 면직, 휴직, 직위해제 시

② 발령해제 ⇒ 서면으로 발령 해제
- 업무변동으로 비밀취급 불필요시
- 고의 또는 중대한 과실로 보안사고를 범하였을 때
- 보안관계 규정 위반으로 보안업무에 지장을 초래한 때

② 문서보안

2-1. 비밀의 취급 및 구분

가. 비밀의 취급

비밀을 생산(수집, 작성, 분류), 관리(수발, 재분류, 보관, 열람), 파기하는 일체의 행위

나. 비밀의 구분(규정 제2조, 제4조)

Ⅰ급비밀	누설되는 경우 대한민국과 외교관계가 단절되고 전쟁을 유발하며, 국가의 방위계획·정보활동 및 국가방위상 필요 불가결한 과학과 기술의 개발을 위태롭게 하는 등의 우려가 있는 비밀
Ⅱ급비밀	누설되는 경우 국가안전보장에 막대한 지장을 초래할 우려가 있는 비밀
Ⅲ급비밀	누설되는 경우 국가안전보장에 손해를 끼칠 우려가 있는 비밀

다. 대외비(규칙 제7조)

누설되는 경우 "행정상 지장"을 초래할 우려가 있거나 직무 수행상 특별히 보호를 요하는 사항.

Point

• 모든 대외비는 비밀에 준하여 처리 및 관리

2-2. 비밀의 분류

가. 비밀분류의 원칙 및 금지사항(규정 제10조, 규칙 제7조)

① 분류원칙

- 과도 또는 과소분류 금지의 원칙 : 비밀을 적절히 보호할 수 있는 최저등급으로 분류
- 독립분류의 원칙 : 비밀은 세부분류지침(세칙 제35조)에 의거 독자적 내용과 가치의 정도에 따라 분류

② 비밀분류상 금지사항

- 행정상 과오나 업무상 과실을 은닉할 목적으로 비밀이 아닌 사항을 비밀로 분류 금지
- 비밀의 제목에 비밀내용이 표시되어서는 안됨

나. 비밀의 기본분류지침(규칙 제8조)

비밀등급	분 류 사 항
Ⅱ급비밀	• 국가방위에 중요한 손해를 초래할 우려가 있는 사항 • 국가방위계획 및 그의 효과를 중대하게 위태롭게 하는 사항 • 국가의 중요한 정보활동계획 및 특수치안활동에 부분적인 사항 • 국방에 중대한 과학 및 기술발전에 관한 사항 • 국가정책의 전환이 외국 또는 국민전체에 직접적인 영향이 있는 부분적인 사항
Ⅲ급비밀	• 국가 외교상황중 공개됨으로써 적 또는 가상적국에 유리 하게 악용될 우려가 있는 사항 • 각군의 중요한 활동장비 및 그의 연구 발전 등에 관한 사항 • 국가안전보장상 필요로 하는 특수정보활동계획의 일부분으로 실시되는 국부적인 사항 • 계획단계에서 공개 또는 누설됨으로써 실적 또는 시책면에서 차질을 가져올 우려가 있는 계획 및 방침

다. 비밀의 분류권자와 제한사항(규정 제9조)

① 분류권자

- 분류권자란? 비밀이 몇 등급에 해당하는 가를 결정하는 권한을 인가받은 자
- 비밀의 등급을 결정하는 권한을 인가받은 자
- 비밀취급인가를 받은자는 비밀분류권한이 있음
- 비밀의 최초 분류권자(기안 책임자), 비밀의 최종 분류권자(결재권자)

② 제한사항

- 인가받은 등급의 비밀과 그 등급이하의 비밀만 분류할 수 있음
- 상위직은 하위직이 분류한 비밀등급을 조정할 수 있음

라. 비밀의 재분류 검토(규정 제13조)

① 비밀의 재분류

- 정의 : 비밀의 효력이나 처리방법을 변경하는 것
- 목적 : 비밀의 효율적인 보호
- 방법 : 비밀등급 · 보호기간(예고문)의 변경 또는 파기 등

※ 비밀을 취급하는 자는 계속적으로 소관비밀의 예고문에 의한 재분류 검토를 실시하여야 함.

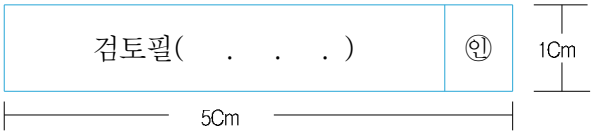
마. 비밀의 재분류 검토 시기(규칙 제10조)

① 월 별 재분류 : 보관비밀의 재분류시기 도래 여부(예고문) 확인
월별 비밀 증가 및 감소현황 파악
장기보유 비밀에 대한 재분류 검토

② 반기별(6월말, 12월말 기준) 재분류 : 생산비밀(원본) 재분류 검토

Point

• 이 경우 원본 표지 여백에 필히 검토필 표시



바. 재분류 방법(규정 제13조, 규칙 제10조 내지 제13조)

① 비밀 발행자

– 비밀 발행자가 수시로 직권 재분류 할 수 있는 비밀의 종류

• 생산비밀 중 과다 또는 과소 분류된 비밀의 재분류시
• 생산비밀중 예고문 도래전 비밀의 재분류시

Point

• 비밀을 재분류하였을 경우에는 그 비밀이 배포된 모든 기관에 이를 통보

• 타기관으로부터 인수한 비밀원본

② 비밀 접수기관

– 비밀 접수기관이 직권 재분류 할 수 있는 비밀의 종류

• 타기관으로부터 접수한 비밀사본 중 발행기관이 불분명한 Ⅱ급 이하 비밀
• 동일계통의 상급기관(조정감독기관)이 하급기관(피조정 감독기관)으로부터 접수한 비밀사본 ⇒ 이 경우 발행기관에 통고

– 비밀(사본)을 접수한 기관이 그 비밀을 검토한 결과 다음의 경우에 해당할 때에는 그 사유를 명시하여 발행기관에 재분류 요청

• 과도 또는 과소 분류되었다고 인정될 때
• 비밀로 분류되어야 할 사항이 분류되지 아니한 때

③ 예고문에 의한 방법

– 타기관으로부터 접수된 비밀은 예고문에 의거 재분류함.

Point • 다만, 다음의 경우에는 예고문에도 불구하고 파기 가능

- 긴급·부득이한 사정으로 비밀을 계속 보관하거나 안전하게 지출할 수 없을 때
- 국가정보원장의 통고가 있을 때
- 보안유지를 위하여 예고문의 파기시까지 계속 보관할 필요가 없을 때 (다만, 이 경우에는 소속 비밀취급인가권자의 사전 승인을 얻어야 함)

④ 비밀 존안시 재분류

- 비밀을 존안하고자 할 때에는 그 예고문 또는 비밀등급 변경 불가
- 존안된 비밀은 존안기간 중 재분류하지 않으며, 다만 일반문서를 재분류하는 때에는 그러하지 아니함.

♣ 존안이란?

① 사전적 의미 : 없애지 않고 보존하여 두는 행위 또는 문건

② 보안실무상 의미 : 비밀문서 원본의 보호기간이 만료되어 파기하여 할 경우에도 보안업무 규정 제13조제4항의 규정에 따라 예고문이나 비밀등급을 변경하지 않고 계속 보존하는 것

2-3. 비밀의 표지(標識)

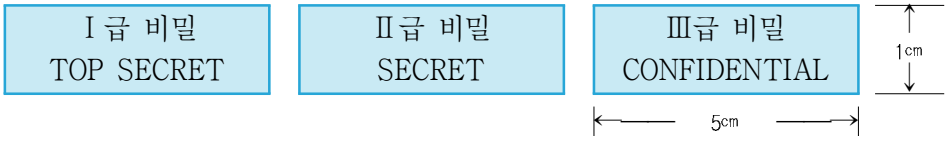
가. 비밀의 표지(규정 제14조, 규칙 제16조 내지 제 23조)

① 비밀 표지(標識)란?

비밀 취급자 또는 관리자에게 취급상의 경각심을 제고하고 비인가자의 접촉을 방지하기 위하여 비밀의 분류(재분류 포함)와 동시에 구분하는 표시나 징표

– 비밀종류별 등급표지 방법

- 표지형태



– 문서의 표지

- 전후면의 표지와 매면 상·하단 중앙
- 적색 원칙(복사 또는 복제시는 복사물과 동일한 색 가능)

• 매면의 비밀등급이 다른 경우는 각 면별로 해당등급을 표지하되, 그 표지의 양면은 그중 최고의 비밀등급 표지
• 비밀문서는 철하여져 있거나 보관되어 있을 때를 제외하고 보안업무규정시행규칙 별지 제6호 서식의 비밀표지를 해당 등급에 따라 첨부하고 취급하여야 한다.

Point
• 파일표지에 여러건의 비밀을 보관할 경우에는 파일표지에 부착하여 관리한다.

– 지도, 괘도, 기타 도안 등의 표지
  • 매면 상·하단 중앙에 적당한(눈에 잘 띄는) 크기로 표지
  • 접거나 말았을 경우 그 이면의 적당한 곳에 표지
– 상황판 등의 표지
  • "지도, 괘도, 기타 도안" 등의 표지와 같이하되 비밀표지를 한 가림막 설치 다만, 보호상 불이익하거나 충분히 위장된 경우에는 가림막에 표시를 하지 아니함
– 비밀의 녹음
  • 녹음 첫부분과 마지막 부분에 누설시 처벌한다는 경고문 삽입

나. 대외비 표지(標識)

• 대외비의 표지는 표면의 상단중앙에 적색으로 표지하고 보호기간을 반드시 삽입

대 외 비		
원본	보호기간, 로 재분류(일자또는조건)	보존기간 :
사본	파기, ~로 재분류(일자또는조건)	

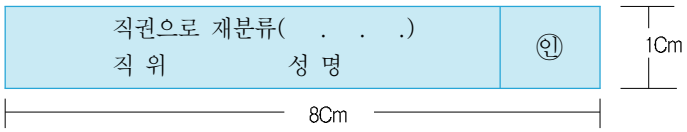
Point
• 대외비 표지는 매면마다 해야 할 의무는 없으나 시행공문(직인날인 페이지)과 분리될 경우 대외비 여부를 확인하기 곤란한 첨부물은 대외비 표지 권장

다. 재분류 표지(규칙 제22조)

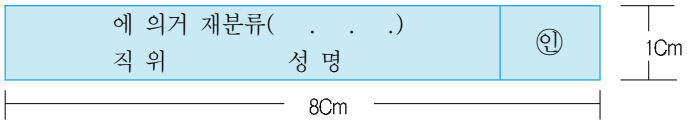
• 구표지(비밀등급표지: Ⅰ·Ⅱ·Ⅲ·대외비)는 대각선으로 삭제하고 그 측면 또는 상단의 적당한 여백에 변경된 비밀등급을 재차 표지
• 책자, 팜플렛 등은 양면표지의 비밀표지만을 삭제표시 후 재차 표지
• 매 면마다 재분류 한 때에는 각 면별로 삭제표시 후 변경등급 재차 표지

• 비밀을 재분류한 때에는 재분류 근거를 다음 서식에 의하여 그 비밀의 첫면 적당한 여백에 기입하고 날인

(발 행 처)

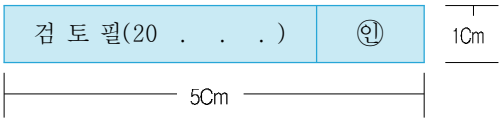


(접 수 처)



라. 재분류 검토필 표시(규칙 제22조)

• 검토 대상 : 자체에서 생산한 비밀의 원본
• 검토 시기 : 연 2회(6월, 12월) 재분류 검토 실시 후
• 표시 위치 : 문서 표지(表紙)의 적당한 여백
• 표시 방법



마. 비밀의 면 표시(규칙 제23조)

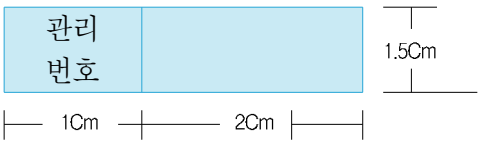
– 면표시 대상 : 2장 이상으로 이루어진 비밀문서.
– 표시위치 : 문서의 중앙하부
– 표시방법
  • 전(全)면수와 그면의 일련번호를 기입(예, 전체가 3면인 경우 3-1, 3-2, 3-3)
  • 붙임물 또는 첨부물은 한건문서의 전체 면수에 포함
  • 첨부된 관련 문서의 면표시는 위 방법에 따르되 본문과 구분하여 따로 부여한다.
  • 양면문서인 경우에는 각 면마다 번호 부여

바. 비밀관리번호(규칙 제31조)

① 비밀의 관리번호는 비밀관리를 위한 가장 기초적인 수단

② 표시 위치
  • 문서의 경우 : 표지(表紙)의 좌측 상단

- 기타 도서, 자재 등의 경우 : 문서에 준하여 식별이 용이한 적정한 부위
- 표지(標識) 규격



③ 부여 방법

- 모든 비밀은 작성 및 접수되는 순서에 따라 누년일련번호 부여
- 자체 내에서 작성되는 비밀의 관리번호는 최종결재자가 재결(裁決)하여 그 내용이 확정된 후에 부여
- 비밀의 보관부서별로 비밀등급에 따라 누년 일련번호 부여
- 동일한 문서·책자라 할지라도 2부이상일 경우 반드시 개개(별개)의 관리번호 부여
- 자체 생산(작성) 비밀은 원본에만 부여하고 발송되는 비밀(사본)에는 미부여
- 접수된 비밀에 의하여 생산된 비밀에 대하여도 접수된 비밀과 별도로 부여
- 암호자재는 관리번호를 부여하지 아니함.(보안시스템관리기록부에 기록)

사. 사본번호(규칙 제33조)

♣ 사본이란? 비밀의 생산 원본을 복제·복사 ·발간 등에 의해 원형을 재현한 것을 말한다.

– 비밀의 사본을 생산하였을 경우 원본과 모든 사본 부수에 개개의 번호를 부여함.

※ 비밀발간에 있어서 보관용 비밀은 필요최소한에 한 함. 단 부득이한 경우 보안담당관의 승인을 거친 경우는 그러하지 아니함

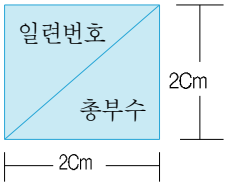
– 사본 부여 방법

- 비밀을 복제·복사한 때에는 원본과 동일한 비밀등급과 예고문을 명시
- 전(全)사본에 대한 개개의 일련번호를 기입
- 비밀 원본의 예고문이 "파기"로 되어 있을 때에는 사본의 파기시기를 원본의 파기시기보다 줄일 수 있음.

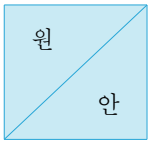
– 표시 위치 : 비밀 표지(表紙)의 우측 상단

– 표지(標識) 규격 및 방법

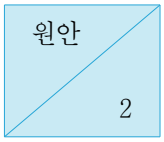
※ 일반례

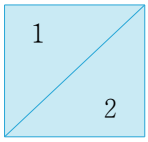


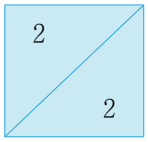
※ 내부결재의 경우



※ 받는곳이 2곳일 경우의 예

(기안문) 

(시행문) 



♣ 실제 생산된 건수는 사본 + 1(원본)인 3개임

Point

- 세칙 제29조제3항의 "이때 총 사본 수량은 원본을 포함한 사본의 총수량을 말한다." 라는 규정의 의미는?
  생산된 전체 비밀의 개수를 기산할 때의 기산점을 1이 아니라 0으로 본다는 말이다. 따라서 기산점인 0은 원본이 된다. 그러므로 배부선이 10곳인 경우 총사본수량은 10이 되지만 전체 비밀의 개수는 원본을 포함한 11개가 된다는 뜻이다

아. 예고문 기재(비밀기록물원본의 보존관리지침)

① 비밀기록물 생산시 그 원본에 반드시 보호기간과 함께 보존기간 병기

② 예고문은 효력만료 기간을 연월일시로 기재함으로써 명확히 표기하여야 함

Point

- 「처리후, 불필요시, 참고후」 등과 같이 불확실한 표현은 재분류 과정의 혼란 또는 방과를 초래함으로 표기 지양

③ 재분류시기를 예측할 수 없는 비밀은 발행일로부터 통상 1년 이내의 일자 기재

④ 표시 방법

원본	보호기간, 로 재분류(일자 또는 조건)	보존 :
사본	파기, ~로 재분류(일자 또는 조건)	

- 비밀기록물의 원본에는 그 원본의 복제 또는 복사 등 사본을 제작할 경우 "사본"의 예고문까지 함께 표기하며, 대외비의 예고문은 비밀에 준하여 표시함
- 유첨문서의 경우(첨부물이 비밀이고 시행문은 단순히 첨부물을 통보하기 위한 경우)

(본 문) 첨부물에서 분리되면 ( )로 재분류 (1Cm)

6Cm

(첨부물) . . .( )로 재분류 파기(일자 또는 경우) (1Cm)

- 비밀 자체에 기입할 수 없는 경우에는 비밀관리기록부에 기록하고 이를 발송할 때에는 송증 또는 비밀통보서 말미에 기입

2-4. 비밀의 수발

가. 수발의 기본원칙(규정 제15조, 규칙 제24조, 세칙 제31조)

① 수발 방법

- 비밀취급인가자의 직접 접촉에 의한 수발(원칙)
- 암호화 한후 전신 수발
- 문서수발계통에 의한 수발
- 등기우편에 의한 수발

② 수발 원칙

- 수발 비밀은 최대한으로 보호할 수 있는 방법을 이용하여야 함.
- 비밀은 전신·전화 등의 통신수단에 의하여 평문으로 수발하여서는 아니됨.

③ 수발 방법상 유의사항

- 비밀 수발은 계통(수발부서)을 경유하여 취급자의 직접접촉으로 수발함을 원칙으로 함.
- 다만, 취급자의 직접접촉이 불가능할 경우 I 급비밀 및 암호자재는「암호화하여 전신」, 「취급자와 직접접촉」으로, Ⅱ·Ⅲ급비밀은 등기우편으로 수발 가능

④ 비밀 파급상 유의사항

- 타기관으로부터의 접수비밀은 발행기관의 승인 없이 재차 다른 기관으로 발송 불가. 다만, 이첩시달하는 경우는 예외로 함.
- 타기관으로부터 접수한 비밀은 「(비밀)수발대장」(규칙 별지 제10호서식)에 기록하고, 근무시간 이내에 소관부서(취급자)에 인계한 후 수발대장의 "수령자"란에 수령인을 받아야 함.
- 기관내의 수발은 수신기관이 3개 미만일 때에는 수발대장에 의하지 않고 비밀관리기록부에 의하여 수발

⑤ 비밀 수발시 유의사항

– 접수시

- 수신관서의 정확성 여부 확인
- 예고문의 기재여부 확인
- 비밀열람기록전 첨부여부 확인(대외비 제외)
- 영수증 반송(규칙 별지 제8호 서식)

– 발송시
  • 비밀의 표지(標識), 예고문 및 사본번호 기재여부 확인
  • 비밀열람기록전, 영수증 및 배부표 첨부여부 확인
  • 등기우송시 규칙 별지 제7호서식에 의한 이중봉투 사용

Point
• 대외비의 수발은 Ⅲ급비밀에 준하되, 비밀열람기록전 및 영수증은 불필요함.

나. 비밀 수발 주관 부서

• 본부 및 소속기관 : 운영지원과 또는 보안총괄부서
• 산하기관 : 문서수발 주관 과장 또는 비상계획부장, 안전관리실장 기타 등등
• 수발담당자 : 소속 직원중 Ⅱ급 비밀 취급이 인가된 직원 지정

♣ 비밀수발대장의 『원본인수자인』란과 『수령자인』란 기재방법

비밀발송을 위해 비밀발송번호를 등재할 경우(접수의 경우도 같은 요령임)

• 보안담당부서 비밀수발담당자는 비밀 『원본』 및 『사본』의 발송번호 부여후 비밀 원본은 담당자에게 돌려주고, 사본을 전량 인수받은 다음 비밀수발대장(규칙 별지 제10호서식)의 『원본인수자인』 란에 서명

비밀 배부선인 해당 부서의 비밀수발담당자는 운영지원과 비밀수발담당자가 보관하고 있는 비밀 사본을 수령한 후 운영지원과 비밀수발대장의 『수령자』란에 서명

Point
• 비밀의 유통경로를 명확히 함으로써 분실 등 보안사고 발생시 책임소재를 분명히 하기 위함

다. 비밀의 통제

① 비밀 발송통제
– 통제 대상 : 생산비밀로 외부 시행문서
– 통제 시기 : 문서 시행을 위해 총무과 발송대장 등록시
– 통 제 관 : 보안담당관(보안담당자 또는 비밀 수발취급자)
– 통제사항
  • 비밀세부분류지침에 의한 분류여부 검토
  • 과소 또는 과도 분류여부 확인 및 불필요한 비밀생산 억제
  • 분류표지 · 사본번호 · 비밀열람기록전 · 영수증 유무
  • 예고문과 배포선의 타당성 검토 등

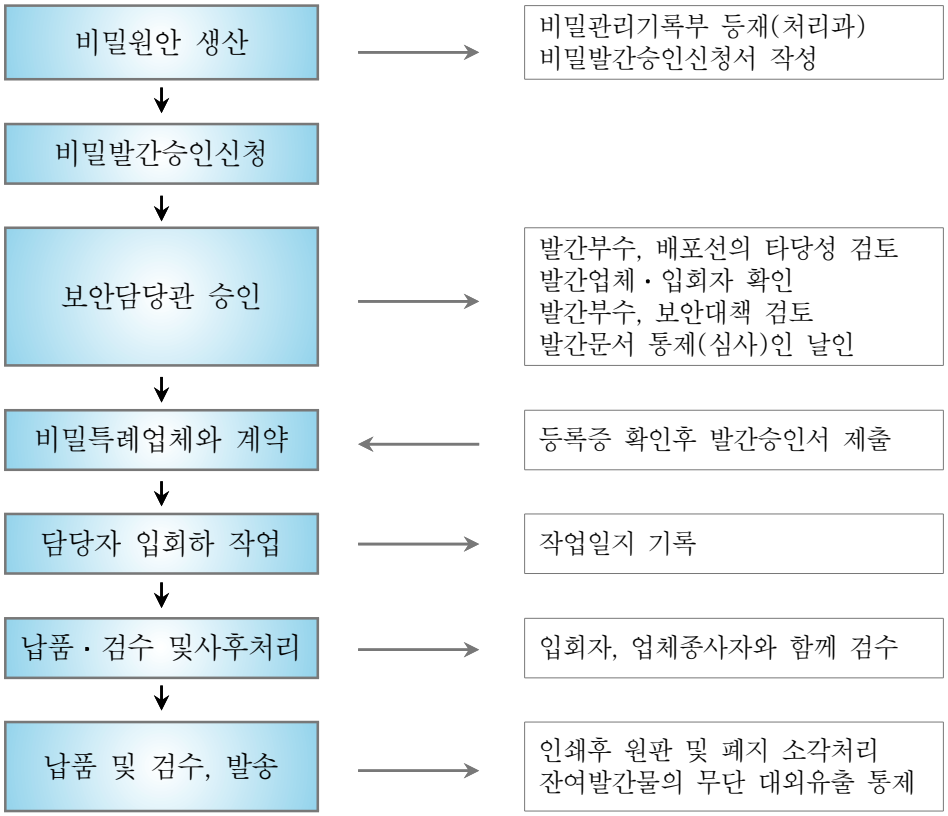
② 비밀 외주발간 통제 ⇒ 비밀(대외비)문서는 자체발간이 원칙

– 외주발간시는 국가정보원장의 보안조치를 받은 업체중에서 조달청장 또는 지방자치단체장이 비밀발간업체로 인가한 업체를 이용

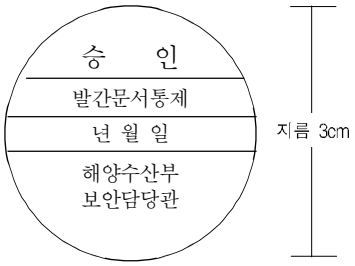
Point

• 조달청 등 미인가 민간시설 이용 비밀발간시는 20일 전까지 관할 국가정보원 대공분실에 통보후 발간시설에 대한 보안측정을 받아야 함

– 발간절차



– 발간문서통제(심사)인 표시



– 민간시설을 이용하여 비밀 또는 대외비를 외주발간 하였을 경우에는 그 문서나 책자의 말미 또는 후면표지 이면에 다음과 같이 기재한다(규칙 제37조 제3항)

서기 년 월 일 발간		
발간업체명	전화( )	
대표자명		
인가근거		
참여자	소속	
	성명	

6cm

10cm

③ 비밀 복제·복사 통제

– 비밀(대외비)의 복제 및 복사는 원칙적으로 불가

• 복제·복사란 기 생산된 비밀을 특별한 필요에 의해 원본에 대한 훼손 또는 수정없이 원안의 내용 그대로를 사본 생산하는 것을 말한다.

Point

• 비밀의 생산시 배부선에 해당되는 사본 생산을 위한 프린트, 복사 등

– 비밀(대외비)의 복제 및 복사시 지켜야 할 사항

• 타인의 접근 방지 조치 후 자체시설(장비) 활용
• 원본과 동일한 등급의 비밀 표시와 예고문 명시, 별도 사본번호 부여
• 원본에 사본번호를 포함한 배포선 첨부
• 등록된 보조기억장치(디스켓, usb 등)에서 작업 및 출력
• 비밀입출력관리대장 기록 관리

– 비밀의 복제 및 복사가 가능한 경우

• Ⅰ급 비밀의 경우 발행자의 허가를 받은때
• 규칙 제32조에 의한 복제 복사 제한표시가 없을 때

– 사본근거 표지 방법

• 접수한 비밀을 이첩기안 등 복제 또는 복사할 경우 해당 비밀의 첫면 또는 말미의 적당한 여백에 사본근거를 다음과 같이 기입한다.

사 본 일 자	년 월 일	성명	인
사 본 부 수	면부터 면까지 매		부
사본의 처리			

④ 복제·복사의 제한근거 표시(규칙 제32조)

- 표시대상 : Ⅱ급 및 Ⅲ급 비밀로 복제·복사를 제한할 필요가 있는 비밀

Point

- 암호 및 음어자재는 복제, 복사할 수 없음
- Ⅰ급비밀은 그 발행자의 허가를 받아야 함

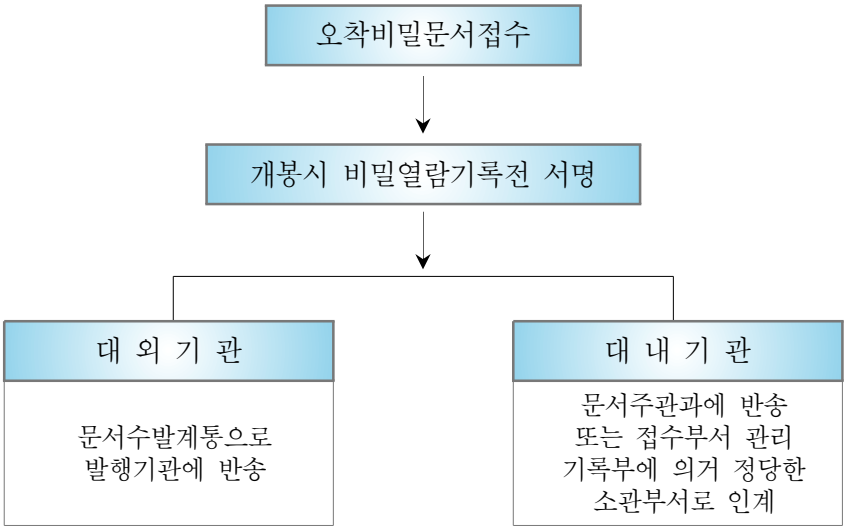
- 제한근거의 형식 및 내용

이 비밀의	는 발행자의 허가없이 복제 복사할 수 없음

- 색상 : 적색
- 표시위치 : 비밀의 표지 이면 또는 예고문 상단

※ 필요시 비밀취급에 관한 유의사항을 추가하여 표시

라. 오착비밀문서의 반송(세칙 제31조)



- 오착비밀(잘못 전달된 비밀)은 문서수발계통을 통하여 발행기관에 반송하여야 하며 자체 판단으로 타기관에 발송하여서는 안됨.
- 접수기관의 접수자는 비밀의 제목, 사본번호, 수량 등을 대조한 후 비밀영수증 영수인 서명 후 반송

마. 비밀접수 처리

- 접수 즉시 관리기록부 등재, 열람기록전 기재(서명 포함) 및 결재(공람)
- 대외문서의 경우 총무과 외의 부서에서 수령시는 반드시 총무과에 접수·등재

2-5. 비밀영수증 관리

가. 영수증 관리대상

- Ⅰ급 및 Ⅱ급 비밀 수발시 영수증 사용

나. 기재요령

- 송증과 영수증의 일련번호 일치
- 영수증의 수신란에는 비밀을 발송한 기관의 장을 기입
- 비밀발송자는 영수증을 기재함에 있어 "이상시의 사유" 난과 "접수자" 난 및 "접수일자" 난을 제외한 기타란 전부를 기재

다. 영수증 발급·송부 및 관리요령(규정 제17조, 규칙 제25조, 세칙 제31조)

- 영수증 부분만 절취
- 직접 접촉에 의하여 발송하는 경우는 직접 교부
- 등기우송할 경우에는 이중봉투의 내부봉투와 외부봉투의 사이에 삽입·발송
- 등기우편으로 발송시는 "비밀(대외비)문서 발송(등록)대장"
  (규칙 제10호의 "비밀수발기록부" 서식)의 수령자란에 등기물 영수증 번호를 기입하고, 등기물 영수증은 문서실에서 보관
- 비밀을 접수한 기관의 접수자는 즉시 영수증을 발행기관에 반송
- 반송받은 영수증은 비밀송증에 원래대로 첨부하여 비밀영수증철에 보관
- 비밀문서를 접수한 접수자는 비밀의 제목, 사본번호, 수량 등을 기재내용과 대조한 후 이상이 있을 때에는 그 사유를 기재하여 반송하고 그 비밀은 처리담당자에게 통보

2-6. 비밀의 보관

가. 비밀 보관원칙(규정 제18조 내지 제19조)

- 비밀은 도난·화재 또는 파괴로부터 보호하고 비밀취급비인가자의 접근을 방지할 수 있는 적절한 시설에 보관해야 함.
- 비밀을 휴대하고 출장 또는 여행하는 자는 비밀의 안전한 보호를 위하여 국내경찰기관 또는 국외주재공관에 위탁 보관할 수 있으며, 수탁기관은 이를 보관하여야 함.

나. 비밀 보관기준(규칙 제26조, 세칙 제41조)

- 원칙 ⇒ 보관책임자 (분임보안담당관) 단위로 보관
  (대외비는 업무 편의상 각 과별 보관 부책임자가 관리 할 수 있음)
  ※ 보관과를 변경할 때에는 당해기관 보안담당관 승인을 요함

- 비밀은 일반문서 또는 자재와 혼합 보관할 수 없음.
- Ⅰ급 비밀은 보안담당관이 집중관리(세칙 제12조제2항)
- 비밀보관책임자가 Ⅱ급 비밀취급인가자일 경우에 한하여 Ⅱ·Ⅲ급 비밀을 동일 용기에 보관 가능
- 보관용기에 넣을 수 없는 비밀은 제한구역이나 통제구역에 보관하거나 내용이 노출되지 않도록 특별한 보호책 강구

다. 비밀 보관용기(규칙 제27조, 세칙 제41조)

- Ⅰ급 비밀 : 반드시 금고에 보관
- Ⅱ·Ⅲ급 비밀 : 철제 이중 캐비넷에 보관관리(이중 시건장치)
- 비밀 보관용기의 외부에는 비밀보관을 나타내는 표시를 못함.
- 캐비넷의 외부에는 일반서류 보관 캐비넷과 같이 다음과 같은 보관책임자 표시를 함.

라. 열쇠관리

- 비밀보관함의 열쇠와 다이얼 번호는 반드시 2개(부) 작성하여 1개(부)는 보관책임자가 보관하고, 나머지 1개(부)는 당해기관의 「안전지출 및 파기계획」이 정한 바에 따라 당직함에 보관

2-7. 비밀 인계·인수(규칙 제29조, 세칙 제14조)

가. 비밀보관책임자 교체시 보안담당관 확인하에 비밀 인계·인수

- 비밀(대외비)관리기록부에 의거 인계·인수 함
- 후임 비밀보관책임자 공석시는 부 책임자에게 인계하고 비밀보관책임자 임명시 재 인계

나. 비밀인계인수사항 기재방법

– 인계·인수는 비밀(대외비)관리기록부의 최종 기입란 밑에 공란없이 다음과 같이 기재함.

> 비 밀 인 계 인 수
>
> 1. 인계인수 일시 :
> 2. 비밀건수 : ○ 급 ○ 건
> 3. 인계인수 사유 :
> 4. 인계자 전임 분임보안담당관 직 성명 (인)
> 인수자 신임 분임보안담당관 직 성명 (인)
> 5. 확인자 보암담당관 직 성명 (인)

– 확인자인 보안담당관이 지역을 달리하는 별도 청사에 위치한 경우 보관책임자의 상급자가 있을 때는 상급자가, 상급자가 없을 때는 차 하위자가 입회, 확인

– 조직 통·폐합, 업무이관 등 직제변경으로 인한 보관책임자 교체시의 인계인수는 이외에도 세칙 제27조의 인계인수서 작성 후 본부 보안담당관에게 보고

2-8. 비밀관리기록부 관리(규정 제21조, 규칙 제30조, 세칙 제 조)

– 비밀의 작성, 분류, 수발, 취급 등 일체의 관리사항을 기록관리하기 위하여 비밀보관단위별로 「비밀관리기록부」(규칙 별지 제9호 서식) 작성·비치

Point

• 암호자재의 관리는 지침 별지 제9호서식「국가용 보안시스템 관리기록부」에 의거 관리

– 비밀관리기록부 및 보안시스템 관리기록부에는 모든 비밀과 암호자재에 대한 보안책임 및 보안관리사항이 정확히 기록·보존되어야 함.

– 비밀의 파기 또는 타기관으로 이송·이관하였을 경우 비밀관리기록부의 해당란을 2개의 주선으로 삭제한 후 그 사유를 재분류란에 명시
(비밀관리기록부의 서식 중 “비밀등급” 부터 “사본번호” 난까지만 주선 처리)

가. 비밀관리기록부 작성방법

부처명 :　　보관책임자 :

① 관리번호	② 수 발			③ 문서번호	④ 비밀등급	⑤ 형태	⑥건명	⑦ 사본번호	⑧ 예고문	⑨ 처리담당	⑩ 보관장소	⑪재 분 류				⑫ 참조	
	년월일	발행처	수신처									등급변경	파기	파기확인	근거	영수증	수령자

① 관리번호 : 작성 또는 접수순서에 따라 누년일련번호 부여
② 수　　발 : 년 월 일, 발행처, 수신처 기재
③ 문서번호 : 공문서 번호 기재
④ 비밀등급 : 해당 비밀 등급 기재(Ⅰ급, Ⅱ급, Ⅲ급, 대외비로 구분 기재)
⑤ 형　　태 : 문서, 책자, 상황판, 도면, 필름, 슬라이드, 디스켓, USB 등 비밀의 형태 기재
⑥ 건　　명 : 비밀의 제목 기재
⑦ 사본번호 : 기재된 원본 또는 사본번호 부여(원본 예시 : 원본, 원본/1, 원본/12)
⑧ 예 고 문 : 부여된 예고문 기재 (파기, 일반 재분류 등 예고문 내용 명시)
⑨ 처리담당 : 당해 비밀업무 처리 담당자 성명 기재
⑩ 보관장소 : 비밀 보관 사무실명 기재
⑪ 재 분 류 : 비밀 재분류 또는 이송시 사유 기재
- 등급변경 : Ⅰ급⇒Ⅱ급, Ⅱ급⇒대외비 등 , ○ 파기 : 파기한 경우 파기일자 및 파기지 서명 ○ 파기확인 : 확인자 서명
- 근 거 : 예고문, 파기지시 · 통보 공문서 번호 등 파기 또는 재분류 근거 기재

⑫ 참　　조 : 비밀 수발사항 확인
- 영수증 : 규칙 별지 제8호 서식에 의한 비밀송증 번호 기재
- 수령자 : 직접 접촉에 의해 수발한 경우 수령자 서명

Point
- 비밀 수발대장의 수령자와 관리기록부의 수령자는 다를수 있음
- 비밀 원본의 파기 표시의 경우 관리기록부 해당 빈 공란에 『기록보존소 이관』 기재

2-9. 비밀관리기록부의 갱신방법(세칙 제 조)

– 비밀관리기록부를 갱신하고자 할 경우에는 구대장 말미에 다음과 같이 보안담당관의 확인을 거쳐야 함

> 신대장으로 이기하였음.
>
> 1. 이기사유 :
> 2. 비밀건수 : 급 건
> 3. 이기년월일 : 년 월 일
> 4. 이기자 직/성명
> 5. 보관책임자 : 서명 날인
> 6. 보안담당관 : 서명 날인

– 구대장 정리방법

• 구대장 주서 삭제는 비밀등급부터 사본번호까지

• 이기되는 비밀의 관리번호에 신대장에 부여되는 관리번호 병기

예)

관리 번호	수 발		
	년월일	발행처	수신처
287 ⇒1	2008. 10. 1	국정원	농식품부 운영지원과
288 ⇒2	2009. 1. 15	국방부	농식품부 운영지원과

– 신대장 정리방법

• 신대장 제일 첫면에 다음과 같이 갱신내용을 표기하고 보안담당관의 확인을 거쳐야 함

> 구대장에서 이기하였음.
>
> 1. 이기사유 :
> 2. 비밀건수 : 급 건
> 3. 이기년월일 : 년 월 일
> 4. 이기자 직/성명
> 5. 보관책임자 : 서명 날인
> 6. 보안담당관 : 서명 날인

Point

• 구대장 이기 비밀의 누락 등을 방지하고, 임의로 수정하는 것을 예방하기 위해 신대장 갱신시 제일 첫 면에 위의 갱신내용 기재 후 이기되는 비밀 등재

♣ 신대장에 이기된 비밀의 관리번호는 1번부터 새로 부여한다.

• 이기되는 비밀의 관리번호는 아래 예시와 같이 구대장 관리번호 병기

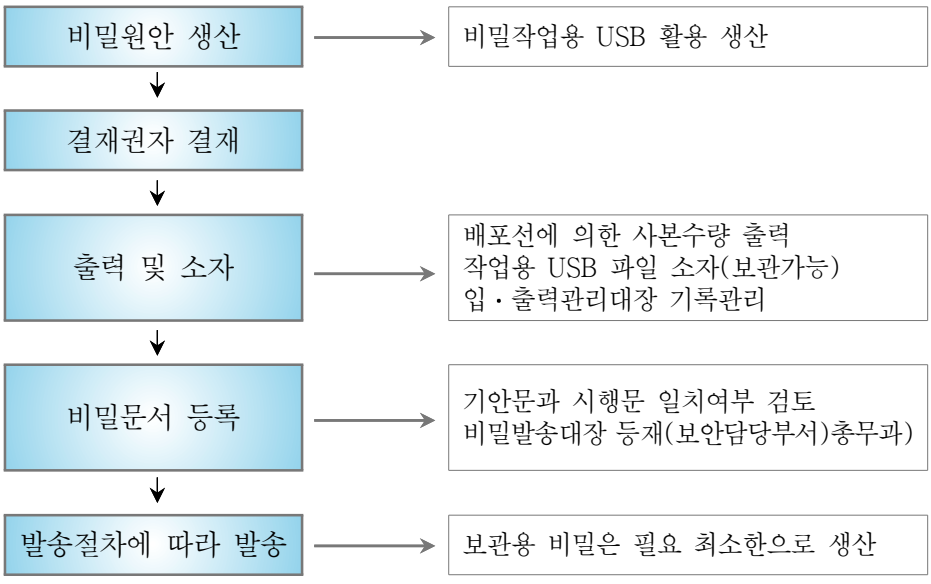
예)

관리 번호	수 발		
	년월일	발행처	수신처
287 ⇒1	2008. 10. 1	국정원	농식품부 운영지원과
288 ⇒2	2009. 1. 15	국방부	농식품부 운영지원과

※ 이기된 비밀의 수발 연월일 및 발행처는 구 대장에 기재된 당초의 내용으로 기재

※ 비밀 이기 후 비밀 문서의 관리번호는 대각선으로 삭제표시 후 신관리번호 부여

2-10. 비밀문서 생산(세칙 제 조)



※ 비밀의 생산은 관리기록부에 미리 등재된 보조기억장치에서 작업

※ 모든 비밀은 생산후 등록대장에 등재함으로써 발송번호를 부여받는 것이 원칙이나, 대내문서의 경우 자체 관리기록부에 등재후 관리번호를 등록번호로 활용할 수 있음

2-11. 비밀의 대출·열람(규정 제23조, 규칙 제36조, 세칙 제 조)

- 비밀의 대출 및 열람은 해당등급의 비밀취급인가자(업무상 직접관계자)에 한 함
  ※ 대출시 비밀대출부(규칙 별지 제11호 서식)에 기재
- 발행기관은 개개 비밀문서 말미에 열람자의 범위를 파악하기 위하여 「비밀열람기록전」(규칙 별지 제12호 서식)을 첨부하여야 하며, 비밀을 파기할 때에는 그 비밀과 분리하여 별도 보관(5년)
  ※ 열람기록전 미첨부 비밀은 접수전 발행기관에 반송 또는 열람기록전 첨부 관리
- 모든 비밀열람자는 비밀의 열람시(비밀문서 선람·결재포함) 그에 앞서 비밀열람기록전에 관계사항을 기재하고 서명 또는 날인 후에 열람 결재
  ※ 대출 및 열람은 당일 일과시간 및 청사내로 제한함(≠ 비밀의 지출)
  ※ 대외기관 자료제공시는「국가기밀자료 국회지원지침('04.11.24)」에 따라 제공

2-12. 비밀의 지출(규정 제25조, 규칙 제38조, 세칙 제50조)

가. 비밀은 시설 밖 지출 불가 원칙

※ 공무상 부득이 지출시에는 「비밀지출승인서」(규칙 별지 제13호 서식)에 의하여 보안담당관을 경유, 기관장의 승인을 얻은 후 지출할 수 있음.

Point

- 외주발간 목적 지출시는 비밀문서발간승인신청서로 갈음

나. 지출 절차

신청서 작성	결 재	제 출	지출 및 발간
비밀지출승인서 (규칙 별지 제13호 서식) 2부 작성	분임보안담당관 ⇒ 보안담당관 ⇒ 소속기관장	승인서 1부 제출 ⇒ 보안담당관 승인서1부 보관 ⇒ 지출자 보관	보안대책 강구 (밀봉포장 등)후 지출 및 발간

2-13. 비밀의 파기(규칙 제14조, 세칙 제53조 내지 제54조)

- 비밀의 파기는 소각, 용해 또는 기타의 방법으로 원형을 완전히 소멸시켜야 함.
- 비밀파기의 집행은 보관책임자 또는 그가 지정하는 입회자(비밀취급인가자)의 참여아래 비밀의 처리담당자가 집행함.
- 집행종료 후 비밀관리기록부의 파기란에 집행자가 일시를 기입·날인하고, 파기확인란에 입회자의 확인 날인(파기사실 증명)

2-14. 비밀소유 및 비밀취급인가자 현황 보고(규정 제29조, 규칙 제41조, 세칙 제32조)

소속기관	본 부
• 보고기준 : 6월말, 12월말 • 보고기한 : 7월 및 익년 1월 10일 까지 ※ 전 반기 보고내용과 이월건수 일치 여부 반드시 확인	→ • 실·국은 본부 보안담당관에 반기익월 10일까지 보고 • 보안담당관은 익월 25일까지 국정원 보고

2-15. 보안교육(세칙 제70조)

가. 보안담당관은 자체 보안업무의 향상과 발전을 위하여 전직원을 대상으로보안교육을 실시하여야 함

Point

• 특히 신규채용자와 비밀취급인가예정자에 대하여는 사전에 충분한 보안교육과 보안조치 필요

나. 교육의 종류 및 실시

– 정기교육 : 연 1회 이상 실시(정보 보안교육과 병행 가능)

※정보보안담당관은 연1회 이상의 정보보안교육을 실시한다.

– 수시교육

• 신규임용직원 및 전입자 : 임용 후 5일 이내에 실시

• 비밀취급인가 예정자 : 교육실시 후 인가

• 해외여행 예정자 : 보안담당관은 해외여행 전에 해당직무과 관련된 교육 실시(해외여행 계획 방침 결재 시 협조)

2-16. 비밀 관리부철의 보존(규칙 제55조)

♣ 다음 비밀관리부철은 5년간 보존하여야 함

① 서약서철
② 비밀영수증철
③ 비밀관리기록부(국가용 보안시스템 관리기록부 포함)
④ 비밀수발대장 및 영수증
⑤ 비밀열람기록전(철)
⑥ 비밀발간(복사) 통제부
⑦ 비밀대출부
⑧ 보안감사철

♣ 다음 비밀관리부철은 3년간 보존하여야 함

① 비밀입출력관리대장
② 보안심사위원회 회의록
③ 비밀발간 신청서
④ 보호구역 출입자 대장
⑤ 비밀취급인가증 교부대장 및 관계철

※ 상기 외의 비밀관리부철은 공공기관의 기록물관리에 관한 법률에 따름

❸ 시설보안

3-1. 보호구역의 설정

가. 보호구역(규정 제30조, 규칙 제42조, 세칙 제56조)

- 국가기밀의 보호와 주요시설, 장비 및 자재의 보호를 위하여 필요한 장소에 일정한 범위를 정하여 보호하는 구역
- 보호구역 설정권자 : 각급기관의 장, 국가중요시설·장비 및 자재를 관리하는 자
- 보호구역 설정자는 보안상 불필요한 인원의 접근이나 출입을 제한 또는 금지시킬 수 있음

Point
• 제한구역 및 통제구역의 설정은 최소한의 범위로 제한(규칙 제43조)

나. 보호구역의 지정(규정 제30조, 규칙 제42조, 세칙 제56조)

종 류	개 념	지 정
제한지역	비밀 또는 정부재산을 보호하기 위하여 울타리 또는 경비원에 의하여 일반인의 출입에 감시가 요구되는 지역	본부, 소속기관 및 산하기관이 사용하는 건물과 소속기관장이 지정하는 보안울타리 내 구역
제한구역	비밀 또는 주요시설 및 자재에 대한 비인가자의 접근을 방지 하기 위하여 출입에 안내가 요구되는 구역	종합상황실, 관제실, 통신실, 전산실
통제구역	비인가자의 출입이 금지되는 보안상 극히 중요한 구역	전시종합상황실, 국가지도통신실, 외교전문실, 암호장비실, 변전실, 저유탱크 또는 위험물 저장소, 보안장비가 설치된 장소

♣ 제한구역과 통제구역은 동일구역 내 중복해서 지정할 수 없음.

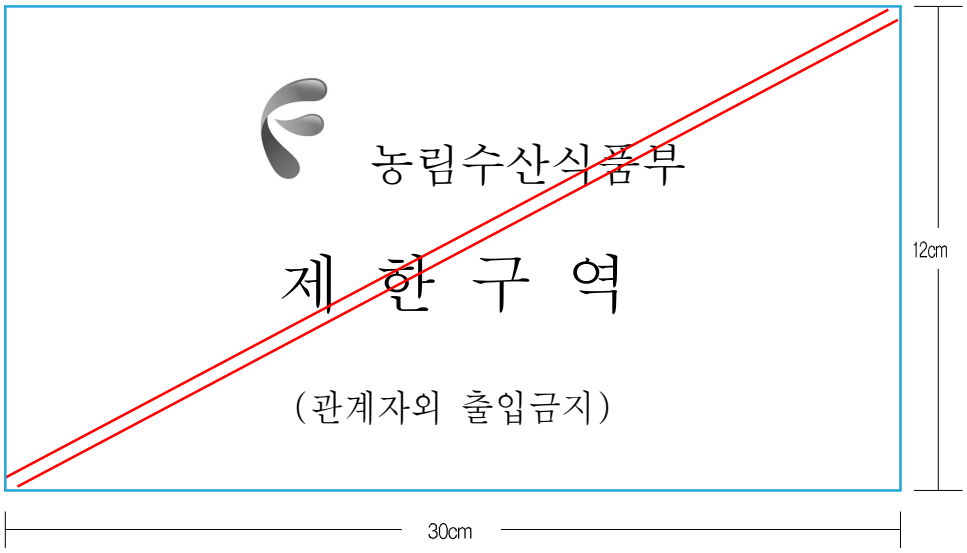
3-2. 보호구역의 관리

가. 보호구역의 관리(규정 제30조, 규칙 제42조, 세칙 제57조)

- 보호구역 총괄관리책임자 : 보안담당관
- 제한구역(통제구역) 관리책임자 : 동 구역 관할과장(팀장, 담당관)
  ※ 제한구역(통제구역) 관리 부책임자 : 관리책임자가 지정할 수 있음
- 보안담당관은 보호구역에 대한 보호대책 강구

Point

• 제한구역(통제구역)에는 아래와 같은 보호구역 표지를 부착하여야 한다.



※ 제한구역(통제구역)에 비인가자 출입시는 보안담당관이 지정하는 안내원 입회

나. 보호구역의 통제(규정 제30조, 규칙 제42조, 세칙 제59조)

① 보호구역 통제 일반 기준

보호구역	통 제 기 준
제한지역	외부출입자 동태감시 및 안내, 통제 등 실시
제한구역	관계직원 외 출입통제 실시
통제구역	상근자, 정·부책임자, 기관장 등 출입이 인가된 자 이외의 출입통제

※ 제한지역 출입시는 출입증 패용(정부청사출입증 및 출입에 관한규정)자만 출입 가능

- 제한구역(통제구역)에는 출입자관리대장(세칙 별지 제19호 서식) 비치 및 출입상황 기록 유지

※ 당해 보호구역에 근무하는 자 및 담당자는 상시출입 인가자로 간주, 별도 기록하지 않을 수 있음(세칙 제59조 제1항)

※ 종합상황실 등 근무인원이 24시간 상주하는 통제구역의 경우 별도의 출입기록 필요 없음

❹ 정보보안

4-1. 정보보안 용어의 정의(지침 제3조)

♣ 정보통신보안 ? 정보보안 ?

• 여기서 사용하는 『정보보안』이란 용어는 기존의 『정보통신보안』이라는 용어가 보안환경의 변화를 거치면서 보완된 용어임

⇒ 인터넷 사용 환경의 급진전과 이에 따른 고도 정보화가 진행됨에 따라, 통신수단에 대한 보호가 상대적으로 중요시 되는 통신보안이란 용어를 유, 무선통신수단을 매개로 하는 정보 그 자체의 보호를 중요시 하게 됨에 따라 정보통신보안에서 정보보안으로 용어 사용례 변화

① "정보통신망"
유·무선을 매개로 하는 다양한 정보통신 수단에 의하여 부호·문자·음향·영상 등의 정보를 수집·가공·저장·검색·송수신하는 정보 통신체제

② 정보보안" 또는 "정보보호"
정보통신수단으로 수집·가공·저장·검색·송수신 되는 정보의 유출·위변조·훼손 등을 방지하거나 정보통신망을 보호하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위

③ "국가용 정보보안시스템(또는 '보안시스템')"
국가정보원장이 기밀 등 중요자료를 보호하기 위하여 승인한 암호장비·암호자재 또는 암호논리·사이버안전기술이 적용된 프로그램이나 장치

④ "암호장비"
정보통신수단으로 처리·저장·송수신되는 정보를 보호할 목적으로 암호논리를 내장하여 제작된 장비나 장치

⑤ “암호자재”
Ⅱ급비밀 이하의 통신내용 및 정보자료를 비닉할 목적으로 사용하는 문자·숫자·기호 등으로 구성된 환자표(煥字表)와 난수 또는 암호논리 등을 저장한 문서나 도구

⑥ “음어자재”
Ⅲ급비밀 이하의 통신내용 및 정보자료를 비닉할 목적으로 사용하는 문자·숫자·기호 등으로 구성된 환자표 또는 암호논리 등을 저장한 문서나 도구

⑦ “약호자재”라 함은 대외비 이하의 통신내용을 비닉할 목적으로 특정 용어를 문자·숫자·기호 등으로 변환하여 수록한 문서나 도구를 말한다.

⑧ “암호취급자”라 함은 암호취급인가를 받아 암호체계를 연구·제작·수발하거나 국가용 보안시스템을 취급 관리하는 자를 말한다.

⑨ “전산자료”라 함은 전산장비에 의하여 전자기적인 형태로 입력·보관되어 있는 각종 정보(data)를 말하며, 그 자료가 입력되어 있는 자기테이프, 디스크 등 보조기억매체를 포함한다.

4-2. 정보보안의 대상 및 소통시 유의사항

가. 대 상

- 텔렉스, 팩시밀리, 국제전화 등 유무선 통신망
- 관계법령에 의한 허가를 요하는 무선국 통신
- 데이터 통신망
- 암호, 음어, 약호 등 자재 제작 취급사항

나. 소통시 유의사항

- VIP 행사 등 주요 행사일정
- 내·외신 동정에 관한 사항
- 주요협약 및 계약사항
- 주요시설, 사업계획서 등 주요현황
- 미확정된 주요계획 등

4-3. 정보 소통 방식별 취약성 및 보안대책

소통방식	취 약 성	보 안 대 책
유선전화	• 수화기접속 및 교환원에 한 도청 가능	• 주요내용 암호화 또는 암호 장비 이용
무선전화 (무전기, 차량전화, 휴대용전화, 국제전화, 시외전화)	• 무선 인식부족으로 보안의식 희박 • 통신방식이 무선으로 어느 곳에서나 도청가능 • 국제간의 통신위성 이용으로 어디서나 도청가능	• 암호사용, 암호장비 설치 • 비밀이나 불요불급 통화 엄금 (간단한 업무연락만 사용) • 통신보안의식 고취 및 교육 • 특히 휴대용 전화 및 차량 전화 운용자는 사전고지 및 보안관련 내용 소통시 제지 의무화
텔 렉 스	• 유선, 무선인식 부족으로 보안의식 희박 • 국제간은 통신위성 이용으로 어디서나 도청가능 • 유선도 중간선로단자 등에 의한 도청 가능	• 보안대책 없이 비밀내용 소통 금지 • 암호사용 또는 암호장비 확대 설치 • 국제간은 국가기관 외교 통신망 적극 활용
데이타통신	• 전산요원의 보안의식 희박 • 제3자 도청 용이 • 종합된 정보의 일시전송 기능으로 풍부한 정보 원천	• 데이터통신 보안장비 설치 • 암호 프로그램 개발 사용 (수시변경 운용) • 전송선로의 특별보호
팩시밀리	• 사진, 지도, 설계도 등 송신 편리로 보안성 무시 • 동일 수신장치로 도청가능 • 국제간은 통신위성 이용으로 어디서나 도청 가능	• 보안대책 없이 비밀내용 소통 금지 • 공개된 자료 이외의 소통 금지 • 암호화 소통 또는 도면 및 그림 등 암호화가 불가능한 내용은 국가기관 외교통신망이나 문서 수발계통 이용

※ 통신보안의 소통기준
- 대외비, Ⅲ급 비밀은 음어
- Ⅱ급 비밀은 암호
- 보안장비 사용

4-4. 정보 소통 방식별 보안통제

가. 모사전송기 사용에 따른 보안통제

- 비밀, 대외비문서는 물론 일반문서라 하더라도 국가안보 및 국가이익을 위하여 공개를 제한할 필요가 있다고 인정되는 사항은 음어화하지 아니하고는 송신 불가
- 모사전송하고자 하는 비밀 사항은 보안담당관 또는 분임보안담당관의 보안성 검토후 전송

나. 국제전화 사용에 따른 보안통제(지침 제21조)

- 보안담당관(또는 분임보안담당관)은 국제통신망으로 업무와 관련된 사항을 송수신 할 경우 통신내용, 통신망의 보안성 및 안정성에 대한 보안통제 실시

4-5. 국가용정보보안시스템의 배부·관리(규정 제5조, 규칙 제45조 내지 제52조)

※ 『국가용정보보안시스템』 은 암호장비, 암호자재 또는 암호논리, 사이버 안전기술이 적용된 프로그램 또는 장치로 통상 암호자재로 통용됨

① 암호자재

: 환자표(문자,숫자,기호등 으로 구성)와 난수 또는 암호논리 등 저장한 문서나 도구로 Ⅱ급비밀로 분류(암호자재는 현용, 예비용, 반납용으로 구분)

② 암호자재의 배부·반납

- 국가정보원이 지역별 기관단위로 배포
- 배부기관에 비치된 「인감등록서」(지침 별지 제14호 서식)에 등록된 자의 등록된 인감으로 직접 접촉에 의하여 배부 또는 반납

Point

- 암호자재 취급 인감은 본부를 경유해서 국정원에 이송(인감 등록사유 발생시 소속은 인감등록서를 본부 및 국정원 지부에 각 1부씩 제출 하여야 함)

- 암호자재는 사용기간 1개월 이전에 배부하고, 항시 예비용 암호자재를 최하단위 사용기관까지 48시간내에 배부할 수 있는 조치를 취해야 함.
- 암호자재의 배부, 반납, 파기, 오인소각 또는 분실 기타 사고의 증명은 「보안시스템증명서」(지침 별지 제12호 서식)에 의함

③ 암호자재의 관리

- 「국가용보안시스템관리기록부」(지침 별지 제9호 서식)에 의해 관리

※ 암호자재는 현용을 제외한 예비용 및 반납용에 대해서는 봉인후 보관

– 암호자재는 따로 비치된 비밀보관 용기에 보관하되, 그 보관함에 암호자재 이외의 다른 문건은 보관 불가 (지편식은 코팅부분 절단)
– 암호자재 취급자는 암호자재 등에 대해 수시점검 실시하고 「국가용보안시스템점검기록부」(지침 별지 제10호 서식)에 수시로 점검사항을 기록유지 하여야 함
– 암호자재를 보유하고 있는 보안담당관은 취급직원에게 수시로 교육 실시(단, 현용·예비용 암호자재는 교육용으로 사용 불가)
– 암호문을 작성·해독하기 위하여 사용한 작업용지는 그 유효성이 종료된 때에 파기하고, 통신문 여백에는 암호자재 사용근거 표시
– 암호자재의 긴급 파기
• 파기자 : 암호자재 관리자, 암호의 전송업무관리자
• 파기사유 : 긴급사태 발생으로 암호자재를 안전하게 보호할 수 없을 때
- 파기순위 : 반납용→예비용→현용
반납용 : 긴급사태가 발생하였다고 인정될 때
예비용 : 긴급사태가 악화시
현용 : 계속보유 불가능할 시(배부처가 많은 것부터 차례로 파기)
- 결과 조치 : 암호자재를 긴급파기 하였을 때는 소속 중앙국가기관의 장을 거쳐 국가정보원장에게 통보하고, 산하기관에도 그 사실을 통보
• 파기일시 및 장소
• 암호자재의 수량 및 등록번호
• 파기이유 및 방법
• 파기자 및 참여자의 직책, 성명
• 오인소각·소실·분실·누설시 결과 조치
- 소속 중앙국가기관의 장을 거쳐 국가정보원장에게 전통으로 통보 후 다음 사항을 서면으로 제출
• 사고일시 및 장소
• 암호자재의 명칭 및 수량 및 등록번호
• 사고경위
• 사고자 및 관계자의 인적사항
• 사고자 및 관계자에 대한 조치결과
※ 분실의 경우 분실한 취급자 및 보관책임자는 엄중문책 또는 징계조치

④ 암호자재의 인계·인수
– 암호자재 보관책임자가 교체될 때에는 보안시스템관리기록부에 그 내용을 기록하여 보안담당관의 확인을 받아야 함

암호자재 사용 방법

암호자재는 파손, 분실우려 등으로 인해 실제 사용례가 극히 드문 현실이나, 개인 PC에 각종 자료의 저장 및 인터넷상 자료 소통이 빈번히 이루어 지고 있는 현실을 감안해 볼때 적극 활용 할 필요가 있음

설치디스켓 설치

① “현용자재 설치” 디스켓 삽입
② set-up 파일 실행
③ 패스워드입력(※패스워드는 비밀사항이므로 생략)
④ 현용자재 설치파일 복사
⑤ 패스워드 설정(4자리)
☞ 설치 완료

암 호 화

① 현용자재(안보xx-xx)삽입
※ 암호자재 삽입된 상태에서만 작업가능
② 바탕화면의 “안보-xx"아이콘 실행
③ 비밀번호 입력
④ 암호화 선택(hwp,txt, xls, ppt 등)
⑤ 암호화 할 문서 선택
⑥ “일괄작업시작” 클릭
☞ 암호화 작업 완료
※ 암호화된 파일은 C/temp/encrypted/폴더에 생성됨

복 호 화

① 현용자재(안보xx-xx)삽입
② 비밀번호 입력
③ 복호화 클릭
④ 복호화 할 파일 선택*C/temp/encrypted/암호화화일*
⑤ 복호화 일괄적업 시작
☞ 복호화 작업 완료
※ 복호화된 파일은 C/temp/decrypted/폴더에 생성됨

4-6. 정보통신실 및 정보자료의 보안관리

가. 정보통신실 보호대책(지침 제27조)

- 전산실의 보호구역 설정 : 전산실 운영기관의 장
- 보호대책 강구
  - 방재대책 및 외부로부터의 위해(危害) 방지대책
  - 항시 이용하는 출입문은 한곳으로 하고 이중잠금장치 설치
  - 출입문 보안장치 설치 및 주야간 감시대책
  - 보조기억매체를 보관할 수 있는 철제용기 비치
  - 보조기억매체에 대한 안전지출계획 수립
  - 관리책임자 및 자료·장비별 취급자 지정 운용
- 전산실의 통제구역에는 「통제구역출입자관리대장」(세칙 별지 제13호서식)를 비치, 기록·유지

  ※ 비인가자의 출입을 제한하며, 통제구역 상근자와 업무상 수시로 출입을 요하는 자에 대하여는 기간을 한정하여 출입인가 가능
- 비인가자가 업무상 부득이한 사유로 전산실을 출입하여야 할 경우 통제구역출입자명부에 기재하여 전산보안담당관의 승인을 얻은 후 담당자의 안내를 받음.

나. 정보자료 보호대책(지침 제28조)

- 보호대책 강구
  - 자료복사본(예비) 확보 및 안전지역 별도 보관
  - 전산자료(보조기억매체)보유현황 관리
  - 전산자료 및 장비의 반·출입 통제
  - 불법접근 및 컴퓨터바이러스 피해예방
  - 전산자료 접근권한 구분
  - 예비(Back up)체계 수립 시행

다. 단말기 취급자 및 관리책임자 지정 운용 : 지침 제39조 참조

라. 비밀번호 사용 및 관리 : 지침 제41조 참조

※ 비밀번호가 기록된 「전산장비 관리대장」(지침 별지 제4호 서식)은 비밀에 준해 관리

마. 비밀자료의 입력 : 지침 제34조 참조

※ 비밀자료 입력시 「비밀자료 입·출력대장」 (자체지침 별지 제22호 서식)에 작업내용 기록 유지

바. 보조기억매체의 관리 : 지침 제35조 참조

※ 비밀자료가 저장된 보조기억매체는 매체별로 해당 비밀등급 및 관리번호를 부여하고 비밀관리기록부에 등재 후 이중캐비닛 또는 금고에 보관

※ 보조기억매체가 국가용 보안시스템에 해당될 경우에는 국가용 보안시스템 관리기록부에 등재 및 관리

사. 비밀자료의 출력

※ 취급자가 비밀자료 열람 또는 출력할 때에는 「비밀자료 입·출력대장」에 열람 및 출력 사항을 기록하고 열람자 및 수령자의 서명을 받아야 함, 또한, 비밀자료 출력시 발생한 파지 등은 작업종료 후 회수하여 즉시 파기하고 비밀자료 입·출력대장」의 '비고' 란에 그 사항을 기록하고 서명

4-7. 개인용 컴퓨터 보안관리

가. 관리책임자 표지 부착 : 지침 제39조

부 서 명				
관리책임자	직		성 명	
취 급 자	직		성 명	
관리번호				

나. 컴퓨터의 비밀번호 부여(지침 제41조)

※ 비밀번호가 기록된 「전산장비 관리대장」은 비밀에 준해 관리

다. 비밀자료의 입·출력 작업 관리(지침 제34조)

※ 비밀자료의 전자적 생산·열람·출력·송수신·이관시는 작업내용을 전자적으로 기록 유지하여야 함

※ 전자적 처리된 비밀자료의 종이문서 출력후의 취급관리는 보안업무규정을 따름

※ 비밀자료 생산 완료후에는 비밀내용을 삭제하여야 함.

Point

- 비밀자료를 PC에 별도 저장할 경우에는 독립된 폴더를 지정, 국가용 보안시스템을 사용하여 암호화하는 등 보안대책을 강구하여야 함

– 비밀 입·출력·열람 등의 작업시는 「비밀자료입·출력 관리대장」에 작업내용을 기록하고 수령자의 서명을 받아야 함
– 비밀자료를 입력시에는 비밀자료 생산용 디스켓을 지정하여 사용하고 비밀등급과 예고문을 함께 사용
– 비밀자료 출력을 완료한 디스켓의 비밀내용은 소자 처리
※「비밀자료 입·출력대장」의 '비고' 난에 소자사실 기재하고 서명
※ 비밀 내용이 입력된 디스켓을 계속 사용하거나 보관의 필요성이 있는 경우에는 비밀관리기록부」에 등재하여 관리
– 비밀자료 초안지를 파기할 경우 또는 출력시 발생한 파지등은 즉시 회수하여 파기하고 「비밀자료 입·출력대장」의 '비고' 난에 기록하고 서명
– 출력한 비밀자료의 관리번호는 1부만 출력시는 원본으로 하고 2부 이상 출력시는 1부는 원본 나머지는 사본번호 부여

♣ 소자(消磁)란?

저장매체에 역자기장을 이용해 매체의 자화값을 "0"으로 만들어 저장자료의 복원이 불가능하게 만드는 것을 말함

라. 디스켓 관리(지침 제35조)

– 반복되는 업무나 중요한 자료가 입력된 디스켓을 계속 사용 하고자 하는 경우 반드시 해당 실·와 단위로 관리번호를 부여·사용
– 관리번호는 「비밀관리기록부」에 의한 일련번호 형식으로 부여
※ 다만, 실·와 단위로 관리가 비효율적인 경우 계단위로 관리
– 디스켓에는 『해양수산부 정보보안기본지침』 별지 제9호서식의 디스켓 관리번호 표시를 부착하여 관리하여야 한다.

Point

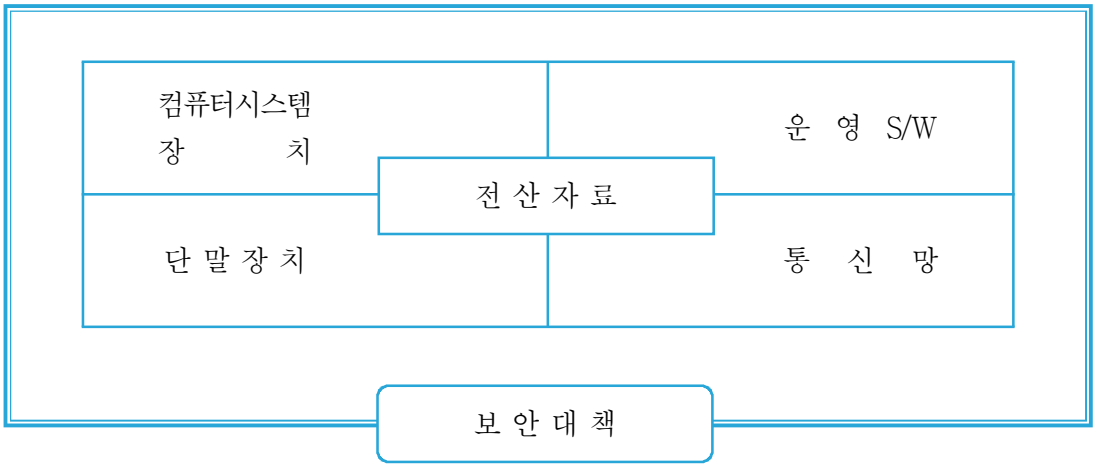
• 비밀(대외비)작업은 관리번호가 사전에 등재된 보조기억장치에 입력하고, 출력후 소자하는 것이 원칙임. 다만, 충무계획, 을지연습 등 매년 반복적으로 생산되고 그 내용이 대동소이한 경우는 매년 새로 작성하는 것이 비 효율적이기 때문에 별도의 보관용 디스켓에 여러건의 비밀내용을 관리할 수 있음.

– 이 경우 보관용 디스켓의 관리번호는 하나로 관리하더라도, 저장된 각각의 비밀 파일 목록은 따로 관리하여야 함

4-8. 전산보안

가. 전산보안의 정의

① 전산보안이란 컴퓨터에 의해 처리·보관·전송되는 전산자료와 이와 관련된 전산자원(컴퓨터·운영S/W 및 통신망 등)을 각종 침해로부터 보호하는 것



② 이론적으로는 기밀성·무결성 및 가용성 등 전산시스템의 3대 특성을 확보하는 행위

※ 기밀성(Confidentiality) : 컴퓨터에 기록된 내용이 비인가자에게 유출되지 않도록 하는 것과 유출되더라도 그 내용을 확인할 수 없도록 하는 것 ⇒ 자료 유출 방지

※ 무결성(Integrity) : 컴퓨터에 기록된 내용이 비인가자에 의해 무단 변경되지 않도록 하는 것 ⇒ 자료의 변조방지

※ 가용성(Availability) : 인가자가 필요할 때 언제든지 전산시스템을 사용할 수 있도록 정상상태로 유지하는 것 ⇒ 자료의 파괴 방지 및 장애방지

③ 전산보안은 통신회선의 연결 유무에 따라 전산망보안과 개인용컴퓨터(PC) 보안으로 구분할 수 있음

※ 전산망보안은 자료접근통제, 모니터일, 암호화 등 기술적인 보안대책이 중요함

※ PC보안은 디스켓관리, 대장기록, 출력자료 등 관리적인 보안대책이 중요하며 문서보안과 일맥 상통 ⇒ 전산보안의 핵심은 비인가자의 접근이나 인가없이 사용하는 것을 방지하는 자료접근통제(Data Access Control)임

나. 보호대상

① 1차 대상 : 전산자료

– 전산화되어 컴퓨터에 보관되어 있는 자료(Data)

- 국가기밀, 개인정보, 산업정보 등 각종자료
- 업무별로 구축된 데이타베이스

– 전산자료가 수록되어 있는 디스크, 테이프 등 보조기억매체 포함

② 2차 대상 : 전산자원

– 주전산기, 단말기 등 전산시스템
– 운영프로그램(s/w)
– 통신망 등

다. 보안취약요인

① 침해형태

– 전산자료의 유출·변조 및 파괴
– 전산장비의 절취, 파괴 및 장애유발

② 위협요소

– 비의도적 위협
  - 자연재해
  - H/W, S/W의 고장
  - 운용요원의 실수 또는 미숙으로 인한 과실
– 사람에 의한 고의적인 행위
  - 외부요소 : 도청(Tapping), 해킹(Hacking)
  - 내부요소 : 운용요원·개발요원·단말기취급자 및 출입자 등

③ 보안취약요인

– 내부요인
  - 전산망 : 운용요원·개발요원 및 유지·보수자 등
  - 워드프로세서 : 취급요원
– 외부요인
  - 해커(Hacker)등 전산전문가, 컴퓨터바이러스 등
  - 홍수·지진·번개 등 기상악화, 정전, 전자파 등

< 전산망운영관련 보안취약요인 >

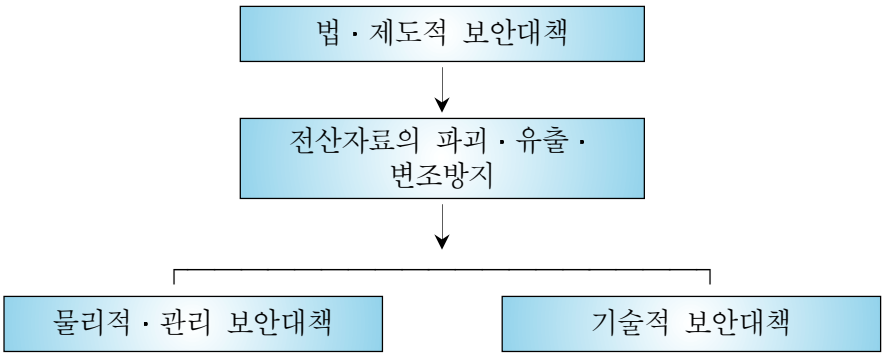
구 분	대 상	취 약 요 인
전 산 망	전산자료	• 도난, 파괴, 손상 • 무단복사, 유출
	주전산기	• 파괴, 고장 • 전자파 방출
	전산회선	• 불법접속, 회선파괴 • 전자파 방출
	단말기	• 비밀번호 파괴
운용요원	시스템 운용자	• 자료변경, 파괴 • 자료유출·누설
	프로그래머	• 프로그램 부정조작 • 조작미숙, 고장유발
	유지보수자	• 고의적인 고장유발 • 조작미숙, 고장유발
	단말기 운용자	• 비밀번호 노출 • 무단열람·출력

라. 전산보호대책

① 전산보안대책이란?

컴퓨터에 의해 처리·보관·전송되는 전산자료와 이와 관련된 전산자원을 각종침해행위로부터 보호하는 제반수단을 말함

- 법·제도적 보안대책
- 물리적·관리적 보안대책
- 기술적 보안대책 등 3가지로 구분, 보안대책 강구



② 인적 보안대책의 중요성

– 보안대책이 아무리 완벽하게 구비되어도 이를 실제로 운영하는 주체는 사람

※ 컴퓨터범죄의 80%이상이 내부인의 소행으로 파악

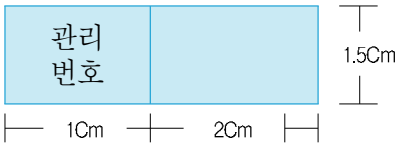
▸ 따라서, 장비, 제도 등 물리적인 보안대책의 보완은 이차적인 보호수단일 뿐 실직적인 보안대책의 토대는 인적 구성원에 대한 의식 제고에 있음

Ⅲ 주요 보안업무 처리요령

① 비밀(대외비)생산시 업무처리

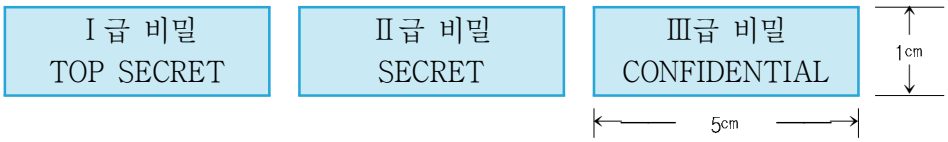
가. 관리번호의 표시

– 비밀(대외비)관리기록부에 등재하여 부여된 일련번호로서 생산문서의 좌측상단에 다음과 같이 표시



나. 비밀표시

– 비밀은 매면 중앙 상,하단에 해당 등급(Ⅰ · Ⅱ · Ⅲ)표시

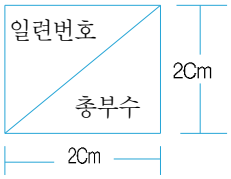


– 대외비는 첫페이지 상단 중앙에 표시하고, 첨부물이 있을 경우 첨부물 첫 페이지에도 표시

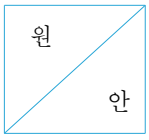
다. 사본표시

– 우측 상단에 다음과 같이 표시

※ 일반례

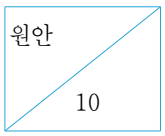


※ 내부결재의 경우

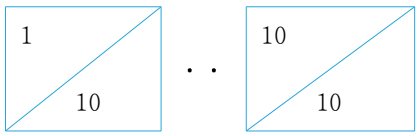


※ 받는곳이 10곳일 경우의 예

(기안문)



(시행문)



♣ 실제 생산된 건수는 사본(10건) + 원본(1건)을 합하여 11개임

라. 첨부물에서 분리되면 일반문서로 재분류 가능여부 표시

– 기안문에 비밀내용이 없고, 첨부물만 비밀인 경우 표시

첨부물에서 분리되면(일반문서)로 재분류

※ 당연히 유첨문서의 문서표지에만 표시가 가능함.

마. 예고문 표시

– 비밀은 그 문서 말미 “끝”옆에, 책자는 표지하단에 표시

원본	보호기간, ~ 로 재분류(일자 또는 조건)	보존기간 :
사본	파기, ~ 로 재분류(일자 또는 조건)	

바. 검토필 표시

– 생산비밀(원본)은 정기적(6월말, 12월말)으로 검토후 하단 여백에 검토필 표시

검토필(. . .) 인

② 비밀(대외비)관리기록부 기재요령

가. 관리번호

– 작성 또는 접수순위에 따라 누년(총) 일련번호 부여

1, 2, 3, 4, · · · · ·

※ 관리기록부 갱신시는 이월되는 비밀의 관리번호를 1부터 새로 부여

나. 연월일

– 접수문서는 실제로 접수된 일자를 기재

– 생산문서는 최종결재권자의 결재를 득한 날을 기재

다. 발행처

– 접수문서는 시행(발행)기관명 또는 기관내 문서일 경우 부서명을 기재

예)행정안전부부, 교과부, 운영지원과 등

– 생산문서는 생산부서명을 기재

예) 운영지원과, 행정지원팀 등

라. 수신처

- 접수문서는 자기 부서명 또는 기관의 문서일 경우 기관명 기재
  예) 운영지원과, 행정안전부 등
- 생산문서는 그 문서가 도달할 기관명 기재
  예) 국가정보원, 통일부

마. 문서번호

- 기관기호 및 문서분류번호 기재
  예) 운영지원과-1234

바. 비밀등급

- 분류된 등급을 로마자로 표기
  예) Ⅰ급, Ⅱ급, Ⅲ급, 대외비
- 전시하 수송할 비밀의 경우는 Ⓐ로 표기("전시비밀문서관리지침"참조)
  전시 수송대상 비밀 : 모든 원본, 충무계획, 을지연습 관련 문서 등

사. 형태

- 비밀문건의 외형상의 형태 기재
  예) 문서, 책자, 사진, 필름, 챠트, 테이프, 디스켓 등

아. 건명

- 문서제목 기재

자. 사본번호

- 비밀문건의 사본번호 기재(원/본, 원본/1, 원본/5, 원본/30, 5/30 등)
- 접수한 비밀은 그 문서의 사본번호 기재(1/1. 1/5 등)

차. 예고문

- 해당문건에 표기된 비밀자체의 예고문 기재

카. 처리담당

- 업무처리담당자 성명 또는 부서명 기재

타. 보관장소

- 비밀을 보관하는 실·과명 또는 부서명 기재

파. 등급변경

– 변경된 등급(일반문서 재분류 또는 직권 재분류)을 기재하고 재분류 일시 기재 및 담당자 날인

예) 2001. 2. 20.
일반문서 재분류(인)

하. 파기

– 파기를 직접 실시한 자의 성명(날인)과 파기일시 기재

예) 2009. 2. 20
홍길동(인)

거. 파기확인

– 비밀 파기시의 입회자의 비밀의 완전 파기를 확인한 후 날인

너. 근거

– 비밀을 재분류 또는 파기하였을 경우 그 근거 기재

예) • 예고문에 의하여 파기 또는 재분류–예고문
• 재분류 통고 공문에 의하였을 때 – 문서번호
• 전언통보에 의하였을 때 – 발신기관명, 송화자, 일시

더. 영수증

– 생산된 비밀(Ⅱ급 이상)을 발송하였을 경우 접수기관 수령자의 영수증 일련번호 기재

러. 수령자

– 비밀 발송시 접수기관에 직접 전달하였을 경우는 인수자의 성명 및 날인을 받으며, 문서수발계통을 통하여 발송할 경우에는 수발담당자의 날인을 받음

3 비밀영수증 기재요령

- 연도별 구분 일련번호 부여 또는 누년 일련번호 부여
- 비밀송증과 비밀영수증의 일련번호는 일치하도록 기재
- 송증의 수신란은 비밀을 접수하는 기관의 장 기재
- 비밀발송자는 이상시의 사유란, 접수자란, 접수일자란을 제외한 기타의 란 전부를 다 기재한 후 발송
- 접수기관의 접수자는 비밀의 제목, 사본번호, 수량 등을 기재내용과 대조한 후 이상이 있을 때는 그 사유를 기재하여 영수증을 반송하고 그 비밀을 처리할 실·국의 담당자에게 통보
- 영수증을 반송받은 기관의 처리담당자는 그 영수증과 분리하여 보관되어 있던 송증에 원래대로 첨부하여 비밀영수증철에 보관

【 비밀영수증 양식】

① 일련번호		비 밀 송 증	②발송일자	20 . . .
③ 수 신		④ 참 조		
⑤ 건 명				
⑥ 사본번호		⑦ 수 량		⑧ 등기번호	
⑨ 발송책임자	직위 직명	주민등록번호	성명	㊞

절 취 선

① 일련번호		비밀영수증	②발송일자	20 . . .
③ 수 신		④ 참 조		
⑤ 건 명				
⑥ 사본번호		⑦ 수 량		⑧ 등기번호	
⑨ 이상시의 사 유				
⑩ 발송책임자	소속	주민등록번호	성명	㊞
	직위 직명			

0103-1-6A
1969.2.26 승인

190×268mm(신문용지 50g/㎡)

④ 비밀취급인가자 및 비밀소유현황 작성

가. 비밀취급인가자 현황

- 조사기준일 : 6월말, 12월말기준(년 2회)
- 해당인가등급별(Ⅰ급, Ⅱ급, Ⅲ급)로 기준일 현재 인가된 인원수를 기재

나. 비밀소유현황

- 조사기준일 : 6월말, 12월말 기준(년 2회)
- 비밀소유현황조사
  - 가 월 란 : 전 기준일 현재의 보유량을 그대로 이기
  - 비밀등급별 상단 : 각 월별 접수, 작성, 이첩 등의 증가 숫자를 청색 또는 흑색
  - 비밀등급별 하단 : 각 월별 파기, 재분류, 기타(이송, 이관 등) 감소숫자를 적색
  - 현 보 유 량 : 상단의 증가치와 하단의 감소치를 상계한 현보유량
- 비밀현황 증감내역
  - 월별 접수,작성, 이첩란은 청색 또는 흑색으로, 파기·재분류·기타란은 적색으로 기재
  - 작성란은 자체 최초 발기작성(응신사항포함)한 비밀의 원본건수 기재

Point

- 비밀현황 증감내역의 이월란에 해당하는 “작성”란(다음 페이지 【서식예시】에서 A 표시란)은 전 반기말 보고된 비밀 총 건수중 이월된 원본의 개수임. 따라서 대부분의 기관은 자체 을지연습 계획 등 자체 원본을 가지고 있기 때문에 서식 예시의 A 표시란이 0인 기관은 정확히 기재하였는지 확인 할 필요가 있음

- 상위비밀등급으로부터 하위등급으로 저하된 경우 상위 비밀등급의 재분류란은 적색으로 하되, 저하된 하위등급의 증가표시는 그 비밀이 접수된 비밀이면 접수란에 자체에서 작성한 비밀이면 작성란에 기재

  예) 접수된 Ⅱ급 비밀이 Ⅲ급비밀로 재분류된 경우

  Ⅱ급비밀의 재분류란 – 적색

  Ⅲ급비밀의 접수란 – 청색 또는 흑색

- 기타란은 보유비밀(관리기록부에 등록보관중인 것)을 타처 이송, 이관, 기타 발송한 숫자를 기록하되 최초 배포계획에 의한 발송숫자는 기록하지 않음

- **계산방법**

  [이월(접수+작성+이첩) + 각월별 증가 – 각월별 감소]= 현보유량(다음 반기 이월)

※ 파기, 재분류, 기타의 감소사유는 이월될 수 없으므로 이월란의 하단(다음페이지 【서식예시】의 B 표시된 란)은 기재할 수 없음

※ 다음페이지 【서식예시】의 C 표시된 현 보유량중 작성(원본 건수)란은 다음분기 보고시 이월란의 작성(원본건수)과 다를 수 있음(월별 증감시 파기된 비밀은 원본 또는 사본일수 있기 때문)

【 서식 예시 】

(상,하)반기 비밀취급인가자 및 비밀소유 현황

1. 비밀취급인가자 현황

구 분	Ⅰ급	Ⅱ급	Ⅲ급	계	비 고
인 원					

2. 비밀소유현황

가. 비밀소유현황조사서

월 / 등급	이월	1월	2월	3월	4월	5월	6월	현보유량
Ⅱ급								
Ⅲ급								
계								

나. 비밀현황 증감내역

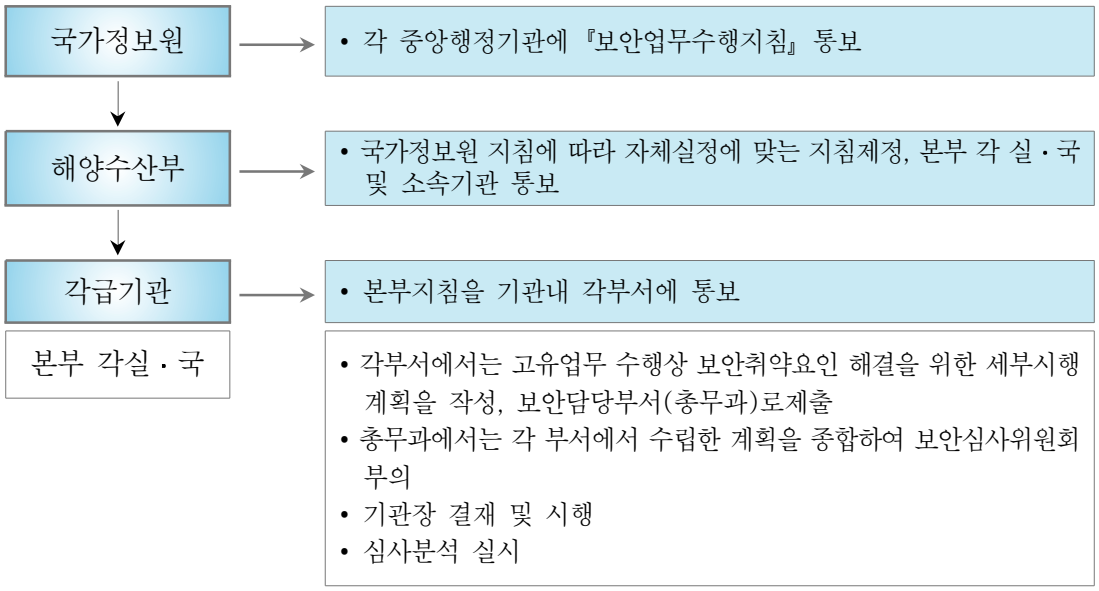
비밀 등급	구분 \ 월	이월	1월	2월	3월	4월	5월	6월	현보유량
Ⅱ급	접 수								
	작 성	A							C
	이 첩								
	파 기	B							
	재분류	B							
	기 타	B							
Ⅲ급	접 수								
	작 성	A							C
	이 첩								
	파 기	B							
	재분류	B							
	기 타	B							

5 연도 보안업무추진계획 수립

가. 계획수립 방침

- 국정원 및 본부 지침에 따라 사업별로 체계적 계획수립
- 구체적으로 실시 가능한 계획수립
- 자체실정에 부합하면서 개선위주의 계획수립
- 기본활동지침(국가정보원 배부)에 의거 작성
- 소속기관 계획 반영통한 종합계획 수립
- 보안심사위원회 심의 확정후 시행

나. 계획수립 절차



다. 계획서 작성요령

1. 보안환경

2. 활동목표 및 기본방침
   가. 활동목표
   나. 기본방침

3. 중점 활동사항

【국가보안】

사업명	세부추진계획	비고

【정보통신보안】

사업명	세부추진계획	비고

4. 보안업무 산하기관 현황

6 보안업무 심사분석

가. 실시시기 : (년 1회, 매월 9월말 기준 10월 15일까지 본부 제출)

나. 심사분석의 의의 및 방업

- 의의 : 목표나 계획을 기준으로 최초에 의도한 성과를 어느정도 달성했는가를 자체 분석하는 사후 평가제도
- 방법 : 년초 보안업무 추진계획상 사업계획의 실효성 및 타당성에 대한 측정, 사업목표에 대한 달성도 측정, 능률성 측정

Point

- 년말 보안업무평가 결과에 대한 포상시 심사분석 결과(50%) 및 보안감사 결과(50%) 반영

다. 유의사항

- 이행상태 확인 점검 및 형식적 심사분석 지양
- 업무개선 실적은 보안업무 제도개선, 규정·지침보완, 보안대책 강구시행, 보안직무지식 배양 및 보안의식 고취사항 등 기재
- 조직개편사항 보완
- 시행실적은 분야별(제도개선, 항만, 선박 등)로 기재
- 계획대 실적의 비교분석이 용이하도록 가능한 계량화하여 개조식으로 작성
- 사업부진원인, 사업이행결과 도출된 문제점 등 적시 및 개선대책 제시
- 보안심사위원회 부의

라. 작성요령

○○ 년도 보안업무심사분석

1. 총 평

기관별 총사업추진개요, 사업중점방향과 성과, 주요사업대비 등 약술

2. 보안조직·인원 변동사항

가. 보안조직

나. 조직·인원 변동사항

【 작성예시】

• 조직 및 인원 변동사항 (전년도 4/4분기 ~ 당해년도 3/4분기)

보안담당관				분임보안담당관				비밀취급인가자		비고
신설	폐지	교체	현원	신설	폐지	교체	현원	2008년	2009년	
–	–	1	1	–	–	11	13	245	246	

※ 신설 : 농관원 00지원 000 출장소 등

※ 폐지 : 농식품부 000과

3. 보안제도 개선 및 주요 성과분석

– 보안제도 개선사항

– 주요 성과분석

– 미흡한 사항

4. 세부사업별 실적 분석

【 국가보안】

사업명	추진실적	문제점	개선대책

【 정보보안업무 심사분석】

「농림수산식품부 정보보안지침」 별지 제2호 서식 참조

7 보안담당관 인계인수서 작성 예시

보안담당관 인계인수서

20 . .

농림수산식품부
Ministry for Food, Agriculture, Forestry and Fisheries

【00000과】

인 계 인 수 서

20 . 00. 00자 인사발령에 의거 농림수산식품부 보안담당관의 업무를 붙임과 같이 인계인수함.

20 . 00. 00.

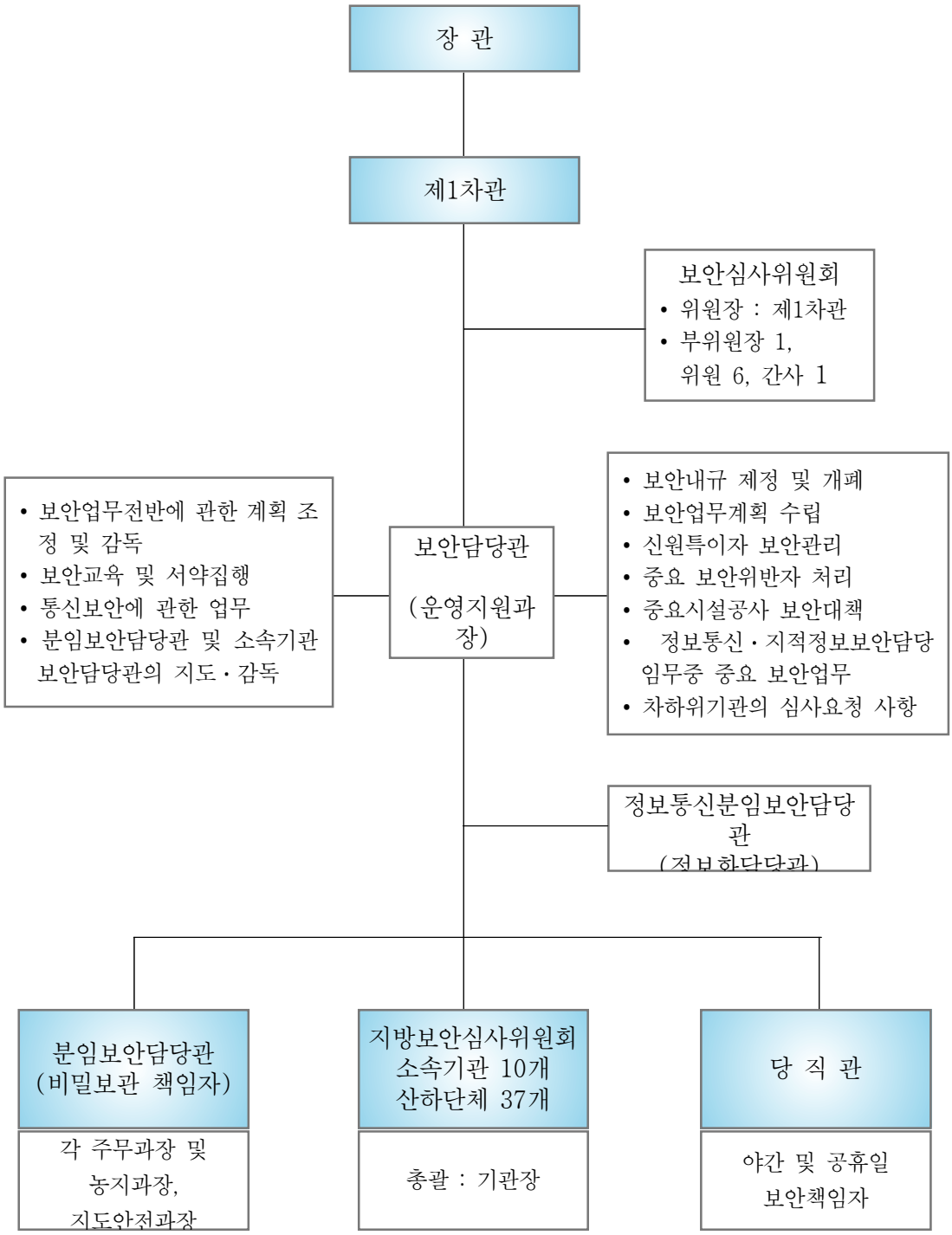
인계자 전임 보안담당관 직급 성명 (인)

인수자 신임 보안담당관 직급 성명 (인)

입회자 서무담당 직급 성명 (인)

1. 보안관리체계

【작성예시】



2. 00연도 보안업무 활동목표 및 중점 활동사항

가. 활동목표

○
○
○

나 중점 활동사항

○
○
○

3. 00연도 중요 보안업무 추진 계획 및 실적

('00. 00. 00 현재)

분야별	추진계획	추진실적
일반보안	□ ○ □ ○	□ ○ □ ○
정보보안	□ ○ □ ○	□ ○ □ ○

4. 비밀보유 및 비밀취급인가자 현황

(20 .00.00 현재)

실·국	비밀보유현황(건)				비밀취급인가자(명)		
	계	Ⅱ급	Ⅲ급	대외비	계	Ⅱ급	Ⅲ급
0000과							
0000국							
0000실							

5. 음어자재 보유현황

(20 .00.00 현재)

구 분	자 재 명 칭	수 량		등 록 번 호	비고
		보관	배부		
행정공통용	안보 00-00호 국가기관 음어자재 운용매뉴얼			~ N0 - N0	지편 책자
동원업체용	안보 00-00호			K - K	CD
	계				

6. 암호장비 보유현황

(20 .00.00 현재)

순위	장비명	등 록 번 호	장 비 일련번호	설 치 장 소	상 대 국	회선 방식	설치일	비 고
1	AF-87							
2	AF-87							

⑧ 암호자재 운용 및 관리

< 관 련 법 규 >

- 보안업무규정 및 보안업무규정시행규칙
- 국가정보보안기본지침
- 통신보안자재운용 관리지침
- 사무관리규정 및 동 시행규칙

가. 암호자재의 종류 및 소통한계

– 암호(난수+환자표) : 평문을 1차 숫자로 변환한 후 2차 난수를 가감하는 것으로 Ⅱ급 비밀까지 소통

나. 암호자재의 배부·반납

– 암호자재의 수발권자
  • 암호자재는 인감등록된 정·부책임자가 직접 수·발
  • 정·부 책임자가 직접 수령이 불가능할 경우
– 정책임자의 위임장을 소지한 관계자
– 배부, 반납시 확인사항
  • 등록번호와 보안시스템증명서와의 일치여부
  • 보안시스템증명서상의 부수와 실부수와의 일치여부
  • 보안시스템증명서 인감도장 확인

다. 보안시스템증명서

– 암호자재의 배부, 반납, 파기 및 잘못파기, 분실 등 모든 증명은 지침 별지 12호 서식에 의한 보안시스템 증명서에 의거 증빙

라. 인감등록서 관리

– 인감등록은 정·부책임자 및 실무자 공동 등록
– 인감등록철 보관은 10년
– 구인감등록은 사선후 인감등록 보관철에 합철보관
– 정·부책임자 및 실무자중 한명만 교체되더라도 함께 신규등록

마. 암호자재의 관리

– 책 임

• 모든 암호자재의 관리에 관하여는 제작기관의 장이 책임을 진다.
• 암호자재를 배부받은 기관은 그 기관의 장이 책임을 지며 또한 인감등록이 되어 있는 정·부책임자 및 실무자가 행위에 대한 책임을 진다.

– 기록유지
• 암호자재를 보유하고 있는 모든 기관은 보안시스템 관리기록부를 별도 비치하고 기록, 유지하여야 하며, 수령과 동시 동 관리기록부에 기록한다.
• 암호자재는 비밀관리기록부에 기록하지 아니하고 관리번호도 부여하지 않는다.
• 따라서 보안시스템 관리기록부는 비밀관리 기록부와 동일하게 취급하여야 한다.

– 인수인계
• 보관 정·부책임자 교체시에는 자재기록부에 인수인계 사항을 명시

<예 시>

보안시스템(암호자재) 인계 인수서

1. 인계인수사유
2. 보유자재 현황

행정공통용(디스켓식)

(예시) 안보 55-00호 부(현용)
안보 55-00호 부(예비용)
행정공통용(지편식)
(예시) 안보 56-00호 부(현용)
안보 56-00호 부(반납용)

위와 같이 정히 인계 인수함

년 월 일

인 계 자	직	급	성명	(인)
인 수 자	직	급	성명	(인)
확 인 자	보안담당관		성명	(인)

바. 암호자재의 보관

– 보관장소

• 암호자재를 생산하는 기관은 암호취급소를 별도로 시설한 후 암호취급소내 2중금고 또는 2중 캐비넷에 보관

• 암호자재를 운용하는 기관은 암호자재를 보유하고 있는 당해부서의 비밀캐비넷내에 별도의 자재함을 비치하여 보관

– 보관방법

• 암호자재는 반납용, 현용 및 예비용으로 구분 보관

• 현용을 제외한 반납용, 예비용은 봉인하여 보관

• 자재 보관함에는 암호자재 이외의 문건과 혼합 보관 금지

– 점 검

• 암호자재의 점검은 암호책임자에 의하여 수시 점검

• 암호자재의 수시 점검에 대한 기록은 월1회 보관책임자가 확인(점검기록부 관리)

사. 암호자재의 운용

– 암호자재 사용범위

• 비밀·대외비 또는 비밀이 아니더라도 누설될 경우 국가이익을 해할 우려가 있는 내용은 평문으로 수발 금지

– 암호자재의 사용표시

• 문서를 암호자재를 사용하여 통신망으로 수발한 경우에 기안용지의 취급난에 사용 암호자재 표시

• 암호자재 사용대장 비치 기록유지

– 암호자재 사고시 조치사항

암호자재를 잘못 파기, 분실 또는 누설하였을 때는 지체없이 교육부장관에게 미리 전통으로 보고하고, 사고일시 및 장소, 암호자재의 명칭, 수량 및 등록번호, 사고경위, 사고자 및 관계자의 인적사항, 사고자 및 관계자에 대한 조치결과를 서면으로 제출하여야 함

※ 현 행정공통용 보안시스템은 비밀키 알고리즘 방식으로 전 국가기관이 동일한 보안시스템을 사용함에 따라, 분실등 사고가 발생할 경우 자재 분실시 즉시 배부된 전 국가기관을 대상으로 회수후 폐기처리 되어야 하므로 보관 및 관리에 신중을 기해야 함

Point

• 향후 보안시스템의 제작 방식이 공개키 알고리즘 방식(USB 형태)으로 전환될 경우 분실자재외의 동일 자재는 전 배부처를 대상으로 회수 및 파기하는 불편이 해소될 예정임

⑨ 암호장비 운용 및 관리

< 관 련 법 규 >

- 통신정보및통신보안업무조정규정
- 통신보안장비제작및운용관리지침
- 통신보안장비개발지침
- 국가 정보보안 기본지침

가. 암호장비의 종류

- FAX용 암호기(1호기)
- TTY용 암호기(2호기)
- 유·무선용 비화기(3호기)
- DATA용 암호기(4호기)
- 회로용 암호기(5호기)

나. 암호장비 제작 및 설치

- 암호장비 사용승인
  - 암호장비를 사용할 기관의 장은 사전에 국가정보원장의 승인후 설치

<사용 승인요청시 구비사항>

1. 사용목적
2. 사용기관
3. 암호장비의 종류, 소요량 및 산출근거
4. 관련 정보통신시스템 제원
5. 대상 정보통신망 구성도
6. 보안대책
7. 기타 참고자료

- 암호장비는 지정된 암호장비 제작업체에서 제작하여야 함.
- 암호장비 납품시 비닉부분에 대한 검사 및 암호프로그램 주입 요청 (각급기관→해양부→안기부)
- 비닉부분 검사 및 암호프로그램 주입 실시(국가정보원)
- 암호장비 설치후 30일이내 등록(각급기관→교육부→안기부)

※ 암호장비의 외부에는 일반적인 운용상의 기능, 형식승인번호, 기관번호 및 일련번호를 제외한 어떠한 표지도 할수 없음

※ 암호장비의 고유명칭, 제원, 대상국소 및 수량 등 운용현황이 기록된 문서는 대외비 이상으로 분류하여야 함(자체 지침 제56조제3항)

다. 암호장비 취급관리

- 암호장비의 보관

• 암호기 ⇒ 통제구역 설정(단, 탁상용 비화기는 별도 보안대책 수립시 예외)
• 비화기 ⇒ 통제구역 또는 제한구역 설정
※ 전화용 등은 부득이한 경우 은폐설치
• 미사용 암호장비는 별도 포장후 통제구역내 보호용기에 보관관리

– 암호장비의 운용
• 암호운용 키는 주기적으로 변경하고, 키운용지시는 Ⅱ급비밀로 분류 및 관리
• 암호장비 제원·설비내역 등의 인가자외 공개금지
• 운용교범 등 관련자료의 보관관리 철저
• 암호장비 관리책임자(정·부) 및 운용자 지정
• 암호장비 설치내용 각부서 홍보 및 적극 활용 유도

<관리책임자 및 운용자의 임무>

• 암호장비 비익부호(암호코드) 변경운용
• 암호장비의 수·발 및 관리기록
• 암호장비 운용 및 조작법 숙지
• 암호장비의 일일점검결과 기록유지
• 설치 암호장비의 보안대책 강구 및 보안유지 상태 확인감독
• 암호장비 사고 보고 및 기타 보안장비 관련 일체의 업무
• 암호장비 수발시 보안대책 수립 시행

– 암호장비의 운송
• 암호장비는 암호자재에 준하여 수불 ▶ **인감등록된 자에 한하여 수불**
• 수불시 보안시스템 증명서 사용
• 운송책임자의 타업무 겸무배제 및 목적지 도착 즉시 이상유무 통보
• 운송시 보안대책강구 철저 ▶ **무장경호원 탑승 또는 이에 상응한 경비대책 강구**

♣ 보안장비 운송시 준수사항
• 원거리 운송 ▶ **열차 이용**
• 근거리운송 : 업무용 차량 이용,
• 야간·토요일·공휴일 운송금지
• 보안장비 운송시 유의사항에 대한 사전교육 실시

라. 암호장비의 정비
– 운용기관 : 일반부분
– 제작업체 : 비닉부분
– 경비요원 : 암호자재 취급인가
– 정비장소 : 통제구역으로 설정

– 정비절차 : 운용기관의 장이 별도 절차 명시

<암호장비 정비절차>

가. 1단계 정비(자체정비)

- 전원부 내의 휴즈 불량 및 콘넥터 접속여부
  ※ 전원부 및 비닉부 분리형 장비에 한함
- 각종 외부신호 콘넥터 접속여부

나. 2단계 정비(제작업체 정비)

- 제작업체와 장비 구매계약시 용역 정비계약
- 비상스위치 작동으로 비닉프로그램 소거후 정비업체 의뢰
- 보안시스템 증명서에 의거 관리책임자가 제작업체에 장비 인도
- 정비 완료후 장비 인수시에도 동일

【참조】

비밀등급별 및 통신망별 소통기준

통신망(방식별) / 보안장비 자재별 / 비밀등급별		모사전송	전신타자	전 화	전산망	무선전신
Ⅱ급 비밀	장 비	1호기	2호기	3호기	4호기	
	자 재	암 호	암 호	암 호	암 호	암 호
Ⅲ급 비밀	장 비	1호기	2호기	3호기	4호기	
	자 재	약 호 음 어	약 호 음 어	약 호 음 어	약 호 음 어	약 호 음 어
대 외 비	장 비	1호기	2호기	3호기	4호기	
	자 재	약 호 음 어 약 호	약 호 음 어 약 호	약 호 음 어 약 호	약 호 음 어 약 호	약 호 음 어 약 호
기타 보안을 요하는 주요내용	장 비	1호기	2호기	3호기	4호기	
	자 재	약 호 음 어 약 호	약 호 음 어 약 호	약 호 음 어 약 호	약 호 음 어 약 호	약 호 음 어 약 호

※ 3호기의 경우, 전시 및 긴급사태 발생시에는 음어화하여 Ⅱ급 비밀까지 소통 가능

⑩ 공무원 해외출장시 주의사항

□ 이것만은 꼭 알아두세요!

가. 외국공항 입국하는 순간부터 감시대상

세계 대부분의 정보기관은 자국을 방문하는 주요 인사들을 대상으로 무차별적인 정보수집 활동을 전개하고 있습니다. 입국과 동시에 '나를 감시하는 눈이 있다'는 사실을 항상 명심해야 합니다.

나. 방문국 제공 차량보다는 우리공관 차량 이용

방문국가에서 제공하는 의전용 차량을 이용하면 운전기사가 대화내용을 엿들을 수도 있고, 행선지가 노출될 수 있으며, 차량에 도청장치가 설치되어 있을 수도 있으니 우리 공관차량을 이용하는 것이 보다 안전합니다.

다. 중요 회의자료는 항시 휴대

중요한 문서나 수첩 등은 잠시 자리를 비우는 경우라도 항시 휴대하여야 합니다. 해당국 정보기관 요원이 자료 내용을 보거나 복사할 수도 있다는 사실을 잊지 말아야 하겠습니다.

라. 우리 공관은 안전한 보관창고

숙소나 차량 트렁크는 상대국 정보기관의 주요 타깃이므로 중요서류나 물품 등을 방치해서는 안됩니다. 외출시나 식당 출입시 항시 휴대하거나 꼭 필요한 경우 우리 공관에 맡겨야 합니다.

□ 외국공항 이용시 . . .

가. 방문국 출입국 규정 준수

'규정에 어긋난다'는 핑계로 정밀한 보안검색을 요구하는 경우가 종종 있습니다. 검색의 빌미를 제공하지 않기 위해서는 사전에 해당 국가의 출입국 규정을 꼭 확인해야 합니다.

나. 입국심사부터 말조심

외국공항에 도착한 이후에는 평소처럼 얘기하던 습관을 버리고 말 하나하나에 주의를 기울여야 합니다. 입국심사시에도 불필요하게 방문목적 및 세부일정에 관해 자세히 얘기할 필요가 없습니다.

다. 탁송 물품은 철저히 시건

휴대하지 않고 탁송하는 물품은 반드시 열쇠로 잠그고 보조 자물쇠를 채우는 등 시건장치를 견고히 해야 합니다. 혹시라도 가방을 열어보려는 의도를 아예 갖지 못하도록 해야 합니다.

라. 세관 검색시 반드시 입회

세관 검색대를 통과할 때에도 본인의 짐에서 한시도 눈을 떼지 말아야 합니다. 세관에서 어떤 핑계로 노트북 등을 확인해 본다며 별도의 장소로 가져가는 경우 반드시 따라가서 자료를 무단 복사하지는 않는지 끝까지 확인해야 합니다.

□ 숙소 이용시 . . .

가. 숙소는 대사관 추천호텔 이용

방문국가에서 제공하는 영빈관 등에 투숙하는 것이 대접을 받는 기분이 들 수도 있습니다. 그러나 '24시간 감시당하고 있다'는 사실을 명심해야 합니다. 따라서 공관에서 추천하는 숙소를 이용하는 것이 좋습니다.

나. 실내 대화시에는 커튼을 쳐야

실내에서 대화할 경우 유리창을 통한 레이저도청에 대비하여 커튼을 항시 쳐두는 것이 좋습니다. 또한 커튼을 치게 되면 내부 동향이 노출되는 것을 차단하는 효과도 얻을 수 있습니다.

다. 외출 후 숙소로 돌아왔을 때 한번쯤 의심을

숙소에 들어갈 때도 이상한 점은 없는지 확인해 봐야 합니다. 숙소를 나서기 전 내부를 둘러보고 나중에 돌아왔을 때 변한 것은 없는지, 요청하지 않은 물품이 들어와 있는지 등을 점검해야 합니다.

라. 중요회의는 공관에서

숙소내에서는 업무와 관련된 중요한 대화를 가급적 하지 않는 것이 좋습니다. 긴밀히 협의할 내용이 있을 경우에는 공관 회의실을 이용하도록 합니다.

□ 전화 통화시 . . .

가. 통화는 간단히, 우리만 아는 용어로

암호장비가 없는 일반전화나 휴대폰으로 통화할 경우에는 될 수 있는대로 용건만 간단히 하고, 다른 사람이 들어도 무슨 뜻인지 잘 알지 못하도록 당사자들만 아는 용어를 사용하는 것이 좋습니다.

나. 중요통화시 공관내 비화전화 사용

업무와 관련된 중요한 통화를 해야 할 경우에는 반드시 암호장비가 설치된 공관전화를 이용해야 합니다. 숙소내 전화는 도청될 우려가 많으므로 되도록 사용을 자제해야 합니다.

다. 휴대전화라고 안심은 금물

휴대폰도 도·감청될 수 있다는 사실을 명심해야 합니다. 특히 로밍서비스 이용을 자제하고, 부득이하게 사용시에는 전화번호 및 가입자 인증모듈(SIM) 번호가 노출되지 않도록 유의해야 합니다.

라. 휴대전화 필요시엔 임대폰 사용

휴대전화가 필요하다면 공관에서 현지인 명의로 등록된 휴대폰을 빌려 사용하고 부득이한 경우에는 공중전화나 현지 일회용 선불카드를 구입하여 사용합니다.

□ 노트북 사용시 . . .

가. 패스워드 설정은 기본

부팅·로그인·화면보호기 패스워드 설정은 본인 허락없이 노트북을 사용하는 경우를 막기 위한 최소한의 장치입니다. 패스워드는 영문·숫자 등을 조합하여 8자리 이상으로 설정합니다.

나. 저장할 때는 무조건 암호화

노트북을 인터넷에 연결한 채 중요문서를 작성하거나 하드디스크에 저장해서는 안되며, 저장할 경우에는 반드시 암호를 설정한 상태로 해야 합니다. 또한 호텔 등에서 무선랜을 이용하여 인터넷을 해서도 안되겠습니다.

다. 보안 프로그램은 최신 버전으로

윈도우즈 업데이트를 통해 주기적으로 보안패치을 설치하고 백신 프로그램은 항상 최신 버전으로 유지해야 합니다. 또한 도난이나 분실에 대비하여 '위치추적 프로그램'을 설치해야 합니다.

라. 이메일은 조심 또 조심

출처가 분명하지 않거나 첨부파일이 의심스러운 메일은 해킹프로그램이 자동설치될 우려가 있기 때문에 처음부터 열어보지 말고 삭제하여야 합니다. 또한 중요내용 이메일 소통시 반드시 암호시스템을 이용하도록 하고 분실 등에 대비, 노트북과 암호자재 USB는 별도 보관해야 합니다.

□ 항시 도청 의심을!

가. 중요 대화시에는 TV 또는 음악을

중요내용을 협의할 때에는 TV를 켜고 볼륨을 크게 하거나 음악을 틀도록 합니다. 그래도 안심이 되지 않는다면 종이에 쓰는 방식으로 대화합니다. 물론 쓰고 난 종이는 당연히 폐기해야 합니다.

나. 선물로 받는 물건은 의심의 눈초리로

방문국가 뿐만 아니라 외부로부터 받은 모든 선물은 한번쯤 의심을 가지고 점검해봐야 합니다. 혹시 도청장치가 들어있는 것은 아닌지, 수상한 점은 없는지 꼭 확인해야 합니다.

다. 주변에 대한 일상점검은 기본

숙소내 탁자·액자·화분 등 실내 집기류에 대한 특이한 점은 없는지 살펴봐야 합니다. 또한 벽·바닥·천정 등에 혹시 손상된 부분은 없는지, 도색이 조금 다른 부분은 없는지 점검해 보도록 합니다. 차량·식당 등 내가 다니는 모든 곳이 점검대상입니다.

Point

- 본 내용은 공무원 해외출장시 주의해야 할 사항을 수록한 것으로 대외 반출을 금지하며 관리에 유의하시기 바랍니다.

보안업무 관계 규정

제2편

I 국가정보원 관계 규정

❶ 보안업무규정 및 보안업무규정시행규칙

보 안 업 무 규 정	보안업무규정 시행규칙
	제2장 통신보안
	제45조(음어 및 약호자재의 제작) ····· 118
	제46조(음어자재의 배부·반납등) ····· 118
	제47조(음어자재의 관리) ····· 119
	제48조(음어자재의 보관) ····· 119
	제49조(음어자재의 운용) ····· 119
	제50조(음어자재의 긴급파기) ····· 120
	제51조(음어자재의 사고) ····· 120
	제52조(음어자재의 인계·인수) ····· 121
	제53조(통신보안위규) ····· 121
제3장 신원조사	제3장 신원조사
제31조(신원조사) ····· 122	제54조(조사기관 및 대상) ····· 122
제32조(조사의 실시) ····· 122	
제33조(권한의 위임) ····· 122	
	제55조(요청절차) ····· 123
	제56조(신원조사사항) ····· 123
제34조(조사결과의 처리) ····· 124	제57조(신원조사결과의 처리) ····· 124
	제58조(조회 및 협조) ····· 124
제4장 보안조사	제4장 보안조사

보 안 업 무 규 정	보안업무규정 시행규칙
제정 1970. 5.14 대통령령 제 5004 호 개정 1981.10. 7 대통령령 제10478호 개정 1999. 3.31 대통령령 제16211호 개정 1999.12. 7 대통령령 제16609호 개정 2001.1. 29 대통령령 제17116호 개정 2002. 2. 9 대통령령 제17517호 개정 2006. 2. 8 대통령령 제19321호 개정 2006. 3.29 대통령령 제19431호 개정 2008.12.31 대통령령 제21214호	제정 1964. 6.30 대통령훈령 제 4 호 개정 1969. 5.30 대통령훈령 제 25 호 개정 1974. 1.21 대통령훈령 제 35 호 개정 1981.10 .7 대통령훈령 제 46 호 개정 2005. 6.25 대통령훈령 제149호
제1장 총 칙	제1장 비밀보호
	제1절 총칙
제1조(목적) 이 영은 국가정보원법 제3조제2항의 규정에 의하여 보안업무수행에 필요한 사항을 규정함을 목적으로 한다.<개정 99・3・31>	제1조(목적) 이 규칙은 「보안업무규정」(이하 “규정”이라 한다)의 시행에 관하여 필요한 사항을 규정함을 목적으로 한다.
제2조(정의) 이 영에서 사용되는 용어의 정의는 다음과 같다. 1. “비밀”라 함은 그 내용이 누설되는 경우 국가안전보장에 유해로운 결과를 초래할 우려가 있는 국가 기밀로서 이 영에 의하여 비밀로 분류된 것을 말한다. 2. “각급기관”이라 함은 헌법・정부조직법 기타 법령에 의하여 설치된 국가기관(군기관 및 교육기관을 포함한다)과 지방자치단체 및 공공단체를 말한다. 3. “암호자재”라 함은 통신보안을 위하여 통신문의 내용을 보호할 목적으로 문자・숫자・기호 등의 암호로 만들어진 문서나 기구를 말한다	

보 안 업 무 규 정	보안업무규정 시행규칙
제3조(보안책임) 국가안전보장에 관련되는 인원·문서·자재·시설 및 지역을 관리하는 자와 관계기관의 장은 이에 대한 보안책임을 진다.	
제2장 비밀보호	
제4조(비밀의 구분) 비밀은 그 중요성과 가치의 정도에 따라 다음 각호에 의하여 이를 Ⅰ급비밀·Ⅱ급비밀 및 Ⅲ급비밀로 구분한다. 1. 누설되는 경우 대한민국과 외교관계가 단절되고 전쟁을 유발하며 국가의 방위계획·정보활동 및 국가방위상 필요불가결한 과학과 기술의 개발을 위태롭게 하는 등의 우려가 있는 비밀은 이를 Ⅰ급비밀로 한다. 2. 누설되는 경우 국가안전보장에 막대한 지장을 초래할 우려가 있는 비밀은 이를 Ⅱ급비밀로 한다. 3. 누설되는 경우 국가안전보장에 손해를 끼칠 우려가 있는 비밀은 이를 Ⅲ급비밀로 한다.	
제5조(암호자재의 제작공급 및 반납) ①암호자재는 국가정보원장(이하 "국정원장"이라 한다)이 제작하여 필요한 기관에 공급한다. 다만, 국정원장이 필요하다고 인정할 때에는 암호자재의 사용기관으로 하여금 국정원장이 인가하는 암호체계의 범위안에서 암호자재를 제작하게 할 수 있다. ②사용기간이 만료된 암호자재는 지체없이 그 제작기관의 장에게 반납하여야 한다.	
제6조(비밀의 취급) 비밀은 해당 등급의 비밀취	제1조의2(비밀의 취급) 비밀취급인가권이 있는

보 안 업 무 규 정	보안업무규정 시행규칙
급인가를 받은 자에 한하여 취급할 수 있다.	직위에 임명된 자는 임명됨과 동시에 비밀을 수집·작성·관리·분류(재분류를 포함한다. 이하 같다) 및 수발하는 행위(이하 "비밀의 취급"이라 한다)를 할 수 있다.
제7조(비밀취급인가권자) ①Ⅰ급비밀 및 암호자재취급인가권자는 다음과 같다. 1. 대통령 2. 국무총리 3. 감사원장 3의2. 국가인권위원회위원장 4. 각 부·처의 장 5. 국정원장 6. 삭제 7. 국무총리실장·방송통신위원회위원장·공정거래위원회위원장·금융위원회위원장 및 국민권익위원회위원장 8. 대통령실장 9. 대통령 경호처장 10. 검찰총장 11. 합동참모의장·각군참모총장 및 육군의 1,2,3군 사령관 12. 국방부장관이 지정하는 각군 부대장 ②Ⅱ급 및 Ⅲ급비밀취급 인가권자는 다음과 같다. 1. Ⅰ급비밀취급 인가권자 2. 중앙행정기관인 청의 장 3. 도지사 및 특별자치도지사 4. 도 및 특별자치도 교육감 5. 제1호부터 제4호까지의 사람이 지정한 기관의 장	제2조(비밀취급의 한계) ①비밀취급인가를 받은 자가 취급할 수 있는 비밀의 한계는 관계업무 범위 내에 국한한다. ②비밀취급비인가자(이하 "비인가자"라 한다)가 비밀을 입수하였을 때에는 지체없이 해당 비밀취급인가를 받은 자에게 이를 인도하여야 한다.

보 안 업 무 규 정	보안업무규정 시행규칙
제8조(비밀취급인가 및 해제) ①비밀취급 인가권자는 비밀을 취급 또는 비밀에 접근할 직원에 대하여 해당 등급의 비밀취급을 인가한다. ②비밀취급의 인가는 대상자의 직책에 따라 필요한 최소한의 인원으로 제한하여야 한다. ③비밀취급의 인가를 받은 자가 다음 각호의 1에 해당하는 경우에는 그 취급의 인가를 해제하여야 한다. 1. 고의 또는 중대한 과실로 보안사고를 범하였거나 이 영에 위반하여 보안업무에 지장을 초래한 때 2. 비밀취급이 불필요하게 된 때 ④비밀취급의 인가 및 해제와 인가등급의 변경은 문서로써 하여야 하며, 직원의 인사기록사항에 이를 기록하여야 한다.	제3조(비밀취급인가의 제한) ①비밀취급인가권자는 임무 및 직책상 해당등급의 비밀을 항상 사무적으로 취급하는 자에 한하여 비밀취급을 인가하여야 한다. ②비밀취급인가권자는 소속직원의 인사기록카드에 기록된 비밀취급의 인가 및 해제사유와 임용시의 신원조사회보서에 의하여 새로 신원조사를 행하지 아니하고 비밀취급을 인가할 수 있다. 다만, Ⅰ급비밀취급을 인가할 때에는 새로 신원조사를 실시하여야 한다. ③신원조사결과 국가안전보장상 유해로운 정보가 있음이 확인된 자에 대하여는 비밀취급을 인가할 수 없다. ④비밀취급인가가 해제된 자는 비밀을 취급하는 직책으로부터 해임되어야 한다. 제4조(비밀취급인가의 특례) 비밀취급인가권자는 업무상 조정감독을 받는 기업체나 단체에 대하여 소관비밀을 계속적으로 취급하게 하여야 할 필요가 있을 때에는 해당인원에게 Ⅱ급 이하의 비밀취급을 인가할 수 있다. 다만, 이에 의하여 비밀취급인가를 받은 자는 규정 및 이 규칙이 정하는 바에 따라 비밀을 취급하여야 한다.
제9조(비밀의 분류) ①비밀취급인가를 받은 자는 인가 받은 비밀 및 그 이하등급비밀의 분류권을 가진다. ②동등이상의 비밀취급인가를 받은 자로서 직속 상급직위에 있는 자는 그 하위직위에 있는 자가 분류한 비밀등급을 조정할 수 있다. ③비밀을 생산 또는 관리하는 자는 그 비밀을	제5조(서약) 비밀취급인가를 받은 자는 인가와 동시에 별지 제1호 서식에 의하여 서약을 행하여야 한다. 제6조(비밀취급인가증) ①비밀취급인가를 받은 자에게는 별지 제2호 서식에 의한 비밀취급인가증을 교부하여야 한다.

제2편

보 안 업 무 규 정	보안업무규정 시행규칙
분류 또는 재분류할 책임이 있다.	②제1항의 규정에 의하여 교부한 비밀취급인가증은 인가를 해제한 때에는 이를 회수하여야 한다.
	제2절 비밀의 분류
제10조(분류원칙) ①비밀은 적절히 보호할 수 있는 최저등급으로 분류하되, 과도 또는 과소하게 분류하여서는 아니된다. 다만, 암호자재는 제4조의 규정에 불구하고 Ⅱ급이상으로 분류하여야 한다. ②비밀은 그 자체의 내용과 가치의 정도에 따라 분류하여야 하며, 다른 비밀과 관련하여 분류하여서는 아니된다. ③외국정부 또는 국제기구로부터 접수한 비밀은 그 발행기관이 필요로 하는 정도로 보호할 수 있도록 분류하여야 한다.	제7조(분류금지와 대외비) ①누구든지 행정상의 과오나 업무상의 과실을 은닉할 목적으로 비밀이 아닌 사항을 비밀로 분류할 수 없다. ②비밀의 제목표시에 있어서는 어떤 경우를 막론하고 비밀내용이 포함된 제목은 이를 사용할 수 없다. ③규정 제4조에서 규정한 외에 직무수행상 특별히 보호를 요하는 사항은 이를 “대외비”로 하며, 비밀에 준하여 보관한다. ④대외비 문서에는 다음과 같은 표시를 그 문서의 표면 중앙상단에 적색으로 표시하고 보호기간을 기입한다. 대 외 비 (1cm) 20 . . .까지 (0.5cm) 5cm
제11조(분류지침) 각급기관의 장은 비밀분류의 통일성과 적절한 분류를 위하여 세부분류지침을 작성 시행하여야 한다.	제8조(비밀세부분류지침) ①국가정보원장(이하"국정원장"이라 한다)은 별표 1의 기본분류지침에 따라 각 중앙국가기관의 장이 제출하는 자료에 의하여 비밀세부분류지침을 작성하여 국가기관 기타 관계기관에 배부한다. 다만, 군사비밀 세부분류지침은 별표 1의 기본분류지침에 따라 국방부장관이 따로 작성하여 배부한다

보 안 업 무 규 정	보안업무규정 시행규칙
	②각 중앙국가기관의 장은 비밀세부분류지침을 새로이 작성하거나 변경할 필요가 있다고 인정할 때에는 그 자료를 국정원장에게 제출하여야 한다.
	제3절 예고문 및 재분류
제12조(예고문) 분류된 비밀에는 보호기간을 명시하기 위하여 예고문을 기재하여야 한다.	제9조(예고문) ①모든 비밀에는 다음과 같은 예고문을 기재하여야 한다. 로 재분류, 파기(일자 또는 경우) ②예고문의 재분류일자 또는 경우는 도래가 명확한 것이라야 하며 “처리후”“불필요시” 또는 “참고후”와 같이 불확실한 것을 기재하여서는 아니된다. ③재분류시기를 예측할 수 없는 비밀은 통상 발행일로부터 1년 이내의 일자를 기재한다. ④유첨문서의 본문이 첨부물로 인하여 비밀로 분류되었거나 자체내용보다 상위비밀등급으로 분류되었을 때에는 다음과 같은 예고문을 기입하고 첨부물에는 따로 제1항의 예고문을 기입하여야 한다. 첨부물에서 분리되면 로 재분류 ⑤예고문은 비밀이 문서(책자를 포함한다. 이하 같다)인 때에는 본문 말미여백에 기입한다. 비밀자체에 기입할 수 없는 때에는 비밀관리기록부에 기록하고 이를 발송할 때에는 송증 또는 비밀통고서 말미에 기입한다.
제13조(재분류) ①비밀은 그 효율적인 보호를 위하여 등급의	제10조(재분류검토) ①비밀을 취급하는 자는 계속적으로 소관 비

보 안 업 무 규 정	보안업무규정 시행규칙
변경 또는 파기등의 재분류를 실시한다. ②비밀의 재분류는 그 비밀의 예고문 또는 발행자의 직권에 의하여 실시한다. 다만, 다음 각호의 경우에는 예고문에 불구하고 이를 파기 할 수 있다. 1. 긴급 부득이한 사정으로 비밀을 계속 보관하거나 안전하게 지출 할 수 없을 때 2. 국정원장의 요청이 있을 때 3. 보안유지를 위하여 예고문의 파기시기까지 계속 보관할 필요가 없을 때. 이 경우에는 당해 소속비밀취급인가권자의 사전승인을 얻어야 한다. ③외국정부 또는 국제기구로부터 접수된 비밀중 예고문이 없거나 기재된 예고문이 비밀관리상 부적당하다고 인정되는 것은 접수한 기관의 장이 그 비밀을 최대한으로 보호할 수 있는 범위안에서 재분류할 수 있다. ④비밀을 존안하고자 할 때에는 그 예고문이나 비밀등급을 변경하여서는 아니되며, 존안된 비밀자료는 존안기간중 이를 재분류하지 아니한다. 다만, 일반문서로 재분류하거나 공공기관의기록물관리에관한법률 및 동법시행령이 정하는 바에 따라 기록물전문관리기관의 장이 존안중의 비밀을 재분류하는 때에는 그러하지 아니하다.	밀의 예고문에 의한 재분류 검토를 실시하여야 한다. ②비밀원본에 대하여는 연 2회(6월과 12월) 의무적으로 그 내용에 의한 재분류검토를 실시하여야 하며 원본의 표면의 적당한 여백에 다음과 같은 검토필표지를 하여야 한다. 검 토 필 (. . .) 인 제11조(재분류요청등) ①비밀을 접수한 기관이 그 비밀을 검토한 결과 과도하게 분류되었다고 인정될 때에는 그 사유를 명시하여 발행기관에 대하여 재분류를 요청한다. ②비밀이 과소하게 분류되었다고 인정될 때에는 적절한 상위비밀등급으로 취급 보호한 후 제1항과 같이 요청한다. 비밀로 분류되어야 할 사항이 분류되지 아니한 때에도 또한 같다. ③비밀의 발행기관이 불명하여 제1항 및 제2항의 요청을 할 수 없을 때에는 접수기관의 직권으로 재분류한다. 다만, 1급비밀의 재분류는 국정원장에게 요청하여야 한다. ④타기관으로부터 인수한 비밀원본의 재분류권은 인수한 기관에게 있다. 제12조(예고문의 변경요청) 비밀을 접수한 기관이 비밀의 예고문에 의한 재분류가 업무수행에 지장을 가져온다고 인정할 때에는 그 사유를 명시하여 발행기관에 예고문의 변경을 요청할 수 있다. 제13조(재분류통고)

보 안 업 무 규 정	보안업무규정 시행규칙
	①비밀을 발행한 기관이 그 비밀의 예고문에 명시한 일자 또는 경우의 도래전에 발행자의 직권으로 재분류하였거나 예고문을 변경하였을 때에는 그 비밀이 배포된 모든 기관에 이를 통고하여야 한다. ②동일한 계통의 상급기관 또는 조정감독기관은 하급기관 또는 조정감독을 받는 기관으로부터 접수한 비밀이 과도 또는 과소하게 분류되었다고 인정되는 때에는 발행기관의 의사에 불구하고 재분류할 수 있다. 다만, 재분류하였을 때에는 이를 발행기관에 통고하여야 한다. ③제2항의 규정에 의하여 재분류 통고를 받은 발행기관은 그 비밀에 대한 재분류조치를 취하고 그 비밀이 배포된 모든 기관에 대하여 재분류 통고를 하여야한다.
	제14조(파기) ①비밀의 파기는 소각 용해 또는 기타 방법으로 원형을 완전히 소멸시켜야 한다. ②비밀의 파기는 보관책임자 또는 그가 지정하는 비밀취급인가자의 참여아래 그 비밀의 처리담당자가 행하며, 비밀관리기록부의 파기확인란에 참여자의 파기확인을 받아야 한다.
	제15조(비밀의 원본보관) 비밀의 원본은 그 예고문에 의하여 파기하여야 할 경우에 있어서도 발행자는 그 직권으로 계속 보관할 수 있다.
	제4절 비밀의 표지(標識)
제14조(표지) 비밀은 그 취급자 또는 관리자에게 경고하고 비밀취급인가자의 접근을 방지하기	제16조(문서의 표지(標識) ①비밀문서는 전후면의 표지(表紙)와 매면 상

보 안 업 무 규 정	보안업무규정 시행규칙
위하여 분류(재분류를 포함한다. 이하 같다)와 동시에 등급에 따라 구분된 표지를 하여야 한다.	하단의 중앙에 별지 제3호 서식의 비밀등급표를 등급에 따라 표지한다. ②비밀등급의 표지는 적색으로 함을 원칙으로 하되, 복제 또는 복사하는 때는 복제 또는 복사물과 동일한 색으로 표지할 수 있으며 비밀표지는 복제 또는 복사물의 글자보다 크고 뚜렷하게 하여야 한다. ③단일문서로서 매면마다 비밀등급을 달리하는 때에는 매면별로 해당등급의 비밀표지를 하되 그 표지(表紙)의 양면은 그 중 최고의 비밀등급으로 표지한다. ④비밀등급을 달리하는 수개의 문서를 1건으로 편철한 때의 표지양면의 비밀표지는 그중 최고의 등급으로 한다. ⑤비밀문서는 철하여져 있거나 보관되어 있을 때를 제외하고 별지 제4호 내지 제6호 서식의 비밀표지(表紙)를 해당등급에 따라 첨부하고 취급한다. 제17조(필름 및 사진의 표지) ①1매로 된 필름은 비밀표지가 되어있는 봉투나 이에 준하는 용기에 넣어 보관한다. ②연결되어 있는 영사필름은 처음과 끝에 해당비밀등급을 사입(寫入)하고 제1항과 같이 보관한다. ③인화한 사진은 매표면상하단 및 이면중앙에 적절한 크기의 비밀등급을 표지하고 제1항과 같이 보관한다. 제18조(지도·괘도 등의 표지) 지도·괘도 기타 도안등은 매면 상하단의 중앙에 적절한 크기의 비밀등급을 표지하고 접거나 말았을 때에

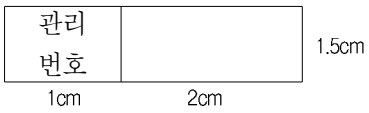
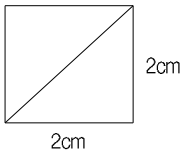
보 안 업 무 규 정	보안업무규정 시행규칙
	도 비밀임을 알 수 있도록 그 이면의 적절한 부위에 표지한다. 제19조(상황판등의 표지) ①고착식 상황판 또는 접거나 말을 수 없는 현황판 등은 제18조와 같이 표지하고 비밀표지를 한 가림막을 쳐야 한다. 다만, 가림막에 비밀표지를 함이 오히려 비밀보호상 불이익하거나 충분히 위장된 때에는 비밀표지를 아니할 수 있다. ②제16조 내지 제19조 및 제1항 이외의 비밀인 자재·생산품 기타 물질은 식별이 용이하도록 적절한 크기로 표지한다. 다만, 비밀등급을 표지(標識)할 수 없을 때에는 문서상으로 그 비밀등급을 통고한다. 제20조(증거물등의 표지(標識)) 수사상의 증거물등과 같이 그 원형을 그대로 보전할 필요가 있는 때에는 그 자체에 비밀등급을 표지(標識)하지 아니하고 표면에 별지 제4호 내지 제6호 서식의 비밀표지(表紙)를 등급에 따라 반영구적으로 첨부하고 취급한다. 제21조(비밀의 녹음 등) 비밀을 녹음할 때에는 처음과 끝에 그 비밀등급과 허가되지 아니한 자에게 전달 또는 누설하는 때에는 관계법규에 의거 처벌한다는 경고를 녹음하고 제17조 제1항과 같이 보관한다. 비밀을 구두로 설명 또는 전달할 때에도 이에 준한다. 제22조(재분류표지(標識)) ①재분류한 비밀은 구표지(舊標識)를 대각선

보 안 업 무 규 정	보안업무규정 시행규칙
	으로 줄을 쳐서 삭제하고 그 측면 또는 상하단의 적당한 여백에 변경된 비밀등급을 재차 표지한다. ②비밀을 재분류한 때에는 재분류근거를 다음 서식에 의하여 그 비밀의 첫면 적당한 여백에 기입하고 날인한다. 직권으로 재분류(. .) 직위 성명 인 (발행처) 에 의거 재분류(. .) 직위 성명 인 (접수처) ③책자, 팜플렛 기타 영구적으로 철하여져 있는 비밀문서를 재분류한 때에는 양면표지(表紙)의 비밀표지만을 제1항과 같이 삭제하고 표지한다. 다만, 매 면별로 재분류한 때에는 그 면마다 제1항 및 제2항에 정하는 절차에 의하여 재차표지를 하여야 한다.
	제23조(면표시) 비밀문서가 두장 이상으로 이루어진 때에는 문서의 중앙하부에 전(全)면수와 그 면의 일련번호를 기입하여야 한다. 첨부문서의 면표시는 위의 요령에 의하여 따로 한다.
	제5절 비밀의 수발
제15조(비밀의 수발) 비밀을 수발함에 있어서는 그 비밀을 최대한으로 보호할 수 있는 방법을 이용하여야 한다.	제24조(비밀의 수발) ①비밀의 수발은 다음 각호에 정하는 절차에 의한다. 다만, 1급비밀 및 암호자재는 제1호 및 제2호의 규정에 의하여서만 수발할 수 있다. 1. 암호화하여 전신으로 수발한다. 2. 취급자의 직접접촉에 의하여 수발한다. 3. 각급기관의 문서수발계통에 의하여 수발한다.
제16조(통신수단에 의한 비밀수발 제한) 비밀은 전신·전화 등의 통신수단에 의하여 평문으로 수발하여서는 아니된다.	

보 안 업 무 규 정	보안업무규정 시행규칙
	4. 등기우편에 의하여 수발한다. ②비밀을 수발할 때에는 별지 제7호 서식에 의한 봉투로 포장하여야 한다. 다만, Ⅲ급 비밀을 등기우편으로 발송할 때에는 Ⅰ급 및 Ⅱ급 비밀에 준하여 2중봉투를 사용하여야 한다. ③문서 이외의 비밀 자재는 내용이 노출되지 아니하도록 이에 준하여 완전히 포장하여야 한다. ④동일기관내에서의 비밀의 수발 또는 전파절차(傳播節次)는 그 기관의 장이 정한다. 다만, 비밀이 충분히 보호될 수 있어야 한다. ⑤다른 기관으로부터 접수한 비밀은 발행기관의 승인없이 재차 다른 기관으로 발송할 수 없다. 다만, 비밀을 이첩 시달하는 경우는 예외로 한다. ⑥비밀수발계통에 종사하는 인원은 Ⅱ급 이상의 비밀취급인가를 받은 자라야 한다.
제17조(영수증) Ⅰ급비밀 및 Ⅱ급비밀을 수발할 때에는 이를 확인하기 위하여 영수증을 사용한다.	제25조(영수증) ①규정 제17조에서 규정한 영수증은 별지 제8호 서식과 같다. ②영수증은 발송문서의 내부봉투와 외부봉투 사이에 삽입하여 발송한다. 다만, 취급자의 직접접촉에 의하는 때에는 직접 교부한다. ③접수기관은 비밀을 접수한 즉시 영수증을 발행기관에 반송(返送)하여야 한다. ④제3항의 영수증을 반송받은 비밀발행기관은 그 영수증을 비밀송증에 원형대로 첨부하여 보관한다.
	제6절 비밀의 보관 및 보안
제18조(보관) 비밀은 도난·화재 또는 파괴로부	제26조(보관기준)

보 안 업 무 규 정	보안업무규정 시행규칙
터 보호하고 비밀취급비인가자의 접근을 방지할 수 있는 적절한 시설에 보관하여야 한다.	①비밀은 일반문서나 자재와 혼합 보관할 수 없다. ②Ⅰ급비밀은 반드시 금고에 보관하여야 하며, 타비밀과 혼합 보관하여서는 아니된다. ③Ⅱ급 및 Ⅲ급비밀은 금고 또는 철제상자나 안전한 용기에 보관하여야 하며, 보관책임자가 Ⅱ급비밀취급인가를 받은 때에는 동일 용기에 혼합 보관할 수 있다. ④보관용기에 넣을 수 없는 비밀은 제한구역 또는 통제구역내에 보관하거나 내용이 노출되지 아니하도록 특별한 보호책을 강구하여야 한다.
제19조(여행중의 비밀보관) 비밀을 휴대하고 출장 또는 여행하는 자는 비밀의 안전한 보호를 위하여 국내경찰기관 또는 국외 주재공관에 위탁 보관할 수 있으며, 위탁받은 기관은 이를 보관하여야 한다.	제27조(보관용기) ①비밀의 보관용기 외부에는 비밀의 보관을 알리거나 나타내는 어떠한 표시도 하여서는 아니된다. ②보관용기의 자물쇠의 종류 및 사용방법은 보관책임자 이외의 인원이 알지 못하도록 특별한 통제를 실시하여야 하며, 타인이 알았을 때에는 즉시 이를 변경하여야 한다.
제20조(보관책임자) 각급기관의 장은 비밀의 보관을 위하여 필요한 인원을 보관책임자로 임명하여야 한다.	제28조(보관책임자) ①보관책임자는 비밀취급인가를 받은 자 중에서 비밀등급별로 임명한다. 다만, 제26조제3항의 경우에는 Ⅲ급 비밀보관책임자를 따로 임명하지 아니한다. ②보관책임자는 보관부서단위로 정책임자 1인을 두고 보관용기의 수 또는 보관 장소에 따라 수인의 부책임자를 둘 수 있다. ③보관책임자는 다음 각호의 임무를 수행한다. 1. 비밀을 최선의 상태로 보관한다.

보 안 업 무 규 정	보안업무규정 시행규칙
	2. 비밀의 누설·도난·분실 및 기타 손괴 등의 방지를 위한 감독을 이행한다. 3. 비밀관리기록부를 비치하고 기록 유지하며 제36조에 의한 비밀 대출부 및 비밀열람기록전(철)의 기록을 확인유지 한다. 제29조(보관책임자의 교체) ①비밀보관정책임자를 교체하는 때에는 소속 보안담당관의 확인하에 인계인수를 하여야 한다. ②제1항의 인계인수는 따로 인계인수서를 작성하지 아니하고 비밀관리기록부에 의할 수 있다.
제21조(비밀관리기록부) ①각급기관의 장은 비밀의 작성·분류·수발 및 취급등에 관한 일체의 관리사항을 기록하기 위하여 비밀관리기록부를 작성·비치하여야 한다. 다만, Ⅰ급비밀관리기록부는 따로 작성·비치하여야 하며, 암호 및 음어자재는 암호자재기록부에 의하여 관리한다. ②비밀관리기록부 및 암호자재기록부에는 모든 비밀과 암호자재에 대한 보안책임 및 보안관리 사항이 정확히 기록·보존되어야 한다.	제30조(비밀관리기록부의 사용방법) ①비밀관리기록부는 별지 제9호 서식에 의하며 문서수발담당부서에서 행하는 비밀의 수발기록은 별지 제10호 서식에 의한다. ②비밀을 재분류 하였거나 다른 곳으로 이송하였을 때에는 관리기록부의 해당란을 2개의 적선으로 삭제한 후 그 사유를 재분류란에 명시한다. 다만, 삭제한 부분은 해득할 수 있도록 자체를 존치(存置)하여야 한다. 제31조(관리번호) ①모든 비밀에는 작성 및 접수되는 순서에 따라 관리번호를 부여하여야 한다. ②자체내에서 작성되는 비밀의 관리번호는 최종결재권자가 재결(裁決)하여 그 내용이 확정된 후에 부여한다. ③관리번호는 다음 규격에 의하여 문서인 때에는 표지(表紙)의 좌측상단에 기입하고 기타

보 안 업 무 규 정	보안업무규정 시행규칙
	도서나 자재 등에는 이에 준하여 식별이 용이하도록 적절한 부위에 기입한다. 
제22조(비밀의 복제·복사의 제한) ①비밀의 일부 또는 전부를 모필·타자·인쇄·조각·녹음·촬영·인화·확대등 비밀의 원형의 재현은 다음 각호의 1에 해당하는 경우를 제외하고는 이를 할 수 없다. 다만, 암호 및 음어자재는 어떠한 경우를 막론하고 복제 또는 복사하지 못한다. 1. Ⅰ급비밀은 그 발행자의 허가를 얻은 때 2. Ⅱ급 및 Ⅲ급비밀은 당해 발행자의 특정한 제한이 없는 것으로서 해당 등급의 비밀취급인가를 받은 자가 공용으로 사용할 때 ②비밀을 복제 또는 복사한 경우에는 그 원본과 동일한 비밀등급과 예고문을 명시하고, 사본 번호를 부여하여야 한다. ③제2항의 예고문의 경우 재분류구분이 “파기”로 되어 있는 때에는 원본의 파기시기보다 그 시기를 줄일 수 있다.	제32조(복제 복사의 제한근거) Ⅱ급 및 Ⅲ급비밀에 대한 복제 복사를 제한하고자 할 때에는 그 비밀의 표지 이면(裏面) 또는 예고문 상단에 다음과 같이 적색으로 기입한다. 이 비밀의 는 발행자의 허가없이 복제 복사할 수 없음 제33조(사본번호) 비밀의 사본번호는 전(全)사본 부수에 대한 개개(個個)에게 일련번호를 부여하며 다음 규격에 의하여 비밀의 표면 우측상단에 기입한다.  제34조(사본근거 표지(標識)) ①복제 또는 복사한 비밀원본의 말미에는 사본번호를 포함한 배포선을 작성 첨부하여야 한다. ②비밀을 접수한 기관이 접수비밀을 복제 또는 복사한 때에는 그 비밀의 첫면 또는 말미 중 적절한 여백에 사본근거를 다음과 같이 기입하여야 한다.

보 안 업 무 규 정	보안업무규정 시행규칙
	사본일자 ㊞ 성명 사본일수 면부터 면까지 매 부 사본의처리
	제35조(비밀문서의 분리) 단일 문서로 된 비밀은 이를 분리할 수 없다. 다만, Ⅲ급비밀인 첩보 및 정보문서는 이의 신속한 처리를 위하여 관계취급자에게 분리취급시킬 수 있으며 업무처리가 끝난 후에는 반드시 그 예고문에 의하여 종합처리 하여야 한다.
제23조(비밀의 열람) ①비밀은 해당 등급의 비밀취급인가를 받은 자로서 그 비밀과 업무상 직접 관계가 있는 자에 한하여 열람할 수 있다. ②비밀취급 비인가자에게 비밀을 열람·공개 또는 취급하게 할 때에는 미리 국정원장의 보안조치를 받아야 한다. 다만, 비밀이 군사에 관한 사항인 경우에는 국방부장관의 보안조치를 받아야 한다.	제36조(비밀의 대출 및 열람) ①비밀보관책임자는 보관비밀을 대출하는 때에는 별지 제11호 서식에 의한 비밀대출부에 소요사항을 기록 유지한다. ②개개 비밀에 대한 열람자 범위를 파악하기 위하여 각개의 비밀문서 말미에 별지 제12호 서식의 비밀열람기록전(秘密閱覽記錄箋)을 첨부한다. 문서 이외의 비밀자재에 대한 열람기록은 따로 비밀열람기록전철을 비치하고 기록 유지 한다. ③제2항의 비밀열람기록전은 그 비밀의 발행기관이 첨부하며, 그 비밀을 파기하는 때에는 그 비밀에서 분리하여 따로 철하여 보관하여야 한다. ④모든 비밀열람자는 비밀을 열람하기에 앞서 비밀열람기록 전에 소정의 사항을 기재하고 서명 또는 날인한 후 비밀을 열람하여야 한다. ⑤타자, 필경 또는 발간업무에 종사하는 자는 비밀열람기록전에 갈음하는 작업일지에 작업내용을 기록 유지하여야 한다.
제24조(비밀의 공개) 공무원 또는 공무원이었던 자는 법률이 정하는 경우를 제외하고는 소속 또는 소속되었던 기관의 장의 승인없이 비밀을 공개하지 못한다.	

보 안 업 무 규 정	보안업무규정 시행규칙
	제37조(보안조치) ①규정 제23조제2항의 규정에 의하여 비인가자에게 비밀을 열람·공개 또는 취급하게 할 때에는 20일전에 다음 사항을 국정원장(비밀이 군사에 관한 사항인 경우에는 국방부장관)에게 통보하여야 한다. 다만, 긴급을 요할 때에는 3일전에 통보할 수 있다. 1. 비인가자의 인적사항 성 명 본적 및 주소(외국인인 때에는 국적) 생년월일 및 성별 직업 2. 비밀의 내용(개요) 3. 이 유 4. 기 간 5. 장 소 6. 자체보안책 7. 기타 참고사항 ②민간시설을 이용하여 비밀을 인쇄, 발간 또는 제작하거나 복제, 복사하고자 할 때에는 20일전까지 다음 사항을 국정원장(비밀이 군사에 관한 사항인 경우에는 국방부장관)에게 통고하여야 한다 1. 민간시설의 명칭, 위치 및 대표자 성명 2. 비밀의 내용(개요) 3. 이 유 4. 기 간 5. 자체보안책 6. 기타 참고사항 ③민간시설을 이용하여 비밀 또는 대외비 문서를 발간하였을 때에는 그 문서의 말미 또는 후면표지 이면에 다음과 같은 표시를 하여

보 안 업 무 규 정	보안업무규정 시행규칙
	야 한다. <table><tr><td colspan="3">서기 년 월 일 발간</td></tr><tr><td colspan="3">발간업체명 전화 ( )</td></tr><tr><td colspan="3">대 표 자</td></tr><tr><td colspan="3">인 가 근 거</td></tr><tr><td rowspan="2">참 여 자</td><td colspan="2">소 속</td></tr><tr><td colspan="2">성 명</td></tr></table> 6cm 10cm 인가근거 : 조달청의 비밀취급인가 근거와 년 월 일 (예 : 내자 126-383, 1968. 4. 5)
제25조(비밀의 지출) 비밀은 보관하고 있는 시설 밖으로 지출하여서는 아니된다. 다만, 공무상 지출이 필요할 때에는 그 소속기관의 장의 승인을 얻어 지출할 수 있다.	제38조(비밀의 지출) ①규정 제25조에 의한 비밀을 지출하고자 할 때에는 별지 제13호 서식에 의하여 소속기관장의 승인서를 그 보관책임자에게 제출하여야 한다. ②각급 기관의 장은 지출후의 보안대책을 확인하지 아니하고는 비밀지출을 승인할 수 없다 제39조(비밀의 인계) ①비밀을 보관하는 기관이 해체되는 때에는 소유비밀을 인수기관에 인계하여야 한다. ②비밀의 인수기관이 없거나 불명한 때에는 접수비밀은 발행기관에 반납하고 자체 내에서 작성된 비밀은 이를 파기한다. 다만, 파기하였을 때에는 그 비밀의 목록과 파기사유를 국정원장에게 통보하여야 한다.
제26조(안전지출 및 파기계획) 각급 기관의 장은	제40조(안전지출 및 파기계획) 안전지출 및 파기

보 안 업 무 규 정	보안업무규정 시행규칙
비상시에 대비하여 비밀을 안전하게 지출 또는 파기할 수 있는 계획을 수립하고 소속직원에게 주지시켜야 한다. 제27조(비밀문서의 통제) 각급기관의 장은 비밀문서의 통제를 위한 규정을 따로 작성·운영할 수 있다. 제28조(비밀의 이관) 비밀은 일반문서보관소에 이관하여서는 아니된다. 다만, 공공기관의 기록물관리에관한법률 및 동법시행령이 정하는 바에 따라 비밀원본을 기록물전문관리기관에 이관하는 경우에는 그러하지 아니하다. 제29조(비밀소유현황통보) 각급기관의 장은 연 2회 비밀소유현황을 조사하여 국정원장에게 통보하여야 한다. 제30조(보호구역) ①각급기관의 장과 국가중요시설·장비 및 자재를 관리하는 자는 국가비밀의 보호와 국가중요시설장비 및 자재의 보호를 위하여 필요한 장소에 일정한 범위를 정하여 보호구역을 설정할 수 있다. ②제1항의 보호구역은 그 중요도에 따라 이를 제한지역, 제한구역 및 통제구역으로 나눈다. ③보호구역 설정자는 제1항의 보호구역에 보	계획은 각급 기관의 지역적 특수성을 고려하여 일정에 부합하도록 작성하여야 하며 다음 사항이 포함되어야 한다. 1. 목 적 2. 적용범위 3. 지출 또는 파기의 시기(상황) 4. 시행책임(일과중 또는 일과후로 구분하고 일과후는 다시 야간·공휴일 등으로 구분한다) 5. 지출 또는 파기의 절차 및 장소 6. 최종 확인 및 보고 7. 행정사항(열쇠관리·계획서의 비치등) 제41조(비밀소유현황 및 비밀취급인가자 현황조사의 절차 및 통보) ①각급기관의 장은 비밀의 재분류검토를 실시한 후 별지 제14호 서식에 의하여 매년 6월과 12월 말일을 기준하여 비밀의 소유현황 및 비밀취급인가자 현황을 조사하여야 한다. ②중앙행정관서의 장은 소속기관의 비밀소유현황 및 비밀취급인가자 현황을 종합하여 조사기준 익월 25일까지 안전기획부장에게 통보하여야한다. 제42조(보호구역) ①규정 제30조의 “제한지역”이라 함은 비밀 또는 정부재산의 보호를 위하여 울타리 또는 경호원에 의하여 일반인의 출입의 감시가 요구되는 지역을 말한다. ②규정 제30조의 “제한구역”이라 함은 비밀 또는 주요시설 및 자재에 대한 비인가자의 접근을 방지하기 위하여 그 출입에 안내가 요구되는 구역을 말한다.

보 안 업 무 규 정	보안업무규정 시행규칙
안상 불필요한 인원의 접근 또는 출입을 제한하거나 금지시킬 수 있다.	③규정 제30조의 "통제구역"이라 함은 비인가자의 출입이 금지되는 보안상 극히 중요한 구역을 말한다. ④보호구역에 대하여는 철저한 보안대책을 수립, 이행하여야 하며, 특히 제한구역 및 통제구역에는 그 구역의 기능 및 구조에 따라 다음과 같은 대책이 강구되어야 한다. 1. 출입인가자의 한계설정과 비인가자의 출입통제책 2. 주야경계대책 3. 외부로부터의 투시, 도청 및 파괴물질의 투척방지 대책 4. 방화대책 5. 경보대책 6. 기타 필요한 보안대책 제43조(보호구역의 설정방침) 제한구역 및 통제구역의 설정은 필요한 최소한의 범위로 제한되어야 한다. 제44조(보호구역의 설정대상) 규정 제30조에 정하는 보호구역으로 설정이 가능한 일반적 대상은 다음과 같다. 1. 종합비밀보관소 2. 암호취급소 3. 비밀상황실 4. 정보존안실(情報存案室) 5. 정보공작실 6. 전파관리소 7. 군항 및 항공기지 8. 군사요새지 9. 탄약고지대

보 안 업 무 규 정	보안업무규정 시행규칙
	10. 기타 보안상 특별한 통제가 요구되는 지역 또는 시설
	제2장 통신보안
	제45조(음어 및 약호자재의 제작) ①각 기관에서 공통으로 사용할 음어자재는 국가정보원장이 제작·배부한다. ②각 기관의 자체용 음어자재는 국정원장의 인가를 받아 그 기관의 장이 제작·배부한다. ③음어자재는 Ⅲ급비밀로 분류하며, 약호자재는 대외비 이상으로 분류하여야 한다. ④각 기관의 자체용 음어자재는 제작 또는 변경될 때마다 그 1부를 국정원장에게 제출하여야 한다. ⑤모든 음어자재(약호자재를 포함한다. 이하 같다)의 관리에 관하여는 제작기관의 장이 책임을 진다. ⑥전파관리국장은 약호자재가 제작되거나 변경될 때마다 그 1부를 국정원장에게 제출하여야 한다.
	제46조(음어자재의 배부·반납등) ①음어자재를 배부하는 기관은 별지 제15호서식에 의한 인감등록대장을 비치하고 인감등록이 되어 있는 자에 한하여 배부한다. 반납을 받는 경우에도 또한 같다. ②각 기관은 항시 예비용 음어자재를 최하단위 사용기관까지 48시간내에 배부할 수 있는 조치를 취하여야 한다. ③모든 기관은 사용기간이 만료된 음어자재를 지체없이 배부기관에 반납하여야 한다.

보 안 업 무 규 정	보안업무규정 시행규칙
	④음어자재의 배부, 반납, 파기 또는 오인 소각이나 분실 기타 사고의 증명은 별지 제16호 서식에 의한다. 제47조(음어자재의 관리) 음어자재를 보유하고 있는 모든 기관은 별지 제17호 서식에 의한 음어자재기록부를 비치하고 기록·유치하여야 한다. 제48조(음어자재의 보관) ①음어자재는 과거용·현재용 및 미래용으로 구분하여 보관하되 현재용을 제외하고는 이를 포장한 후 봉인하여 보관하여야 한다. ②음어자재는 비밀보관용기에 보관하되, 음어자재 보관함을 따로 비치하여야 하며, 그 함에는 음어자재 이외의 다른 물건을 보관하지 못한다. ③음어자재를 보유하고 있는 기관은 별지 제18호 서식에 의한 음어자재 점검기록부를 비치하고 주 1회 이상 점검하여야 하며 보안담당관은 월 1회 점검사항을 확인하여야 한다. 제49조(음어자재의 운용) ①삭제 ②Ⅱ급비밀 이상의 내용은 음어화하여 수발하지 못한다. 다만, 연습의 경우에는 그러하지 아니하다. ③Ⅲ급비밀, 대외비 또는 비밀이 아니라도 누설될 경우 국가이익을 해할 우려가 있는 내용은 음어화하여 수발하여야 한다. 다만, 인가된 암호기 또는 비화기를 설치한 때에는 승인된 범위안에서 평문으로 수발할 수 있다. ④현재용 및 미래용 음어자재는 교육목적으로 사용하지 못한다.

보 안 업 무 규 정	보안업무규정 시행규칙
	⑤음어문을 작성 또는 해독하기 위하여 사용한 작업용지는 그 유효성이 종료된 때에 파기하여야 하며 통신문 여백에 음어자재사용근거를 표시하여야 한다. ⑥통신문을 음어화할 때에는 평문과 혼합하여 사용할 수 없다. 제50조(음어자재의 긴급파기) ①음어자재를 직접 관리하는 자 또는 전송업무를 담당하는 자는 긴급사태의 발생으로 음어자재를 안전하게 보호할 수 없는 경우에는 긴급파기를 할 수 있다. ②음어자재의 긴급파기 계획은 평상시에 이를 수립하여야 하며 파기는 다음 순서에 따라 행하여야 한다. 1. 긴급사태가 발생하였다고 인정될 때에는 과거용부터 파기하며 상황이 더욱 악화되었을 때에는 미래용을 파기한다. 2. 현재용 음어자재를 계속 보유할 수 없을 때에는 배부처가 많은 것부터 차례로 파기하여야 한다. ③음어자재를 긴급 파기하였을 때에는 다음 사항을 소속중앙국가기관의 장을 거쳐 국정원장에게 통보하여야 하며 소속기관의 장은 그 산하기관에 그 사실을 통보하여야 한다. 1. 파기일시 및 장소 2. 음어자재의 명칭·수량 및 등록번호 3. 파기이유 및 방법 4. 현 보유 음어자재의 명칭 5. 파기자 및 참여자의 관직·성명 제51조(음어자재의 사고)

보 안 업 무 규 정	보안업무규정 시행규칙
	①각 기관의 장은 음어자재를 오인소각·소실·분실 또는 누설하였을 때에는 지체없이 소속중앙국가기관의 장을 거쳐 국정원장에게 미리 전통으로 통보하고 다음 사항을 서면으로 제출하여야 한다. 1. 사고일시 및 장소 2. 음어자재의 명칭·수량 및 등록번호 3. 사고경위 4. 사고자 및 관계자의 인적사항 5. 사고자 및 관계자에 대한 조치결과 ②국정원장은 음어자재가 분실 또는 누설되었을 때에는 해당 음어자재의 즉각적인 사용중지와 예비 음어자재의 사용지시를 하여야 하며 해당 음어자재를 회수하고 분실 또는 누설의 경위를 조사하여야 한다. ③음어자재의 분실 또는 누설의 통보를 받은 각 기관의 보안담당관은 그 음어자재로 송수신된 전문을 검토하고 현행 또는 장차의 계획에 영향을 미칠 수 있는 전문을 발췌하여 소속기관의 장에게 제출하고 필요한 조치를 취할 수 있도록 하여야 한다. 제52조(음어자재의 인계·인수) 음어자재 보관책임자가 교체될 때에는 음어자재 기록부에 그 내용을 기록하여야 하며 보안담당관의 확인을 받아야 한다. 제53조(통신보안위규) ①통신보안위규 사항은 별표 2와 같다. ②통신보안기관의 장은 통신보안위규 사항을 적발한 때에는 통신운용기관의 장에게 통고하여야 한다.

보 안 업 무 규 정	보안업무규정 시행규칙
	③통신운용기관의 장은 제2항의 통고를 받은 때에는 지체없이 시정조치하고 그 결과를 관계 통신보안기관의 장에게 회보하여야 한다.
제3장 신원조사	제3장 신원조사
제31조(신원조사) ①국가보안을 위하여 국가에 대한 충성심·성실성 및 신뢰성을 조사하기 위하여 신원조사를 행한다. ②신원조사의 대상이 되는 자는 다음과 같다. 1. 공무원임용예정자 2. 비밀취급인가예정자 3. 해외여행을 하고자 하는 자 (입국하는 교포를 포함한다) 4. 국가중요시설·장비 및 자재등의 관리자와 기타 각급기관의 장이 국가보안상 필요하다고 인정하는 자 5. 공공단체의 직원과 임원의 임명에 있어서 정부의 승인이나 동의를 요하는 법인의 임원 및 직원 6. 기타 법령이 정하는 자	제54조(조사기관 및 대상) ①국정원장은 다음 각호에 해당하는 자에 대한 신원조사를 실시한다. 1. 중앙행정기관의 3급이상 공무원 및 동등한 공무원 임용예정자 2. 서울특별시·광역시의 행정부시장 및 각도의 행정부지사 3. 판사 신규임용예정자 4. 검사 신규임용예정자 5. 국·공립대학교 총장 및 학장 6. 외국인으로서 공무원 임용예정자 7. 그밖에 제1호 내지 제6호 외의 자로서 각급기관의 장이 국가보안상 필요하다고 인정하여 요청하는 자 ②국방부장관은 군인, 군무원, 「방위산업에 관한 특별조치법」에 의한 방위산업체 및 연구기관의 종사자와 기타 군사보안에 관련된 인원에 대한 신원조사를 실시한다. ③경찰청장은 제1항 각호 및 제2항의 규정에 의한 자 외의 자에 대한 신원조사를 실시하되, 여권발급신청자중 신원특이사항이 있는 경우에는 그 신원조사서와 신원조사 월별통계를 국정원장에게 통보하여야 한다. ④국정원장은 제1항 내지 제3항의 규정에 불구하고 필요한 인원에 대한 신원조사를 관계
제32조(조사의 실시) 신원조사는 국정원장이 그 직권 또는 관계기관의 장의 요청에 의하여 이를 실시한다.	
제33조(권한의 위임) 국정원장은 신원조사에 관한 권한의 일부를 국방부장관과 경찰청장에게 위임할 수 있다. 다만, 국방부장관에 대한 위임은 군인·군무원·「방위사업법」에 규정된	

보 안 업 무 규 정	보안업무규정 시행규칙
방위산업체 및 연구기관의 종사자와 기타 군사보안에 관련된 인원의 신원조사의 경우에 한한다.	조사기관에 요청할 수 있다. 제55조(요청절차) 신원조사는 다음 사항을 첨부하여 요청하여야 한다. 1. 대상자명단(별지 제19호 서식) 2. 신원진술서 2부(별지 제20호 서식) 3. 최근 3개월내에 촬영한 상반신 반명함판 사진 2매 4. 호적등본 1부<신설 05. 6. 25.> 5. 외국인의 경우 자기소개서(별지 제21호 서식), 여권사본, 자국 공안기관발행 범죄기록증명원, 외국인등록사실증명원(국내 등록시) 각1부 및 사진 2매<신설 05.6.25> 제56조(신원조사사항) 신원조사사항에는 다음 각호의 사항이 포함되어야 한다. 1. 성명·주민등록번호 2. 본적, 주소 3. 호주 및 본인과의 관계 4. 삭제<05.6.25> 5. 보증인 6. 교우관계 7. 정당, 사회단체 관계 8. 삭제<05.6.25> 9. 학력 및 경력 10. 가족관계 11. 재산관계 12. 상벌관계 13. 인품 및 소행 14. 병역관계 15. 해외거주사실

보 안 업 무 규 정	보안업무규정 시행규칙
	16. 기타 참고사항
제34조(조사결과의 처리) ①각 조사기관의 장은 신원조사의 결과 국가안전보장상 유해로운 정보가 있음이 확인된 자에 대하여는 관계기관의 장에게 그 사실을 통보하여야 한다. ②제1항의 통보를 받은 관계기관의 장은 신원조사의 결과에 따라 필요한 보안대책을 강구하여야 한다.	제57조(신원조사결과의 처리) ①신원조사의 요청을 받은 기관의 장은 조사결과를 별지 제22호 서식에 의한 신원조사회보서 또는 별지 제23호 서식에 의한 신원조사회보서에 의하여 요청기관에 회보하여야 하며 특별한 사유가 없는 한 요청을 받은 날로부터 30일을 초과할 수 없다.<개정 05.6.25> ②삭제 < 05.6.25 > ③각급기관의 장은 신원조사결과 국가보안상 유해로운 사항이 발견된 자를 중요 보직에 임용하고자 하는 경우에는 사전에 필요한 보안대책을 강구하여야 한다. 개정 < 05. 6. 25 >
	제58조(조회 및 협조) ①각급 조사기관은 신원조사를 위하여 필요한 범위내에서 관계기관에 조회 또는 협조를 요청할 수 있다. ②제1항의 요청을 받은 관계기관은 정당한 사유없이 이를 거부할 수 없다.
제4장 보안조사	제4장 보안조사
제35조(보안측정) 국정원장은 국가보안에 관련된 시설·자재 또는 지역을 파괴·태업 또는 비밀누설로부터 보호하기 위하여 보안측정을 실시한다.	
제36조(측정대상) 보안측정은 파괴·태업 또는 비밀누설로 인하여 전략적 또는 군사적으로	제59조(보안측정의 대상) 보안측정의 일반적인 대상은 다음과 같다.

보 안 업 무 규 정	보안업무규정 시행규칙
막대한 손해를 초래하거나 국가안전보장에 연쇄적 혼란을 초래할 우려가 있는 시설 또는 지역(이하 "보안목표시설"이라 한다)과 선박, 항공기 등 중요장비(이하 "보호장비"라 한다)에 대하여 실시한다. 제37조(측정의 실시) ①보안측정은 국정원장이 그 직권으로 실시하는 경우를 제외하고는 보안목표시설 및 보호장비의 관리자 또는 관계감독기관의 장의 요청에 따라 이를 실시한다. ②보안목표시설 및 보호장비의 관리자와 그 감독기관의 장은 국정원장이 그 시설 및 장비의 보호를 위하여 요구하는 보안대책을 성실히 이행하여야 한다. ③국정원장은 관계기관에 대하여 보안측정상 필요한 협조를 요구할 수 있다.	1. 전기시설(발전 및 변전시설) 2. 전신, 전화, 전파시설 3. 주요교통시설 4. 비행장 및 항만시설 5. 수원지 6. 방송시설 7. 과학시설 8. 군수산업시설 9. 국가기간산업시설 10. 기타 국가안전보장상 주요한 지역 및 시설 제60조(보안측정의 요청) ①보안측정을 요청할 경우는 다음과 같다. 1. 보안측정을 실시한 일이 없을 때 2. 삭제 3. 시설을 개수 또는 증축하였거나 보안사고가 빈번하여 새로운 보안대책이 요구될 때 4. 기타 필요하다고 인정할 때 ②보안측정을 요청할 때에는 다음 사항을 첨부하여야 한다. 1. 명칭, 소재지 및 대표자 성명 2. 연 혁 3. 임무기능 및 능력 4. 비밀소유현황 5. 시설의 평면도 6. 관할경찰서 및 소방서 7. 보안사고의 유무 8. 측정이유 9. 기타 참고사항
제38조(전말조사) 국정원장은 비밀의 누설 또는 분실과 국가 중요시설 및 장비의 파괴, 보호	제61조(측정결과에 대한 조치) 보안측정을 행한 기관의 장은 측정결과에 의하여 소요보안대책

보 안 업 무 규 정	보안업무규정 시행규칙
구역에 대한 불법침입 등 보안사고에 대하여 전말조사를 실시한다.	을 수립 이행하여야 한다. 제62조(보안사고의 통보) ①보안사고가 발생한 기관의 장 또는 사고를 범하였거나 이를 인지한 자는 지체없이 사고의 일시·장소·사고내용 및 현재 취하고 있는 조치를 다음 기관에 통보하여야 하며 제2호에 정하는 기관이 보안사고의 통보를 받았을 때에는 즉시 국정원장에게 이를 통보하여야 한다. 1. 국가정보원 2. 인근 경찰기관 또는 군보안기관 3. 비밀발행기관 및 제(諸)배포선 ②보안사고는 이에 대한 전말조사가 종결될 때까지 공개하여서는 아니된다.
제39조(보안감사) 이 영에서 정한 인원·문서·자재·시설·지역 및 장비 등의 모든 보안관리상태와 그 적정여부를 조사하기 위하여 중앙행정기관의 장은 보안감사를 실시한다. 제40조(통신보안감사) 통신수단에 의한 비밀의 누설방지와 모든 통신시설의 보안상태를 조사하기 위하여 중앙행정기관의 장은 통신보안감사를 실시한다.	제63조(조치) 국정원장은 보안사고의 전말 조사 결과에 의하여 비밀의 효력의 정지 또는 취소 등의 필요한 조치를 취한다.
제41조(감사의 실시) ①보안감사 및 통신보안감사는 정기감사와 수시감사로 구분하여 실시한다. ②정기감사는 연 1회, 수시감사는 필요에 따라 수시로 이를 실시한다. ③보안감사 및 통신보안감사를 실시함에 있어	제64조(감사의 실시) ①보안감사 및 통신보안감사는 미리 그 계획을 대상기관에 통보하여야 한다. 다만, 수시감사는 계획의 통보 없이 실시할 수 있다. ②감사관은 감사에 필요한 관계기관의 증언 또는 필요한 서류의 제시를 요구할 수 있다.

보 안 업 무 규 정	보안업무규정 시행규칙
서는 정책자료의 발굴에 중점을 둔다.	③국정원장은 국방부본부를 제외한 합동참모본부, 국방부직할부대 및 기관, 각군, 「방위산업에 관한 특별조치법」에 의한 방위산업체 및 연구기관 기타 군사보안대상에 대한 감사업무를 국방부장관에게 위임한다. 다만, 군공작사항에 대하여는 국정원장이 감사한다. ④국방부장관은 제3항 본문의 규정에 의하여 감사를 실시한 때에는 국정원장에게 그 결과를 통보하여야 한다.
제42조(조사결과의 처리) ①중앙행정기관의 장은 보안감사 및 통신보안감사의 결과를 국정원장에게 통보한다. ②국정원장은 보안조사의 결과를 해당기관의 장에게 통보한다. ③제2항의 규정에 의하여 조사결과를 통보받은 기관의 장은 조사결과에 대하여 필요한 조치를 하여야 한다.	제65조(감사결과의 처리) ①국정원장 또는 국방부장관은 감사의 결과를 대통령에게 서면보고하고 대통령의 재가를 받아 피감사기관에 이를 통보한다. ②제1항의 통보는 감사의 결과보고가 보안제도의 변경을 가져오는 사항이 없는 것에 한하여 국정원장 또는 국방부장관이 전결할 수 있다.
제43조(권한의 위임) ①국정원장은 필요하다고 인정할 때에는 관계기관의 장에게 보안조사에 관한 권한의 일부를 위임할 수 있다. 다만, 국방부장관에 대한 위임은 국방부 본부를 제외한 합동참모본부, 국방부 직할부대 및 기관, 각군, 「방위사업법」에 규정된 방위산업체 및 연구기관 기타 군사보안대상의 보안조사의 경우에 한한다. ②국정원장은 필요하다고 인정할 때에는 제1항의 규정에 의하여 권한을 위임받은 관계기관의 장에 대하여 조사결과의 통보를 요구할 수 있다.	

보 안 업 무 규 정	보안업무규정 시행규칙
제5장 보칙	제5장 보칙
제44조(보안담당관) 각급기관의 장은 이 영에 의한 보안업무를 담당하게 하기 위하여 소속직원 중에서 보안담당관을 임명하여야 한다.	제66조(보안담당관의 임무) 보안담당관은 다음 각 호에 정하는 임무를 수행한다. 1. 자체보안업무수행에 관한 계획조정 및 감독 2. 보안교육 3. 비밀소유현황조사 4. 서약의 집행 5. 통신보안에 관한 업무
제45조(계엄지역의 보안) ①계엄이 선포된 지역의 보안을 위하여 계엄사령관은 이 영의 규정에 불구하고 특별한 보안조치를 할 수 있다. ②제1항의 경우에 계엄사령관은 평상시의 보안업무와의 연계성을 고려하여 필요하다고 인정할 때에는 미리 국정원장과 협의한다.	
	제67조(보안교육) ①다음 각 호에 해당하는 자에 대하여는 관계기관의 장이 사전에 충분한 보안교육과 보안조치를 행하여야 한다. 1. 신규 채용직원 2. 비밀취급인가 예정자 3. 공무, 학술, 체육, 문화, 시찰, 유학 또는 취업 등을 목적으로 하는 해외여행자 ②관계 각급 교육기관의 장은 비밀교재 및 비밀교육 내용을 기록한 피교육자의 필기장 등에 대한 보안유지책을 강구 이행하여야 한다.
	제68조(비밀 관리부철의 보존) 다음 각호의 부철

보 안 업 무 규 정	보안업무규정 시행규칙
	(簿綴)은 5년간 보존하여야 하며 그 이전에 폐기하고자 할 때에는 국정원의 승인을 받아야 한다. 1. 서약서철 2. 비밀영수증철 3. 비밀관리기록부 4. 비밀수발대장 5. 비밀열람기록전(철) 6. 비밀대출부 제69조(위임규정) ①국방부본부, 합동참모본부, 국방부 직할부대 및 기관, 각군, 「방위산업에 관한 특별조치법」에 의한 방위산업체 및 연구기관의 보안에 관한 사항은 이 규칙에 준용하여 국방부장관이 따로 정한다. 다만, 미리 국정원장의 조정을 받아야 한다. ②중앙행정기관의 장은 이 규칙에 저촉되지 아니하는 범위 내에서 이 규칙 운용에 필요한 세칙을 작성 운용하여야 한다.
부 칙 < 제5004호, 1970. 5. 14. >	부 칙 < 제4호, 1964. 6. 30. >
①(시행일) 이 영은 공포한 날로부터 시행한다. ②(경과조치) 이 영 시행전에 분류된 비밀은 이 영에 의하여 분류된 것으로 본다. ③(경과조치) 이 영 시행전에 비밀취급인가를 받은 자는 이 영에 의하 여 비밀취급인가를 받은 것으로 본다.	이 규칙은 1964년 6월 30일부터 시행한다.
	부 칙 < 제25호, 1969. 5. 30. >
	이 규칙은 1969년 6월 1일부터 시행한다.
부 칙 < 제10478호, 1981. 10. 7. >	부 칙 < 제35호 , 1974. 1. 21. >
	이 규칙은 1974년 1월 21일부터 시행한다.

보 안 업 무 규 정	보안업무규정 시행규칙
이 영은 공포한 날로부터 시행한다. 부 칙 < 제16211호, 1999. 3. 31. > 이 영은 공포한 날로부터 시행한다. 부 칙 < 제16609호, 1999. 12. 7. > 이 영은 2000년 1월 1일부터 시행한다. 부 칙 < 제17116호, 2001. 1. 29. > 이 영은 공포한 날부터 시행한다. 부 칙 < 제17517호, 2002. 2. 9. > 이 영은 공포한 날부터 시행한다. 부 칙 < 제19321호, 2006. 2. 8. > 이 영은 공포한 날부터 시행한다. 부 칙 < 제19431호, 2006. 3. 29. > 이 영은 2006년 3월 30일부터 시행한다.	부 칙 < 제46호, 1981. 10. 7. > 이 규칙은 발령한 날로부터 시행한다. 부 칙 < 제149호, 2005. 6. 25. > 이 훈령은 발령한 날부터 시행한다.

[별표 1]

기 본 분 류 지 침 표

Ⅰ 급 비 밀	Ⅱ 급 비 밀	Ⅲ 급 비 밀
1. 국가방위 및 외교에 결정적인 영향을 주는 사항	1. 국가방위에 중요한 손해를 초래할 우려가 있는 사항 가. 국제관계에 중대한 영향이 있는 비밀활동 즉 조약, 회의 등의 부분적인 사항	1. 국가외교상황중 공개됨으로써 적 또는 가상적국에게 유리하게 악용될 우려가있는 상황 가. 발표되기 전의 부분적인 비밀외교 사항 나. Ⅱ급비밀에 속하지 아니하는 일시적인 보호를 요하는 외사관계 사항
2. 국가 또는 우방국에게 무력침공이나 전쟁을 유발하게 하는 사항 가. 전쟁수행에 관한 전략계획 나. 국내외의 전반적인 특수정보활동 계획 다. 비밀조약 또는 협정이나 비밀합의 내용 라. 비밀무기의 설치 및 사용계획, 전시소요계획 및 비밀무기의 저장량 또는 중요한 과학기술 등의 발전계획 마. 하기사항과 같은 전쟁계획 (1) 핵무기 사용에 관한 전시계획 소요 (2) 기상 및 계획제원 (3) 적 능력의 정보판단 (4) 병력구성 및 운용	2. 국가방위계획 및 그의 효과를 중대하게 위태롭게 하는 사항 가. Ⅰ급비밀에 속하지 아니하는 전쟁계획 및 전략계획 나. 적대행위를 하고 있는 아군의 병력구성 및 배치 사항 다. 장비의 성능·수량 등을 내포하는 국방상 중요한 사항	2. 각군의 중요한 활동장비 및 그의 연구발전 등에 관한 사항 가. 적에게 가치있는 작전 및 전투보고와 정보보고 나. Ⅰ급 및 Ⅱ급비밀에 속하지 아니하는 군부대의 임무·특별활동 및 특수장비의 수량 다. 가치있는 정보를 내포하고 있는 문서교범 및 보고를 요하는 연구 발표계획 라. 부분적 동원 계획 마. 작전상 특히 보호를 요하는 사항 바. 보안상 자주 변경을 요하는 주파수 및 호출부호

Ⅰ 급 비 밀	Ⅱ 급 비 밀	Ⅲ 급 비 밀
3. 국가정보작전 및 특수적인 국내정보활동에 관한 사항 가. 국가정보기관의 능력과 획득된 성과를 판단할 수 있을 정도로 완성된 정보계획 나. 국가의 중요한 정보수집 활동사항 다. 전반적이고 종합된 특수적 치안활동(특수정보)	3. 국가의 중요한 정보화롱계획 및 특수치안 활동에 관한 부분적인 사항 가. 국가가 보유하고 있는 사실을 은폐하여 두어야 가치가 있는 정보 및 자재 나. 국가안전보장을 위하여 필요한 부분적인 특수치안활동에 관한 사항 다. 국가안전보장상 중요한 첩보를 내포하는 통신수단 및 암호자재	3. 국가안전보장상 필요로 하는 특수정보 활동계획의 일부분으로서 실시되는 국부적인 관계사항 가. 정보보고 나. 필요한 존안 다. 조직 및 배치
4. 국방에 매우 중대한 과학 및 기술발전에 관한 사항 가. 국방에 치명적인 극히 새로운 과학 및 기술발전에 관한 사항 나. 원자 및 핵무기의 저장량의 제원	4. 국방에 중대한 과학 및 기술발전에 관한 사항 가. 국방상 중대한 부분에 직접 이용할 수 있는 새로운 군사적 또는 기술적 발전을 가져오는 자재 또는 그 개조에 관한 세부사항	4. 계획단계에서 공개 또는 누설됨으로써 실적 또는 시책면에 차질을 가져올 우려가 있는 계획 및 방침 가. 국가시책의 부분적인 변동에 관한 사항 나. 해외공관의 설치계획
5. 국가정책의 전환이 외국 또는 국민 전체에 직접적인 영향이 있는 사항 가. 계획단계에 있는 종합적인 중대한 경제정책의 급격한 전환 나. 국가관계의 극히 비밀을 요하는 군사원조정책	5. 국가정책의 전환이 외국 또는 국민에게 직접적인 영향이 있는 부분적인 사항 가. Ⅰ급비밀에 속하는 계획을 폭로하지 않는 부분적인 경제정책의 급격한 변화의 일환을 이루고 있는 계획 나. 국방관계의 비밀을 요하는 전반적 군사 원조계획의 세부적 부분	

[별표 2] <신설 74.1.21><개정 05.6.25>

통신보안 위규사항

조	내 용	항	세 부 내 용
1	불온통신	(1)	북한 통신소와의 교신
		(2)	국내 침투 간첩과의 교신
		(3)	적성국 통신소와의 교신
		(4)	비수교 공산국가 통신소와의 교신
		(5)	기타 반국가적인 불온통신
2	군사(경찰포함) 비밀의 누설	(1)	전략 및 작전계획
		(2)	작전 진행 상황
		(3)	특수경비 강화사항
		(4)	작전·병력(군·경·예비군) 동원계획 및 집행
		(5)	군·경·함선·항공기 현황 및 활동계획과 집행
		(6)	군편제·임무 기타 부대현황
		(7)	병력(군·경·예비군) 현황 및 이동상황
		(8)	군사장비(군수품 등) 현황과 집행
		(9)	경찰 및 특수기관의 장비(작전·정보·수사용)현황과 집행
		(10)	군수장비(군수품 등) 생산·공급사항
		(11)	군사시설의 설비·성능에 관한 사항
		(12)	군사시설의 위치 및 이동상황
		(13)	군·경 및 특수목적용 함선·항공기의 위치 또는 배치
		(14)	대공 및 특수경비소의 위치 또는 배치
		(15)	작전지역 위치(작전훈련지역 포함)
		(16)	특수기관 및 국가 중요보안목표 시설 (가, 나, 다급)의 위치 및 이동상황
		(17)	군 전술교리 및 연구사항
		(18)	군사장비의 구성·성능 및 발명 개량연구사항
		(19)	특수장비(작전·정보·보안·수사용)의 구성·
		(20)	성능 및 발명·개량 연구사항
		(21)	기타 국가방위에 영향을 초래하는 사항
3	국가외교 비밀의 누설	(1)	재외공관에 발하는 훈령
		(2)	공개할 수 없는 외교 조약
		(3)	특수임무를 수행하는 외국 주재원의 활동(계획·지시·보고)

조	내 용	항	세 부 내 용
			및 인적사항
		(4)	외교에 관한 방침·계획 및 그 집행
		(5)	기타 국가외교에 영향을 초래하는 사항
4	국가행정 비밀의 누설	(1)	대공관계 특별호구조사
		(2)	대공관계자 신원조사
		(3)	대공관계 교육 및 회합
		(4)	조직·단체에 대한 동향 내사
		(5)	대공관계 신고 및 보고제도(비밀로 분류된 사항)
		(6)	대공용 각종 증명서의 배포 및 관리
		(7)	대공 및 중요사건과 관련된 검문·검색 계획 및 집행
		(8)	기타 국가시책에 영향을 초래하는 사항
5	정보, 첩보의 누설	(1)	첩보수집 활동
		(2)	방첩에 관한 중요시책
		(3)	비공개된 간첩 및 공비의 체포·사살사항
		(4)	간첩 및 용의자 수사활동
		(5)	사상불온자 수사활동
		(6)	정보 및 특수 수사기관의 기구·임무·능력 현황
		(7)	국가원수 및 기타 요인의 비공개 행사계획 및 진행사항
		(8)	군 고급지휘관 및 특수기관 지휘관의 인사에 관한 사항(비공개 사항)
		(9)	적성물(불온삐라 및 간행물 포함) 습득처리
		(10)	불명선박의 발견 및 처리
		(11)	간첩(공비 포함) 및 용의자(괴한 포함) 출현 및 처리
		(12)	아국에서 보유하고 있는 적의 비밀정보
		(13)	중요물자 수송선박의 활동
		(14)	밀수정보 및 수사활동
		(15)	적에 유리한 국가 산업정보
		(16)	공개할 수 없는 사진의 전송
		(17)	기타 국가안전보장 및 공안유지에 영향을 초래하는 정보·첩보
6	보안자재 및 비밀통신 제원의 누설	(1)	암호·음어 및 약호의 누설
		(2)	암호·음어 및 약호의 운용상황
		(3)	암호와 평문의 혼합사용 및 암호문의 평문 이중송신
		(4)	암호전문에 대한 평문 문답

조	내 용	항	세 부 내 용
		(5) (6) (7)	비인가된 암호 및 음어·약호의 사용 군 및 중요통신의 통신운용 및 통신제원 기타 통신자재 보안 및 통신운용에 유해로운 사항
7	비인가 시설의 운용	(1) (2)	비인가 무선시설의 설치운용 비인가 무선시설과 교신
8	비인가 통신제원 사용	(1) (2) (3) (4)	비인가 호출부호 및 주파수 사용 운용허용시간외 전파 발사 비인가 전파형식 사용 지정출력의 초과사용
9	무선침묵 시간위반	(1) (2) (3)	군에서 규정한 침묵시간 위반 전파법 제27조에 의한 침묵시간 위반 기타 특별히 설정한 침묵시간 위반
10	시설목적외 사용	(1) (2) (3) (4)	허가 목적 업무와 관계없는 통신(전파법 제25조) 군사업무와 관계없는 통신(군 통신시설) 사적 중계 통신 기타 사회질서 및 미풍양속을 해하는 통신
11	회로규율 위반	(1) (2) (3) (4) (5) (6) (7)	혼신 및 방해전파 발사 시험전파발사 방법위반 통제국의 지시불용 고의적인 통신의 불이행 및 지연 수신능력 이상의 과속통신 기상논쟁 및 잡담 기타 통신운용 규율 위반
12	통신특성의 노출	(1)	통신사 개인의 괴벽 노출
13	비인가 약부호 사용	(1) (2) (3)	규제외 무선신호 사용 지정외 약부호 사용 음어 및 약호 사용법 위반
14	교신절차의 위반	(1) (2) (3) (4)	호출 및 응답절차의 위반 호출부호 악송 일방적인 교신 중지 응답없음에도 과도한 호출

[별지 제1호 서식] <개정 81. 10. 7>

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 제4조 제1항제2호 및 제5호(국가기밀누설등)
   나. 형 법 제99조(일반이적)
   다. 형 법 제127조(공무상비밀의 누설)
   라. 군형법 제14조 제8호(일반이적)
   마. 군형법 제80조(군사기밀 누설)
   바. 군사기밀보호법 제8조(업무상 누설)
   사. 군사기밀보호법 제9조(과실 누설)

년 월 일

서약자	소속	직급 직위	주민등록번호 성 명	㊞
서약집행자	소속	직급 직위	주민등록번호 성 명	㊞

[별지 제2호 서식]

사 진	비밀취급인가증	No.

소 속

직 책

주민등록번호 성명 20 . . .생

위사람에게 급비밀 암호자재 취급을 인가함

20 . . .

발 행

관 인

0103-1-2A
1969.2.26 승인

9×6cm(백상지 120g/㎡)

Ⅰ 급 ..... 적색
Ⅱ 급 ..... 황색
Ⅲ 급 ..... 청색

[별지 제3호 서식]

Ⅰ 급 비 밀
TOP SECRET

Ⅱ 급 비 밀
SECRET

Ⅲ 급 비 밀
CONFIDENTIAL

가 로 5cm 세 로 1cm

제2편

[별지 제4호 서식]

0103-1-3A 190mm×268mm
69.2.26 승인 (중절지 60g/㎡)

[별지 제5호 서식]

0103-1-5A 190mm×268mm
69.2.26 승인 (중절지 60g/㎡)

[별지 제6호 서식]

0103-1-5A 190mm×268mm
69.2.26 승인 (신문용지 50g/㎡)

[별지 제7호 서식]

1. Ⅰ급 및 Ⅱ급비밀(2중봉투)

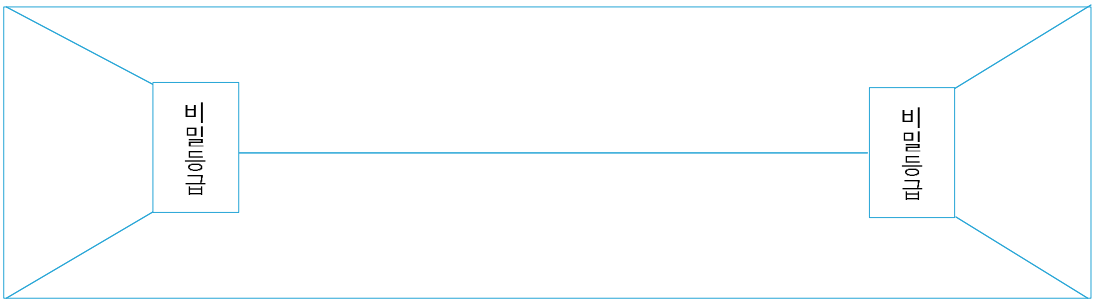
내부봉투(앞)

비 밀 등 급

문서번호
제 목
수 신
참 조
발 신

비 밀 등 급

내부봉투(뒤)



외부봉투

문서번호
제 목
수 신
참 조
발 신

2. Ⅲ급비밀

비 밀 등 급

문서번호
제 목
수 신
참 조
발 신

비 밀 등 급

[별지 제8호 서식]

① 일 련 번 호		비 밀 송 증	②발송일자	20 . . .
③ 수 신		④ 참 조		
⑤ 건 명				
⑥ 사 본 번 호		⑦수 량		⑧ 등기번호
⑨ 발송책임자	직위 직명	주민등록번호	성명	㊞

…… 절 …… 취 …… 선 ……

① 일련번호		비밀영수증	②발송일자	20 . . .
③ 수 신		④ 참 조		
⑤ 건 명				
⑥ 사본번호		⑦수 량		⑧등기번호
⑨ 이상시의 사 유				
⑩ 접 수 자	소속	주민등록번호	성명	㊞
	직위 직명			

0103-1-6A
1969.2.26 승인

190×268mm(신문용지 50g/㎡)

[별지 제9호 서식]

비 밀 관 리 기 록 부

부처명 :　　보관책임자:

관리번호	수량			문서번호	비밀등급	형태	건명	사본번호	예고문	처리담당	보관장소	재분류				참조	
	년월일	발행처	수신처									등급변경	파기	파기확인	근거	영수증	수령자 ㊞

0103-1-7c
1969.2.26 승인

330mm×190mm
(백상지 70g/㎡)

[별지 제10호 서식]

번 호	월 일	분 류 기 호 및 문서번호	발 신	수 신	비 밀 등 급	제 목	수량	원본인수 자 인	수령자인

0103-1-8C
1969.2.26 승인

268mm×190mm
(백상지 70g/㎡)

[별지 제11호 서식]

관리 번호	비밀 등급	건 명	대 출 자			대 출		반 납	
			인가 등급	주민등록번호	성 명	일자	대 출 자 ㊞	일자	보 관 책임자㊞

0103-1-9C
1969.2.26 승인

269mm×190mm
(중절지 70g/㎡)

[별지 제12호 서식]

비 밀 열 람 기 록 전

제 목 :　　[　]급비밀

년월일	소속및직책	인 가 등 급	주민등록 번 호	성 명	열람목적	인장또는 서명

※ 18절 비밀문건의 형태에 따라 세로 또는 가로

[별지 제13호 서식]

비밀지출승인서

1. 지 출 자　　직　책　　주민등록번호　　서명

2. 지출비밀　　관리번호

　　비밀등급　　건　　명

3. 지출목적

4. 지출기간　20　.　.　.　시부터　20　.　.　.까지

5. 지출장소

6. 보안대책

위와 같이 승인함

지 출 자
㊞
보 관 책 임 자
㊞

20　.　.　.

승　인　관

○　○ 장　서　명

[별지 제14호 서식]

비 밀 소 유 현 황 조 사 서

소유처 :　　년　월　일현재

월별 / 비밀등급	이 월 (1)	월 (2)	월 (3)	월 (4)	월 (5)	월 (6)	월 (7)	현보유량 (8)
Ⅰ								
Ⅱ								
Ⅲ								
현보유량								

비 밀 현 황 증 감 내 역

비밀 구분	월별 / 구분	이월 (1)	월 (2)	월 (3)	월 (4)	월 (5)	월 (6)	월 (7)	계 (8)
Ⅰ	접　수								
	작　성								
	이　첩								
	파　기								
	재분류								
	기　타								
Ⅱ	접　수								
	작　성								
	이　첩								
	파　기								
	재분류								
	기　타								
Ⅲ	접　수								
	작　성								
	이　첩								
	파　기								
	재분류								
	기　타								

☆ 기재요령 : 별첨참조　　(18절 · 세로)

기 재 요 령

1. 비밀소유 현황조사서

이월 및 현보유량을 제외한 기타란은 월별 증감 숫자만을 기재하되 증가숫자는 청(흑)색으로 상단에, 감소 숫자는 홍색으로 증가수자 하단에 기록한다.

2. 비밀현황 증감내역

가. 접수와 작성란 및 이첩란은 청(흑)색, 기타란은 홍색으로 기재한다.

나. 작성란은 자체최초 발기작성(응신사항 포함)한 비밀의 원본건수를 기재한다.

다. 이첩란은 상급 또는 타 기관으로부터 접수한 비밀을 이첩 기안한 원본건수를 기재한다

라. 상위 비밀등급으로부터 하위등급으로 저하된 경우 상위 비밀등급의 재분류란은 홍색으로 하되 저하된 하위등급의 증가표시는 그 비밀이 접수된 비밀이면 접수란에 자체에서 작성된 비밀이면 작성란에 기재한다.

예 : 접수된 Ⅰ급비밀이 Ⅱ급비밀로 재분류된 경우

Ⅰ급비밀의 재분류란 – 홍색

Ⅱ급비밀의 접수란 – 청(흑)색

마. 기타란은 보유비밀(관리기록부에 등록 보관중인 것)을 타처로 이송, 이관, 기타 발송한 숫자를 기록하되 최초 배포 계획에 의한 발송숫자는 기록치 않는다.

[별지 제15호 서식]<신설 74.1.21.>

인 감 등 록 서

기 관 명 :

정 책 임 자

계급(직급) : 성명:

인 감	서 명

부 책 임 자

계급(직급) : 성명:

인 감	서 명

위와 같이 당 기관의 음어자재취급(정·부)책임자의 인감을 등록함.

년 월 일

기 관 장 (인)

[별지 제16호 서식]

증명번호

음어(약호)자재증명서			
수 신:		종 류	○ 배부 ○ 반납 ○ 파기 ○ 오파, 분실
발 신:			
자 재 명 칭	부 수	등 록 번 호	비 고

증 명 란	
[배 부]	
(발) 표면에 기록된 자재를 불출하며 정확한 회계유지에 책임을 부담함	(수) 표면에 기록된 자재를 수령하였으며 이의 정확한 회계유지에 책임을 부담함
불출기관	수령기관
불출책임관 계급 성명	수령책임관 계급 성명
불출일자 년 월 일	수령일자 년 월 일
[반 납]	
(발) 표면에 기록된 자재를 반납하였음을 증명함	(수) 표면에 기록된 자재를 반납하였음을 증명함
반납기관	수령기관
반납책임관 계급 성명	수령책임관 계급 성명
반납일자 년 월 일	수령일자 년 월 일
[파 기]	
(발) 표면에 기록된 자재를 파기하였음을 증명함	(수) 표면에 기록된 자재를 파기 또는 정리하였음을 보증함
파기기관	보증기관
피가관 계급 성명	보증관 계급 성명
파기일자 년 월 일	보증일자 년 월 일
[오인파기, 분실]	
(발) 표면에 기록된 자재를 (오인파기, 분실)하였음	(수) 표면에 기록된 자재를 (오인파기, 분실)하였음을 확인함
사고기관	확인기관
사고자 계급 성명	사고확인관 계급 성명
사고일자 년 월 일	사고확인일자 년 월 일

[별지 제17호 서식]<신설 74. 1. 21>

음어(약호)자재기록부

(수령기관용)

자재명칭	부 수	등록번호	수 령		반 납		비 고
			일 자	증명번호	일 자	증명번호	

음어(약호)자재기록부

(배부기관용)

자재명칭	부 수	등록번호	배 부		반 납		비 고
			일 자	증명번호	일 자	증명번호	

[별지 제18호 서식]<신설 74. 1. 21>

음어(약호)자재점검기록부

월 일 시	자 재 명 칭	부 수	보관상태	점 검 란		비 고
				성 명	인	

[별지 제19호]<개정 05.6.25>

신원조사 대상자 명단

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

210mm×297mm(일반용지 60g/㎡(재활용품)

[별지 제20호 서식] <개정 05.6.25> (앞쪽)

신 원 진 술 서

※ 모든 기재사항은 빠짐없이 기재하여 주시기 바랍니다.

(1) 성 명	한글		(2) 주민 등록 번호		(3) 호주 및 관계		사 진 (3cm×4cm)	
	한자							
(4) 본 적								
(5) 주 소						(통 반)		
(6) 직장명 및 소재지	직장명 : 소재지 :				(7) 전화 번 호	직 장 : 가 정 : 이동통신 :		
(8) 신 장	cm	(9) 체 중	kg		(10) 혈액형	형		
(11) 본인 및 배우자 재산	동 산 : 만원, 부동산 : 만원							
(12) 친권자 재산	동산 : 만원, 부동산 : 만원			(13) 특 기		(14)취미		
정 당 및 사회단체 활동관계	(15) 단 체 명			(16) 직 책				
	(17) 가입일자			(18) 가입동기				
	(19) 탈퇴일자			(20) 탈퇴이유				

병역	(21) 군 별	(22) 병 과	(23) 최종계급	(24) 군 번	(25)기간(부터~까지)	(26) 미필사유
					. . ~ . .	

학력	(27) 학 교 명	(28) 기간 (부터~까지)	(29) 전 공 학 과	(30)학 위	(31) 소 재 지
		. . ~ . .			
		. . ~ . .			
		. . ~ . .			
		. . ~ . .			

경력	(32) 기관 또는 업체명	(33) 기간 (부터~까지)	(34) 직 책 (직 급)	(35) 상 벌 관 계 (일자)
		. . ~ . .		
		. . ~ . .		
		. . ~ . .		
		. . ~ . .		
		. . ~ . .		

제2편

(뒤 쪽)

		(36) 관 계	(37) 성 명	(38) 주민등록번호	(39) 최종학교명	(40) 직장명 및 직위	(41) 거주지
가족사항	친가(직계존비속 배우자 형제자매)						
	배우자 부모						
(42) 북한및해외 거주가족							
(43) 교 우							
(44) 보 증 인							

이 내용은 사실과 다름이 없으며, 사실관계 확인을 위해서 「공공기관의 개인정보 보호에 관한 법률」에 의거, 신원조사에 필요한 개인정보 활용에 동의합니다.

년 월 일

작 성 자 성명 인(서명 또는 날인)

210mm×297mm(일반용지 60g/㎡(재활용품)

[별지 제21호 서식]< 신설 05.6.25 >

PERSONAL QUESTIONNAIRE

※ THIS INFORMATION IS ONLY FOR OFFICIAL USE

FULL NAME	Last/ First / Middle			DATE OF BIRTH	Month/Day/Year		【PHOTO】 (3cm×4cm)	
NATIONALITY (include any dual nationality)				PLACE OF BIRTH	City/Country			
ALIEN REGISTRATION NUMBER				DATE & PLACE YOU ENTERED KOREA	Month/Day/Year	City/Country		
ADDRESS					GENDER			
WORK PLACE				JOB/POSITION				
TELEPHONE NUMBERS (Include Area Code)	HOME :		WORK :		MOBILE :			
BLOOD TYPE		HEIGHT	cm	WEIGHT	kg	HAIR COLOR		EYE COLOR

EDUCATION	NAME OF SCHOOL	PERIOD (MM/YY -MM/YY)	DEGREE / DIPLOMA	MONTH/YEAR AWARDED	LOCATION (Street Address & City/Country)

제2편

EMPLOYMENT ACTIVITIES	EMPLOYER/ VERIFIER NAME		PREVIOUS PERIOD (MM/YY-MM/YY)		JOB/POSITION	LOCATION (Street Address & City/Country)
FAMILY	RELATION	FULL NAME Last / First / Middle	DATE OF BIRTH	EDUCATION	OCCUPATION	ADDRESS
RELATIVES & ASSOCIATES IN KOREA	RELATION	FULL NAME Last / First / Middle	DATES KNOWN (MM/YY-MM/YY)	OCCUPATION	TITLE	TELEPHONE NUMBER

I understand that this form maybe submitted for checking against the records of police, security and credit agencies in accordance with security policy.
I declare that the information I have given is true and complete to the best of my knowledge and belief. I understand that any false statement or deliberate omission in the information I have given in this questionnaire may disqualify me for employment or make me liable to disciplinary action which include dismissal.

D A T E :
SIGNATURE :

210mm×297mm(일반용지 60g/㎡(재활용품)

[별지 제22호 서식]< 개정 05. 6. 25>

신원조사회보서

. . . 작성

소 속		직 위		조사목적	
성 명			주민등록번호		
국가관및 직무 자세					
준법성및 보안 의식					
생활 상태					
성질 소행 · 대인 관계					
참고 사항					
국 가 정 보 원 장					

210mm×297mm(일반용지 60g/㎡(재활용품)

[별지 제23호 서식]< 개정 05.6.25>

신원조사 회보서

문서번호 :　　. . . 작성

관련문서		의뢰기관		조사목적	
성명			주민등록번호		
직무자세					
준법성					
생활상태					
대인관계					
특이사항					
기 관 명					

210mm×297mm(일반용지 60g/㎡(재활용품)

② 정보 및 보안업무 기획·조정규정

[일부개정 2008.12.31 대통령령 제21214호 국가정보원(행정안전부와 그 소속기관 직제)]

제1조(목적) 이 영은 국가정보원법 제3조제2항의 규정에 의하여 정보 및 보안업무의 기획·조정에 관하여 필요한 사항을 규정함을 목적으로 한다. <개정 1999.3.31>

제2조(정의) 이 영에서 사용하는 용어의 정의는 다음과 같다.

1. "국외정보"라 함은 외국의 정치·경제·사회·문화·군사·과학 및 지지등 각 부문에 관한 정보를 말한다.
2. "국내보안정보"라 함은 간첩 기타 반국가활동세력과 그 추종분자의 국가에 대한 위해 행위로부터 국가의 안전을 보장하기 위하여 취급되는 정보를 말한다.
3. "통신정보"라 함은 전기통신수단에 의하여 발신되는 통신을 수신·분석하여 산출하는 정보를 말한다.
4. "통신보안"이라 함은 통신수단에 의하여 비밀이 직접 또는 간접으로 누설되는 것을 미리 방지하거나 지연시키기 위한 방책을 말한다.
5. "정보사범 등"이라 함은 형법 제2편제1장 및 제2장의 죄, 군형법 제2편제1장 및 제2장의 죄, 동법 제80조 및 제81조의 죄, 군사기밀보호법 및 국가보안법에 규정된 죄를 범한 자와 그 혐의를 받는 자를 말한다.
6. "정보수사기관"이라 함은 제1호 내지 제5호에 규정된 정보 및 보안업무와 정보사범등의 수사업무를 취급하는 각급 국가기관을 말한다.

제3조(정보 및 보안업무의 기획·조정) 국가정보원장(이하 "국정원장"이라 한다)은 국가정보 및 보안업무에 관한 정책의 수립등 기획업무를 수행하며, 동 정보 및 보안업무의 통합기능수행을 위하여 필요한 합리적 범위내에서 각 정보수사기관의 업무와 행정기관의 정보 및 보안업무를 조정한다. <개정 1999.3.31>

제4조(기획업무의 범위) 국정원장이 정보 및 보안업무에 관하여 행하는 기획업무의 범위는 다음과 같다. <개정 1999.3.31>

1. 국가 기본정보정책의 수립
2. 국가 정보의 중·장기 판단
3. 국가 정보목표 우선순위의 작성
4. 국가 보안방책의 수립

5. 정보예산의 편성
6. 정보 및 보안업무의 기본지침 수립

제5조(조정업무의 범위) 국정원장이 정보 및 보안업무에 관하여 행하는 조정 대상기관과 업무의 범위는 다음과 같다. <개정 1990·1·3, 1991·2·1, 1993·3·6, 1996·8·8, 1999.3.31, 2008.12.31>

1. 통일부
   가. 통일에 관한 국내외 정세의 조사·분석 및 평가에 관한 사항
   나. 남북대화에 관한 사항
   다. 이북5도의 실정에 관한 조사·분석 및 평가에 관한 사항
   라. 통일교육에 관한 사항
2. 외교통상부
   가. 국외정보의 수집에 관한 사항.
   나. 출입국자의 보안에 관한 사항
   다. 재외국민의 실태에 관한 사항.
   라. 통신보안에 관한 사항.
3. 행정안전부
   가. 국내 보안정보(외사정보 포함)의 수집·작성에 관한 사항
   나. 정보사범등의 내사·수사 및 시찰에 관한 사항
   다. 신원조사업무에 관한 사항.
   라. 통신정보 및 통신보안업무에 관한 사항.
4. 법무부
   가. 국내 보안정보의 수집·작성에 관한 사항.
   나. 정보사범등에 대한 검찰정보의 처리에 관한 사항.
   다. 공소보류된 자의 신병처리에 관한 사항.
   라. 적성압수금품등의 처리에 관한 사항.
   마. 정보사범등의 보도 및 교도에 관한 사항.
   바. 출입국자의 보안에 관한 사항.
   사. 통신보안에 관한 사항.
5. 국방부
   가. 국외정보·국내보안정보·통신정보 및 통신보안업무에 관한 사항.
   나. 제4호나목 내지 마목에 규정된 사항.
   다. 군인 및 군무원의 신원조사업무지침에 관한 사항.

라. 정보사범등의 내사·수사 및 시찰에 관한 사항.

5의2. 문화체육관광부

가. 공연물 및 영화의 검열·조사·분석 및 평가에 관한 사항

나. 신문·통신 그 밖의 정기간행물과 방송 등 대중전달매체의 활동 조사·분석 및 평가에 관한 사항

다. 대공심리전에 관한 사항

라. 대공민간활동에 관한 사항

6. 지식경제부

우편검열 및 정보자료의 수집에 관한 사항

6의2. 방송통신위원회

가. 전파감시에 관한 사항

나. 그 밖에 통신정보 및 통신보안업무에 관한 사항

7. 국토해양부

가. 국내 보안정보(외사정보 포함)의 수집·작성에 관한 사항

나. 정보사범등의 내사·수사 및 시찰에 관한 사항

다. 통신정보 및 통신보안 업무에 관한 사항

8. 과학기술부

북한 및 공산국가의 과학기술 정보 및 자료의 수집관리와 활용에 관한 사항

8의2. 삭제 <2008.12.31>

9. 기타 정보 및 보안업무 관련 기관

정보 및 보안관련업무에 관한 사항

제6조(조정의 절차) 국정원장은 제5조의 조정을 행함에 있어 국가안보에 중대한 영향을 미치는 주요사안에 관하여는 직접 조정하고, 기타 사안에 관하여는 일반지침에 의하여 조정한다. <개정 1999.3.31>

제7조(정보사범 등의 내사등) ①정보수사기관이 정보사범등의 내사·수사에 착수하거나 이를 검거한 때와 관할 검찰기관(군검찰기관을 포함한다. 이하 같다)에 송치한 때에는 즉시 이를 국정원장에게 통보하여야 한다. <개정 1999.3.31>

②관할 검찰기관의 장은 정보사범 등에 대하여 검사의 처분이 있을 때에는 즉시 이를 국정원장에게 통보하여야 한다. <개정 1999.3.31>

③관할 검찰기관의 장은 정보사범 등의 재판에 대하여 각 심급별로 그 재판결과를 국정원장에게 통보하여야 한다. <개정 1999.3.31>

제8조(정보사범 등의 신병처리 등) ①정보수사기관의 장은 주요 정보사범 등의 신병처리에 대하여 국정원장의 조정을 받아야 한다. <개정 1999.3.31>
②정보수사기관이 주요정보사범등·귀순자·불온문건 투입자·납북귀환자·망명자 및 피난민에 대하여 신문등을 하고자 할 때에는 국정원장의 조정을 받아야 한다. <개정 1999.3.31>

제9조(공소보류 등) ①정보수사기관(검사를 제외한다)의 장이 주요 정보사범 등에 대하여 공소보류 의견을 붙일 필요가 있다고 인정할 때에는 국정원장에게 통보하여 조정을 받아야 한다. <개정 1999.3.31>
②검사는 주요 정보사범 등에 대하여 공소보류 또는 불기소 의견으로 송치된 사건을 소추하거나 기소의견으로 송치된 사건을 공소보류 또는 불기소 처분할 때에는 국정원장과 협의하여야 한다. <개정 1999.3.31>

제10조(적성압수금품 등의 처리) 정보수사기관이 주요 적성장비 또는 불온문건 기타 금품을 압수하거나 취득한 때에는 즉시 이를 국정원장에게 통보하고 정보수집에 필요한 조정을 받아야 한다. <개정 1999.3.31>

제11조(정보사업·예산 및 보안업무의 감사) ①국정원장은 제5조에 규정된 각급기관에 대하여 연 1회이상 정보사업 및 그에 따른 예산과 보안업무 감사를 실시한다. 다만, 보안업무 감사는 중앙단위 기관에 한한다. <개정 1999.3.31>
②국정원장은 제1항의 감사를 실시함에 있어서 정책자료 발굴에 중점을 둔다. <개정 1999.3.31>
③국정원장은 제1항의 규정에 의한 감사 결과를 대통령에게 보고하고 피감사기관에 통보한다. <개정 1999.3.31>
④제3항의 규정에 의하여 감사결과를 통보받은 피감사기관의 장은 감사결과에 대하여 필요한 조치를 강구하여야 한다.

제12조(시행규칙) 이 영 시행에 관하여 필요한 규칙은 정보조정협의회의 의결을 거쳐 국정원장이 정한다. <개정 1999.3.31>

부 칙 <제10239호,1981.3.2>

이 영은 공포한 날로부터 시행한다.

부 칙(문화부직제) <제12895호,1990.1.3>

제1조(시행일) 이 영은 공포한 날로부터 시행한다.

제2조 생략
제3조(다른법령의 개정) ①내지 ⑧생략
⑨정보및보안업무기획·조정규정중 다음과 같이 개정한다.
제5조에 제4호의2를 다음과 같이 신설하고, 동조제6호를 삭제하며, 동조에 제8호의2를 다음과 같이 신설한다.
4의2. 문화부
공연물 및 영화의 검열·조사·분석 및 평가에 관한 사항
8의2. 공보처
가. 신문·통신 기타 정기간행물과 방송등 대중전달매체의 활동조사·분석 및 평가에 관한 사항
나. 대공심리전에 관한 사항
다. 대공민간활동에 관한 사항
⑩내지 <64>생략

부 칙(통일원과그소속기관직제) <제13269호,1991.2.1>
제1조(시행일) 이 영은 공포한 날부터 시행한다.
제2조 및 제3조 생략
제4조(다른 법령의 개정) ①정보및보안업무기획·조정규정중 다음과 같이 개정한다
제5조제8호를 삭제하고, 동조중 제1호 내지 제7호를 제2호 내지 제8호로 하고, 동조에 제1호를 다음과 같이 신설한다.
1. 통일원
가. 통일에 관한 국내외 정세의 조사·분석 및 평가에 관한 사항
나. 남북대화에 관한 사항
다. 이북5도의 실정에 관한 조사·분석 및 평가에 관한 사항
라. 통일교육에 관한 사항
② 내지 ⑮생략

부 칙(문화체육부와그소속기관직제) <제13869호,1993.3.6>
제1조(시행일) 이 영은 공포한 날부터 시행한다.
제2조 및 제3조 생략
제4조(다른 법령의 개정) ①정보및보안업무기획·조정규정중 다음과 같이 개정한다.
제5조제5호의2중 "문화부"를 "문화체육부"로 한다.
② 내지 <70>생략

부 칙(해양경찰청과그소속기관직제) <제15136호,1996.8.8>

제1조(시행일) 이 영은 공포한 날부터 시행한다.

제2조생략

제3조(다른 법령의 개정) ① 내지 ⑭생략

⑮정보및보안업무기획·조정규정중 다음과 같이 개정한다.

제5조제3호가목중 "외사·해양경찰정보"를 "외사정보"로 한다.

제5조에 제7호를 다음과 같이 신설한다.

7. 해양수산부

가. 국내 보안정보(외사정보 포함)의 수집·작성에 관한 사항

나. 정보사범등의 내사·수사 및 시찰에 관한 사항

다. 통신정보 및 통신보안 업무에 관한 사항

<16> 내지 <19>생략

제4조 생략

부 칙(국가정보원직원법시행령) <제16211호,1999.3.31>

제1조(시행일) 이 영은 공포한 날부터 시행한다.

제2조 및 제3조 생략

제4조(다른 법령의 개정) ①내지 ⑤생략

⑥정보및보안업무기획·조정규정중 다음과 같이 개정한다.

제1조중 "국가안전기획부법 제2조제2항"을 "국가정보원법 제3조제2항"으로 한다.

제3조중 "국가안전기획부장(이하 "안전기획부장"이라 한다)"을 "국가정보원장(이하 "국정원장"이라 한다)"으로 한다.

제4조 본문, 제5조 본문, 제6조, 제7조제1항 내지 제3항, 제8조제1항·제2항, 제9조제1항·제2항, 제10조, 제11조제1항 내지 제3항 및 제12조중 "안전기획부장"을 각각 "국정원장"으로 한다.

제5조제1호중 "통일원"을 "통일부"로 하고, 동조제2호중 "외무부"를 "외교통상부"로 하며, 동조제3호중 "내무부"를 "행정자치부"로 하고, 동조제5호 나목중 "제3호"를 "제4호"로 하며, 동조제5호의2중 "문화체육부"를 "문화관광부"로 하고, 동조제6호중 "체신부"를 "정보통신부"로 하며, 동조제8호중 "과학기술처"를 "과학기술부"로 하고, 동조제8호의2중 "공보처"를 "공보실"로 한다.

⑦내지 <28>생략

부 칙<제21214호, 2008.12.31> (행정안전부와 그 소속기관 직제)

제1조(시행일) 이 영은 공포한 날부터 시행한다. <단서 생략>

제2조부터 제4조까지 생략

제5조(다른 법령의 개정) ① 부터 <89> 까지 생략

<90> 정보및보안업무기획·조정규정 일부를 다음과 같이 개정한다.

제5조제3호 중 "행정자치부"를 "행정안전부"로 하고, 같은 조 제5호의2를 다음과 같이 하며, 같은 조 제6호를 다음과 같이 하고, 같은 조에 제6호의2를 다음과 같이 신설하며, 같은 조 제7호 각 목 외의 부분 중 "해양수산부"를 "국토해양부"로 하고, 같은 조 제8호의2를 삭제한다.

5의2. 문화체육관광부

가. 공연물 및 영화의 검열·조사·분석 및 평가에 관한 사항

나. 신문·통신 그 밖의 정기간행물과 방송 등 대중전달매체의 활동 조사·분석 및 평가에 관한 사항

다. 대공심리전에 관한 사항

라. 대공민간활동에 관한 사항

6. 지식경제부

우편검열 및 정보자료의 수집에 관한 사항

6의2. 방송통신위원회

가. 전파감시에 관한 사항

나. 그 밖에 통신정보 및 통신보안업무에 관한 사항

<91> 부터 <175> 까지 생략

Ⅱ 농림수산식품부소관 보안관계규정

❶ 농림수산식품부 보안업무시행세칙

제 정 1964. 8.11. 농 림 부 훈령 제 108 호
개 정 1964. 9. 7. 농 림 부 훈령 제 110 호
1969. 6.17. 농 림 부 훈령 제 205 호
1969. 8.28. 농 림 부 훈령 제 206 호
1969. 10.7. 농 림 부 훈령 제 209 호
1971. 5.11. 농 림 부 훈령 제 235 호
1972. 2. 9. 농 림 부 훈령 제 252 호
1973. 6.22. 농 림 수 산 부 훈령 제 292 호
1974. 8.29. 농 림 수 산 부 훈령 제 310 호
1975. 7. 8. 농 림 수 산 부 훈령 제 326 호
1976. 8.10. 농 림 수 산 부 훈령 제 361 호
1977. 7. 7. 농 림 수 산 부 훈령 제 387 호
1978. 4.21. 농 림 수 산 부 훈령 제 407 호
1979. 1.15. 농 림 수 산 부 훈령 제 430 호
1980. 1.31. 농 림 수 산 부 훈령 제 452 호
1981. 4. 2. 농 림 수 산 부 훈령 제 474 호
1981.11.12. 농 림 수 산 부 훈령 제 495 호
1982. 6. 1. 농 림 수 산 부 훈령 제 523 호
1984. 11.3. 농 림 수 산 부 훈령 제 590 호
1990. 6.12. 농 림 수 산 부 훈령 제 708 호
1992. 1.25. 농 림 수 산 부 훈령 제 742 호
1993. 4.15. 농 림 수 산 부 훈령 제 767 호
1995. 1. 5. 농 림 수 산 부 훈령 제 806 호
2001. 6.23. 농 림 부 훈령 제1073호
2002. 10.8. 농 림 부 훈령 제1117호
2004. 6.19. 농 림 부 훈령 제1165호
전부개정 2008. 5.20. 농림수산식품부 훈령 제 14 호
개정 2009. 4. 3. 농림수산식품부 훈령 제 83 호

제1장 총 칙

제1조(목적) 이 세칙은 「보안업무규정」(이하 "규정"이라 한다.) 및 「보안업무규정시행규칙」(이하 "규칙"이라 한다)이 정한 바에 따라 보안업무의 적정한 운영과 관리를 위하여 필요한 사항을 규정함을 목적으로 한다.

제2조(적용) ①이 세칙은 농림수산식품부 본부와 그 소속기관 및 산하단체에 적용한다. ②보안업무에 대하여 다른 법령에 특별히 정하지 아니한 경우에는 규정, 규칙 및 이 지침이 정하는 바에 따른다. 다만, 기관별 특수사항은 상위기관의 규정에 저촉되지 아니하는 범위 내에서 기관의 장이 따로 정할 수 있다.

제3조(용어의 정의) 이 내규에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "소속기관"이라 함은 「농림수산식품부와 그 소속기관 직제」(이하 "직제"라 한다) 제2조의 규정에 의한 소속기관을 말한다.
2. "산하단체"이라 함은 「공공기관의 운영에 관한 법률」 제2조에서 정한 공공기관 및 다른 법률에 의하여 업무상 농림수산식품부장관의 관리·감독을 받는 단체를 말한다.

제2장 비밀의 보호

제1절 보안심사위원회

제4조(보안심사위원회 설치) ①보안업무의 효율적인 운영과 중요보안 사항을 심의·결정 하기 위하여 기관별로 보안심사위원회(이하 "심사위원회"라 한다)를 둔다.<개정 2002.10.8.> ②심사위원회를 설치하여야 할 소속기관은 고위공무원단(단, 어업지도사무소 제외)에 속하는 공무원을 장으로 하는 1차 소속기관으로 하고, 산하단체는 중앙 및 도 단위 단체와 이에 준하는 단체로 한다. 심사위원회를 설치하지 아니한 기관의 심사사항은 해당 기관장의 요청에 의하여 차상급기관의 심사위원회에서 심의한다.<개정 2001.6.23.>

제5조(심사위원회의 기능) 심사위원회는 다음 사항을 심사·결정한다.

1. 보안업무내규의 제정 및 개폐에 관한 사항
2. 보안업무계획 수립에 관한 사항
3. 신원특이자 보안관리에 관한 사항
4. 중요 보안위반자의 처리에 관한 사항
5. 중요시설공사에 대한 보안대책
6. 정보통신·지적정보보안담당관 임무중 중요 보안업무에 관한 사항
7. 차하위기관에서 심사요청하는 사항
8. 기타 보안업무 수행상 위원장이 필요하다고 인정하는 사항

제6조(심사위원회의 구성) ① 심사위원회는 위원장 및 부위원장 각 1인과 3인이상 10인이내의 위원으로 구성한다

②농림수산식품부 보안심사위원회의 위원장은 제1차관, 부위원장은 기획조정실장이 되고, 위원은 비상계획관·농업정책국장·국제농업국장·식량정책단장·수산정책관·국제수산관이 된다.<개정 2001.6.23.>.

③소속기관의 심사위원회 위원장은 기관장이 되고, 부위원장 및 위원은 기관장이 소속직원 중에서 상위자로부터 차례로 임명한다.

④산하단체의 심사위원회 위원장은 그 단체의 부책임자가 되며, 부위원장 및 위원은 그 단체의 장이 소속직원 중에서 상위자로부터 차례로 임명한다. 다만, 부책임자가 2인이상인 경우에는 보안업무 관장 부책임자가 위원장이 된다.

제7조(위원장의 직무) ①심사위원회 위원장은 위원회를 대표하며, 위원회를 소집하고 그 의장이 된다.

②위원장이 부득이 한 사유로 직무를 수행할 수 없을 때에는 부위원장이 그 직무를 대행한다. 이하 직무대행은 직제순에 따른다.

③위원장은 표결권을 가지며, 가부 동수인 때에는 결정권을 가진다.

제8조(간사) ①심사위원회의 사무를 처리하기 위하여 간사를 둔다.

②농림수산식품부 심사위원회의 간사는 운영지원과장이 되며, 소속기관 및 산하단체 심사위원회의 간사는 기관 및 단체의 장이 보안업무와 관련된 부서의 직원 중에서 임명한다.<개정 2001.6.23.>

제9조(의안제출 및 심사결정) ①각 기관 및 단체에 속한 부서의 장은 소관업무에 대하여 심사할 의안을 간사에게 제출하여야 하며, 간사는 의안으로서의 타당성 여부를 검토한 후 위원장에게 보고하여야 한다.<개정 2001.6.23.>

②심사위원회의 운영은 회의 개최를 원칙으로 하되, 경미한 사안이나 부득이한 사유로 개의하지 못할 경우에는 서면심사로 대체할 수 있다.<신설 2002.10.8.>

③심사위원회의 회의는 재적위원 과반수 이상 출석으로 개의하고 출석위원 과반수 이상 찬성으로 별지 제1호서식에 따라 의결한다. 서면심의의 경우도 이와 같다.<개정 2002. 10.8.>

④위원장은 필요하다고 인정할 때에는 관련자를 출석시켜 의견을 진술하게 할 수 있다.

⑤농림수산식품부 심사위원회는 소속기관 및 산하단체에서 제청한 사안에 대하여 복심권을 가지며, 이를 최종적으로 심사·결정한다. <개정 2001.6.23.>

⑥간사는 별지 제2호서식의 회의록을 작성·유지 하여야 한다.

제2절 인원보안

제10조(신원조사) ①규정 제31조에 의한 신원조사시 다음 각 호에 해당하는 자는 농림수산식품부장관이 국가정보원장에게 요청한다.

1. 고위공무원단에 속하는 일반직 공무원 또는 3급 공무원 및 이와 동등한 공무원 임용예정자
2. 장관이 국가보안상 필요하다고 인정하여 요청하는 자
3. 외국인으로서 공무원 임용예정자
4. 공공단체의 직원과 임원의 임명에 있어서 정부의 승인이나 동의를 요하는 법인의 임원 및 직원
5. 해외주재공무원, 국제기구 파견 공무원

②농림수산식품부장관과 소속기관장 및 산하기관장은 다음 각 호에 해당하는 자의 신원조사를 관할 경찰청장에게 요청한다.

1. 공무원임용예정자(국가정보원장에 요청하는 자 제외)
2. 공무원이 아닌 자의 비밀취급인가예정자
3. 그 밖에 각급 기관장이 국가보안상 신원조사가 필요하다고 인정하는 자

③신원조사를 하지 아니한 자는 공무원으로 임용할 수 없다. 다만, 부득이한 경우에 한하여 임용후 15일 이내에 신원조사를 의뢰할 수 있다.

④ 임시직이나 단순고용직으로 임용되는 사람중 국가중요시설·지역의 통제·출입 및 중요문서·자재의 취급자로서 당해기관의 장이 보안상 필요로 하는 사람외에는 신원조사를 생략한다.<신설 2009.4.3.>

제11조(구비서류) 신원조사는 다음 각호의 서류를 갖추어 요청하여야 한다.

1. 대상자 명단(규칙 제19호서식)
2. 신원진술서 2부(규칙 제20호서식)

제12조(신원대장) 인사업무 주관과장(이하 “인사담당관”이라 한다)은 별지 제3호서식에 의한 신원대장을 작성·비치하고, 신원조사 내용을 기록하여 비밀취급인가 및 인사관리의 기본자료로 활용하되 현재원 명부가 되도록 관리하여야 한다.

제13조(신원조사회보서의 관리) 신원조사회보서는 개인별 인사기록과 함께 보관하고 전출자 및 퇴직자는 개인별 인사기록과 함께 이송 또는 관리한다.

제14조(신원특이자의 임용) 인사담당관은 특이기록회보자를 임용하거나 보직을 부여할 때에

는 특이내용을 고려하여 결정하여야 한다.

제15조(임시용원의 임용) ①임시직이나 단순고용직(이하 "임시용원"이라 한다.)을 채용하고자 할 때에는 채용 예정자의 채용기간 및 담당업무 내용을 인사담당관에게 제출하여야 한다.<개정 2004.6.19.><개정 2009.4.3.>
②통제구역 및 경비근무자 등 당해기관의 장이 보안상 필요로 하는 자를 1월 이상 임시용원으로 상근하게 할 경우에는 인사담당관은 제11조 각호의 서류를 징구하여 신원조사를 하여야 하며, 신원조사결과 유해로운 내용이 회보되었을 때에는 임시용원으로 임용할 수 없다.<개정 2004.6.19.>

제16조(임시용원의 업무한계 및 감독책임) ①임시용원에게는 비밀취급 담당 및 통제구역 근무 등 보안상 책임있는 주요업무를 부여하여서는 아니된다.<개정 2004.6.19.>
② 임시용원에게 부득이 한 사유로 제1항의 업무를 취급하게 할 때에는 소속기관장 또는 소속과장이 관리·감독을 하며, 임시용원으로 인하여 발생하는 보안사고에 대해 책임을 진다. <개정 2009.4.3.>

제17조(비밀취급인가권자 및 담당부서) ①농림수산식품부장관은 규정 제7조제2항제5호에 의하여 다음 각 호의 기관장을 Ⅱ급이하의 비밀취급 인가권자로 지정한다.<개정 2001.6.23.>
1. 국립농산물품질관리원장
2. 농업연수원장 <개정 2009.4.3.>
3. 국립수의과학검역원장
4. 국립식물검역원장
5. 국립종자원장
6. 국립수산과학원장
7. 국립수산물품질관리원장
8. 수산인력개발원장
9. 동·서해 어업지도사무소장
10. 농업협동조합중앙회장
11. 한국농촌공사사장
12. 농수산물유통공사사장
13. 한국마사회장
14. 수산업협동조합중앙회장
15. 한국원양산업협회장

②제1항 각 호의 기관장은 취임과 동시 비밀업무를 취급(수집·작성·관리·분류·재분류·수발)하며, 당해기관의 보안책임을 진다.
③각 기관의 비밀취급인가 업무는 그 기관의 보안업무 담당부서에서 수행한다.<개정 2004.6.19.>

제18조(Ⅰ급 비밀취급인가 대상자) 농림수산식품부장관이 필요하다고 인정할 때에는 소속직원중에서 Ⅰ급 비밀취급을 인가할 수 있다.<개정 2001.6.23.>

제19조(비밀취급인가 절차) ①비밀취급인가를 신청할 때에는 농림수산식품부는 각 실·국장이, 소속기관는 각 과장이, 산하단체는 실·처장이 다음 각 호의 서류를 갖추어 별지 제4호서식에 의하여 보안담당관에게 제출하여야 한다.<개정 2001.6.23. 2004.6.19.>
1. 신원조사회보서 사본 1부(임용권을 달리하는 기관에 한함, 규칙 별지 제23호서식)
2. 암호자재인 경우에는 암호의 종류, 명칭, 용도, 발행처, 사용범위 및 비밀등급 기타 인가권자가 알아야 될 사항
②보안담당관은 직책상의 필요성 여부, 신원대장 대조, 인사기록카드상 비밀취급인가 여부 등을 검토 후 제1항의 구비서류를 첨부하여 인가 제청한다.<개정 2004.6.19.>
③신원특이자에 대한 비밀취급인가는 심사위원회의 심사를 거쳐 인가 여부를 결정하고 불가로 결정된 자에 대하여는 즉시 다른 보직으로 변경하여야 한다.
④제1항의 규정에 불구하고 별도의 신청절차 없이 보직과 동시에 Ⅱ급 비밀취급인가를 받는 자를 지침으로 정할 수 있으며, 이 경우 비밀취급이 불필요한 직위 임용 시 해제된 것으로 본다.
⑤비밀취급을 인가할 때에는 규칙 제5조에 의한 서약을 집행하는 기초보안교육을 실시하여야 한다. 다만, 제4항에 의하여 특별인가를 받은 자는 규칙 제5조 별지1호서식에 의한 서약서를 보안담당관에게 제출하여야 한다.

제20조(비밀취급해제 절차) ①비밀취급인가권자는 비밀취급인가를 받은 자가 면직 또는 다른 기관으로 전출될 경우에는 면직 또는 전출발령과 동시에 서면으로 해제발령하여야 한다. 다만, 비밀취급인가권자를 달리하지 아니하는 기관 내 전보시는 그러하지 아니하다.
②부서의 장은 인가자가 비밀취급이 불필요하게 된 경우에는 별지 제4호서식에 의하여 해제신청을 하여야 하며, 인가권자는 서면으로 해제 발령하여야 한다.
③규정 제8조제3항제1호에 의한 보안사고인 경우에는 규정 제38조 및 규칙 제62조에 정한 행정조치를 취하여야 한다.

제21조(비밀취급등급변경 절차) 비밀취급등급 변경신청은 별지 제4호서식에 의하고 절차는 제19조 및 제20조의 인가 및 해제 절차에 준한다.

제22조(퇴직공무원에 대한 보안교육) ①공무원이 퇴직시에는 근무중 알게된 기밀의 누설방지를 위한 보안교육을 실시하고 별지 제5호서식에 의한 서약을 집행하여야 한다.
②제1항에 의한 보안교육 서약집행은 인사담당부서에서 실시한다.

제23조(비밀취급인가 및 해제 기록관리) ①비밀취급인가권자가 제19조 및 제20조의 의하여 비밀취급 인가 또는 해제를 한 때에는 별지 제6호서식의 비밀취급인가대장에 그 사유와 일자 등을 기록·관리하여야 한다.
②보안담당관은 제1항에 관한 사항을 인사담당관에게 통보하여 인사리록카드에 기록하도록 하여야 한다.

제24조(비밀취급인가의 특례) ①농림수산식품부 각 실·국장 및 제17조에 지정한 기관장의 업무상 조정감독을 받는 기업체 또는 단체에 대하여 소관 비밀을 계속적으로 취급하게 할 때에는 비밀취급인가에 필요한 조치를 취하도록 하여야 한다.<개정 2001.6.23.>
②제1항의 인가신청서를 접수한 감독기관의 장은 제66조의 규정에 의한 보안교육을 실시한 후 제19조에 준하여 인가 조치하고, 그 결과를 별지 제7호서식에 의거 농림수산식품부장관에게 즉시 보고하여야 한다.<개정 2001.6.23.>
③규칙 제4조에 의한 비밀취급인가의 특례 범위를 다음과 같이 제한한다.
1. 업무상 조정감독을 받는 기업체 또는 단체직원으로서 비밀취급이 필요한 최소한의 인원에 한한다.
2. 비밀취급인가등급은 Ⅱ급 이하로 한다.
④비밀취급인가의 특례에 따른 감독 및 보안책임은 인가기관의 장에게 있다.
⑤ 국가비상훈련(을지연습)을 실시하기 위하여 동원되는 자가 훈련기간중 훈련과 관련된 비밀사항을 취급하기 위해 비밀취급인가를 할 경우에는 서약서 집행으로 신청절차에 갈음하며, 훈련종료와 동시에 해제된 것으로 본다.

제25조(보안담당관의 지정) 다음에 정하는 자는 보직과 동시에 당해기관의 보안담당관이 된다.
1. 농림수산식품부 : 운영지원과장<개정 2001.6.23.>
2. 소속기관 : 1차 소속기관(국립농산물품질관리원 지원 포함)는 서무담당과장 또는 그 기관의 차하위자로 하고, 2차 또는 그 이하의 기관은 기관장<개정 2001.6.23.>
3. 산하단체

가. 본회(사) : 단체의 장이 보안업무와 관련된 부서중에서 지정하는 실(처)장급 책임자.<개정 2001.6.23.>

나. 1차 또는 그 이하기관 : 각 기관의 장이 지정한다.

제26조(분임보안담당관의 지정) 다음에 정하는 자는 보직과 동시에 소속부서의 분임보안담당관이 된다.

1. 농림수산식품부 : 각 실·국 주무담당관 또는 주무과장(이와는 별도로 정보통신 보안분야는 정보화지원팀장, 국가지리정보 보안분야는 농지과장, 어업통신분야는 지도안전과장)<개정 2001.6.23.><개정 2009.4.3.>
2. 소속기관 및 산하단체 : 각 기관의 장이 지정

제27조(보안담당관 교체 및 인계 인수) ①농림수산식품부, 소속기관 및 산하단체의 보안담당관이 교체되었을 때에는 3일 이내에 아래 양식에 의하여 명함판 사진 1매, 신원진술서 1매, 인사기록카드 사본 1부를 첨부하여 국가정보원장 또는 관할 시·도지부장에게 통보하여야 한다.<개정 2001.6.23.>

소 속	전 보안담당관		신 보안담당관		발령 일자	비 고
	직 급	성 명	직 급	성 명		

②각 기관(소속기관 및 산하단체의 1차 및 그 이하기관 포함)의 보안담당관 인계인수서에는 다음사항이 포함되어야 하며, 차상위자(소속기관 및 산하단체의 1차 및 그 이하 기관중 기관장이 보안담당관인 경우에는 그 기관의 차하위자)가 입회하여 확인한다.<개정 2004.6.19.>

1. 보안업무 현황
2. 연도 보안업무 세부시행계획 및 추진실적
3. 비밀취급인가자 현황 및 비밀문서 보유 현황
4. 보안심사위원회 운영에 관한 사항
5. 기타 보안활동에 관한 사항

제3절 문서보안

제28조(비밀세부분류지침) 규정 제11조 및 규칙 제8조에 의한 농림수산식품부 비밀세부분류지침은 국가정보원에서 정하는 국가비밀세부분류지침에 의한다. 다만, 이를 변경 또는 추가하고자 할 때에는 매년 9월말까지 농림수산식품부장관에게 보고하여 그 사항을 국가비밀세부분류지침에 반영토록 한다.<개정 2001.6.23.>

제29조(비밀의 분류) 비밀의 분류는 규정 제9조 및 제10조에 의하여(과도·과소분류 금지, 독립분류, 섭외비밀의 존중) 분류하되, 분류자는 세부분류지침에 의한 근거를 반드시 기안지 여백에 표시하여야 한다.

제30조(재분류 검토) ①비밀을 생산한 과(실)·부서의 과장 또는 부서 책임자는 규칙 제10조 제2항에 의하여 연2회(6월, 12월) 비밀원본의 재 분류검토를 실시하여야 하며, 검토 표시는 매 비밀원본 표면의 적당한 여백에 한다. 다만, 여백이 없을 때에는 문서 후면에 별지를 첨부하여 기록관리한다.
②규정 제13조제2항에 의거 비밀을 재분류할 때에는 그 사유를 명시하여 기관의 장의 결재를 받은 후 실시하고 비밀관리기록부의 관계란에 기록정리한다.
③규칙 제15조에 의하여 비밀원본을 계속 보관하고자 할 때에는 그 사유를 명시하여 농림수산식품부는 실·국장, 소속기관은 기관장, 산하단체는 이사 또는 상무의 결재를 받아 예고문 아래와 비밀관리기록부의 등급변경란에 "직권보관"이라고 각각 붉은 글씨로 표시하고 계속 보관할 수 있다.<개정 2002.10.8.>

제31조(비밀기록물 원본의 보존) ①비밀기록물(대외비 포함. 이하 같다)의 원본 생산부서는 반드시 예고문과 함께 보존기간을 분명하게 기록하여야 한다.<신설 2004.6.19.>
② 비밀기록물의 원본은 공공기관의기록물관리에관한법률 시행령 제29조제2항에 정하는 바에 따라 보호기간 경과시 기록물관리기관으로 이관하여야 한다.<신설 2004.6.19.>

제32조(비밀소유현황 및 비밀취급인가자 현황조사) ①비밀의 소유현황 및 비밀취급인가자 현황조사(이하 "현황조사"라 한다)는 각 보관 책임자가 실시하되, 6월과 12월 말일을 기준하여 규칙 제41조에 의한 제14호서식의 비밀소유현황과 별지 제8호서식 비밀취급인가자 현황을 조사하여 다음 달 10일까지 농림수산식품부장관에게 보고하여야 한다. <개정 2002.10.8.>
②농림수산식품장관은 규칙 제41조에 의거 6월과 12월말 현재 비밀소유현황 및 비밀취급인가자 현황을 다음 달 25일까지 국가정보원장에게 통보한다.<개정 2002.10.8.>
③자체현황조사는 별지 제9호서식에 의거 각 보관책임자가 매월 말일을 기준하여 조사하고 그 결과를 농림수산식품부는 국장, 소속기관은 기관의 장, 산하단체는 소속 각 실·처장에게 보고하고 결재를 받아야 한다.

제33조(대외비 문서) ①규칙 제7조제3항의 규정에 의한 대외비 문서는 다음과 같다.
1. 중요 정책자료로서 일정기간 외부에 대하여 보호를 필요로 하는 사항<개정 2002.10.8.>

2. 신원특이자에 대한 신원관계서류 등 직접 취급자 또는 관계자 이외의 자에게 공개할 수 없는 사항
3. 확정되지 아니한 중요사항의 운영계획서 및 예산관계서류
4. 각종 법령자료중 특히 중요하다고 인정되는 사항
5. 타 기관에서 접수된 대외비 문서

② 대외비 문서의 보호기간은 예측되는 상황 및 경우를 고려하여 최단기의 기간으로 책정하여야 한다. 다만, 예측할 수 없는 사항은 발행일로부터 통상 1년 이내로 한다.

제34조(비밀문서의 통제관 및 통제) ①규정 제27조에 의한 비밀문서통제관 (이하 "통제관"이라 한다)은 각 기관의 보안담당관 또는 보안업무를 주관하는 과장(문서 주관과)이 된다.

②통제관은 다음사항을 확인하여야 하며, 확인결과 미비사항이 있을 경우에는 처리과에서 보완하도록 하여 확인이 완료된 때에는 별지 제10호서식에 의한 통제인을 기안지의 발신명의인 좌측 여백에 날인한다.<개정 2002.10.8. 2004.6.19.>

1. 비밀의 분류표시 여부
2. 예고문
3. 비밀열람기록전의 유무
4. 배포선의 타당성 여부
5. 비밀분류지침에 의한 기준보다 과소 또는 과도분류 여부
6. 비밀의 복제 또는 복사 보안대책 여부

③제2항에 의한 통제를 받은 문서를 시행할 때에는 사무관리규정 제20조에 의한 문서심사를 받아야 한다.<개정 2002.10.8.>

제35조(비밀의 수발) ①비밀의 수발은 다음에 정하는 바에 의하여 수발함을 원칙으로 한다.

1. Ⅰ급비밀 : 암호화하여 전신 또는 취급자의 직접 접촉에 의하여 수발한다.
2. 암호자재(음어자재 포함) : 취급자의 직접 접촉에 의하여 수발한다.
3. Ⅱ급·Ⅲ급 비밀 : 등기우편에 의하거나 취급자의 직접 접촉 또는 암호(음어포함)화하여 전신으로 수발한다.

②비밀문서 수발은 각 기관의 문서담당과(계 포함)에서 한다.

③비밀문서의 발송은 비밀생산과에서 취급담당자가 직접 비밀원본 및 시행문을 지참하여 비밀문서통제관의 통제를 받은 다음 문서과(계)의 발송부에 기재한 후, 원본인수자 란에 서명날인하고 시행문을 문서과(계)에 인계한다.

④발송문서의 사송(접촉)에 의한 발송은 발송부 수령자 란에 수령자의 서명날인을 받고 교부하며 우송(등기발송)을 할 때에는 비밀영수증을 함께 보낸다.<개정 2002.10.8.>

⑤규칙 제30조제1항에 의한 비밀수발대장은 문서수발 담당부서에서 발송대장과 접수대장으로 구분 비치하고 다음과 같이 사용한다.

1. 비밀발송대장

각 주관과에서 비밀을 생산 또는 복제, 복사하여 대내·외로 발송되는 비밀(협조문포함)은 비밀등급에 관계없이 일련번호를 부여한다. 다만, 동일 건으로 수신처가 2개 이상일 때에는 동일한 발송번호를 부여하되 수신처별로 난을 달리하여 기록하여야 한다.

2. 비밀접수대장

대내·외로부터 접수되는 비밀은 비밀등급에 관계없이 일련번호를 부여하여 기록 접수한다.

⑥잘못 온 비밀은 반드시 발송기관에 반송하여야 하며 그 비밀문서를 받아야 할 기관으로 정정 반송할 수 없다.<개정 2002.10.8.>

제36조(대외비 수발) 대외비문서의 수발은 별지 제11호서식의 대외비문서 수발대장에 의한다.

제37조(영수증) ①비밀문서의 영수증 관리 및 작성은 각 기관의 문서담당과(계)에서 함을 원칙으로 한다. 다만, 업무의 형편에 따라 비밀생산과에서 작성할 수 있다.

②등기우편으로 발송할 때에는 발송부에 우편물 수령증 번호를 기재하고 우편물 배달증명서는 1년간 보관한다.<개정 2004.6.19.>

③비밀분류권자가 필요하다고 인정할 때에는 Ⅲ급 비밀 및 대외비도 영수증을 사용할 수 있다.

제38조(도상연습문서의 수발 및 보관) ①도상연습에 관련된 비밀문서 처리는 농림수산식품부 비상대비훈련예규에 의하되, 비밀문서 수발대장 및 영수증은 이미 비치되어 있는 것과는 별도로 작성하여 사용하여야 한다.<개정 2004.6.19.>

②도상연습에 관련된 비밀문서는 연습종료 후에 농림수산식품부 비상대비훈련예규에 의하여 처리한다.<개정 2004.6.19.>

제4절 비밀의 보관관리

제39조(비밀의 보관관리) ①비밀은 다음에 정하는 바에 의하여 보관한다.

1. Ⅰ급 비밀 : 장관실
2. Ⅱ급, Ⅲ급 비밀
   가. 농림수산식품부 : 각 실·국 주무과와 보안담당관이 필요하다고 인정하는 과. 다만, 장·차관실의 비밀문서는 운영지원과에 보관한다.<개정 2001.6.23.>
   나. 소속기관 : 보안업무담당과
   다. 산하단체 : 각 단체의 장이 정하는 부서에서 보관한다.

②대외비 문서는 각 과 단위로 보관함을 따로 설치하여 보관한다. 다만, 문서량이 적을 때에는 일반문서함에 별도의 장금장치를 하여 보관할 수 있다.<개정 2002.10.8.>

제40조(비밀보관 용기) ①비밀문서 보관용기는 금고 또는 철제의 이중 캐비넷을 이용하여야 하며 장금장치는 반드시 이중장치를 하여야 한다.
②보관용기의 외부에는 다른 사람이 알 수 있는 표지를 하여서는 아니된다.<개정 2004.6.19.>
③보관책임자는 비밀보관함의 열쇠 한 개와 캐비넷 번호 및 다이알 번호를 소속 보안담당관에게 제출하여야 하며, 보안담당관은 비밀 안전지출 및 파기계획에 의거 보관 관리한다.
④보관책임자는 보관함 열쇠(캐비넷 및 다이알 번호 포함)의 변동이 있을 때에는 즉시 보안담당관에게 연락하여 필요한 조치를 취하여야 한다.

제41조(비밀보관책임자) ①제39조에 의하여 비밀을 보관하고 있는 실·와의 책임자는 소관비밀의 정 보관책임자가 된다.
②제1항에 정한 각 정 보관책임자의 차하위직에 있는 자로서 보안업무를 담당하는 자는 부 보관책임자가 된다.
③소속기관 및 산하단체의 제1차 기관 또는 그 이하기관의 비밀보관 정·부책임자는 그 기관의 장이 정한다.
④보관책임자가 장기간 부재중이거나 결원일 때에는 부 책임자가 그 업무를 대행한다. 다만, 정·부 책임자가 모두 장기간 부재중이거나 결원중 일 때에는 정책임자의 직무를 대행하는 자가 제42조에 의한 인계인수를 하고 보관책임자가 된다.

제42조(보관책임자의 교체) ① 보관책임자가 교체되었을 때에는 차상위자의 입회하에 인계인수하되, 비밀관리기록부의 최종기록란에 다음사항을 기록하고 소속 보안담당관의 확인을 받아야 한다. 다만, 대외비문서의 인계인수는 분임보안담당관이 확인한다.
1. 인계인수 사유
2. 등급별 비밀건수
3. 인계인수 일자
4. 인계자 직위 성명 (인)
   인수자 직위 성명 (인)
   입회자 직위 성명 (인)
5. 확인자 보안담당관 성명 (인)
② 조직 통·폐합, 업무이관 등 직제변경으로 인한 보관책임자 교체시는 비밀관리기록부에 의한 인계·인수 이외에 세칙 제27조제2항의 인계·인수서를 작성하고 본부 보안담당관에게 보고하여야 한다.<신설 2009.4.3.>

제43조(비밀의 발간) ①비밀(대외비 포함)의 발간(인쇄, 공판, 프린트, 복제, 복사, 필경, 타자 등)은 보안상 자체시설을 이용함을 원칙으로 한다. 다만, 면수나 부수의 양 또는 제작기술상의 곤란 등 부득이한 경우에는 민간시설을 이용할 수 있다.
②민간시설을 이용하여 비밀을 발간하고자 할 때에는 비밀생산부서 과장이 별지 제12호서식에 의한 비밀문서 발간승인 신청서를 보안담당관에게 제출하여 통제조정과 승인을 받아야 한다.
③보안담당관은 제2항의 비밀발간승인 신청서를 검토하여 조달청장이 인가한 비밀발간업체에 발간의뢰토록 하여야 하며, 부득이 비밀발간인가업체가 아닌 민간시설을 이용하여 발간할 때에는 규칙 제37조제2항의 규정에 의하여 국가정보원장(또는 도지부장)의 보안조치를 받은 후 발간 의뢰한다.<개정 2001.6.23.>
④제3항에 따라 민간시설을 이용하여 비밀을 발간할 때에는 보안담당관이 별지 제13호서식에 의한 비밀문서 발간 통제대장을 비치하고 기록유지하여야 하며, 신청서에는 별지 제14호서식의 통제인을 날인한다.
⑤민간시설을 이용하여 비밀을 발간할 때에는 관계 비밀취급인가자가 작업과정을 항상 입회하여 모든 보안사항(원판 해제, 원지·작업지·파지 등의 소각, 나머지 분량 회수 등)을 감독관리하여야 하며, 발간문서의 끝 부분 또는 뒤쪽 겉장 안에 규칙 제37조제3항에 의한 표시를 하여야 한다.<개정 2004.6.19.>
⑥제1항에 의하여 비밀을 발간할 때에는 별지 제15호서식에 의한 비밀문서발간·복사작업일지를 비치하고 작업내용을 기록유지하여야 하며, 비밀생산과정에서의 초안지·파지·원지 등은 규칙 제14조의 요령에 의하여 파기하고, 파기수량·파기일시·파기자 성명을 기재 날인한다.
⑦워드프로세서 등 전산장비로 비밀문서(대외비 포함)를 생산할 때에는 농림수산식품부 정보통신보안기본지침에 의하여 관리하여야 한다.<개정 2004.6.19.>

제44조(중요 정책사업의 보안관리) ①중요 정책사업으로서 외부에 누설될 경우 국가안전보장에 유해하거나 국가통상외교 사항중 공개됨으로써 국익을 저해하는 사안 또는 중대한 사회적 물의가 예상되는 사안은 비밀로 관리한다.
②중요 정책사업으로서 외부에 누설될 경우 공익에 반하거나 사회적 물의가 예상되는 사안 또는 계획집행에 차질이 우려되는 사안은 대외비로 관리한다.
③제1항 및 제2항의 관리기준은 다음 각호의 사항을 고려하여 검토·결정한다.
1. 사전에 누설될 경우 예상되는 국가안전보장 및 국익 또는 사회적 물의의 정도
2. 사안이 이해 관계인에게 미치는 영향력 정도
3. 사안의 내용상 중요성 정도

제45조(중요정책사업의 외주용역에 따른 보안관리) ①대외비 이상으로 관리하는 중요 정책사업을 정부출연기관 또는 민간연구소, 대학 기타 연구용역기관·단체 및 개인과 연구·용

역계약(이하 “용역계약”이라 한다)을 체결하는 경우 동 계약서에 다음 각호의 사항을 명시하여야 한다.

1. 비밀 엄수 의무의 이행과 위계시 손해배상 등 책임감수
2. 보안관리책임자 및 연구·용역업무 참여자의 선정 및 인적사항 제출
3. 보안관리책임자 및 연구·용역업무 참여자에 대한 보안 준수사항 고지 및 서약집
4. 연구·용역 성과물과 각종 자료·원고 등의 임의 복사 및 파기 금지
5. 작업장소의 지정 및 동 장소에 대한 외부인의 출입통제 대책 강구
6. 작업에 동원되는 각종 단말기·컴퓨터·보조기억 장치 등 사무용 장비에 대한 보안관리 대책강구
7. 기타 용역의뢰 기관의 장이 보안상 필요하다고 인정하는 중요한 사항

②용역계약을 체결하는 부서의 장 또는 각급기관·단체의 장은 다음 각호의 보안관리 사항을 이행하여야 한다.

1. 용역사업 보안관리 책임자의 지정 및 연구수행과정에 대한 보안감독 수행
2. 용역종료시 성과물과 각종자료, 원고 등의 전량 회수 조치
3. 제1항제2호의 보안관리책임자 및 연구·용역 업무 참여자의 신원파악
4. 기타 연구용역 과정상 필요한 보안조치의 강구

③용역계약을 체결하는 각급기관의 보안담당관은 중요 정책사업의 연구용역 업무와 관련하여 산하 연구기관에 대하여 연1회 이상 보안교육 및 지도·점검 등 감독을 실시할 수 있다.

④각 연구기관의 장은 자체 보안업무시행세칙에 연구과제 외주용역 및 수탁연구에 따른 보안관리 조항을 규정하여야 하며, 보안담당관으로 하여금 관리하게 하거나 따로 비밀연구과제 보안관리 책임자를 지정·운영할 수 있다.

제46조(비밀정책·과제 연구관련 회의개최에 따른 보안관리) ①제42조에 해당하는 중요정책·회의자료 및 연구결과 발표자료는 적정등급의 비밀 또는 대외비로 분류하고 경고문을 삽입하여 배포하여야 하며 회의종료 후에는 전량 회수하여야 한다. 다만, 공문시행을 겸한 회의시에는 배포선을 작성하고 배부할 수 있다.

②비밀회의 참여자에 대하여는 회의개최 전에 미리 보안준수 사항을 고지하고 보안서약을 집행하여야 한다.

③비밀회의를 주관하는 부서의 장 및 기관·단체장은 불필요한 인원의 회의장 접근을 통제하고 각종자료의 유출방지대책을 강구하여야 한다.

제47조(복사의 통제) ①비밀(대외비 포함)문서는 원칙적으로 복사할 수 없다. 다만, 문서의 시행 등 공용에 사용하기 위하여 복사하고자 할 때에는 별지 제13호서식에 기재하고 규칙 제34조에 의하여 처리하여야 한다.

②제1항에 의한 복사는 당해 문서처리 담당자가 하고, 그 작업사항은 제43조제6항의 비밀문서 발간·복사작업일지에 기록하여야 하며, 해당 등급의 비밀취급인가를 받지 아니한 자에게 대행하게 하여서는 아니된다.

제48조(비밀의 분리취급) Ⅲ급비밀에 해당하는 첩보 및 정보와 같은 비밀문서중 관계취급자에게 분리취급하게 하였을 때에는 업무처리가 끝난 후에는 반드시 예고문에 의하여 종합처리하여야 한다.

제49조(보안조치) ①규칙 제37조제1항에 의하여 비인가자에게 비밀을 열람 또는 공개시키거나 취급하게 할 때에는 자체조치 할 수 있는 경우를 제외하고는 서울에 소재하는 기관은 국가정보원, 지방에 소재하는 기관은 관할 도지부장에게 통보하여 결과 통보를 받은 후 조치하여야 한다.<개정 2001.6.23.>
②제1항의 규정에 의하여 자체에서 조치할 수 있는 사항과 국가정보원(각 도지부 포함)의 조치를 받아야 할 사항은 다음과 같다.<개정 2001.6.23.>
1. 자체 조치사항
가. 도상연습(C.P.X)기간중 도상연습에 참가하는 소속 직원(최소한의 임원에 한함)
나. 비상안전지출 및 파기시 응급조치가 불가피할 때
다. 당직자가 제1항의 예에 따라 긴급한 조치를 할 때<개정 2004.6.19.>
2. 국가정보원에 통보 할 사항
가. Ⅲ급비밀이상의 중요 법안 또는 정책수립의 자문에 응할 자와 제1호 이외의 모든 사항
③대내 보안조치 요청절차중 제2항제1호 가에 해당하는 도상연습 요원은 소속과 직·성명·기간·장소·사유를 명시하여 보안담당관에게 요청한다.
④보안담당관은 제3항의 요청이 있을 때에는 인적사항 및 보안 등의 여러 가지 사항을 생각하여 검토한 후 기관장의 결재를 받은 후 승인한다.<개정 2004.6.19.>
⑤제2항제1호 나·다목의 경우에는 실시한 자가 실시사항을 경위보고 형식에 의거 보안담당관에게 제출하고 보안담당관은 보안상의 이상유무를 검토한 후 기관의 장에게 보고한다.<개정 2002.10.8. 2004.6.19.>
⑥국가정보원에의 보안조치 요청절차는 규정 제37조제1항의 사항을 기재하여 각 기관의 장이 직접 국가정보원(또는 도지부)에 요청함과 동시에 요청 사본을 농림수산식품부장관에게 제출한다. <개정 2001.6.23.>

제50조(비밀의 지출) ①비밀은 보관하고 있는 시설 밖으로 지출할 수 없다. 다만, 공무상 필요하여 지출하고자 할 때에는 규칙 제13호서식에 의하여 농림수산식품부는 실·국장, 소속

기관은 기관장, 산하단체는 이사 또는 상무의 승인을 받아 보안담당관을 경유하여 보관책임자에게 제출하고, 보관책임자는 보안대책을 확인한 후 지출할 수 있다.<개정 2001.6.23.>
②비밀을 발간하기 위하여 지출할 때에는 비밀문서발간승인서를 비밀지출승인서로 갈음한다.

제51조(비밀의 인계) ①규칙 제39조에 의하여 비밀을 소유하고 있는 기관이 해체 또는 개편될 때에는 소유비밀을 인수할 기관에 인계한다. 다만, 인수할 기관이 불명할 때에는 규칙 제39조제2항에 의한다.
②비밀을 인계할 때에는 비밀관리기록부 최종기록란 다음에 제41조에 준하여 인계인수하여야 하며 필요할 때에는 별도로 목록을 작성하여 인수기관에 교부할 수 있다.
③인계받은 비밀문서는 인계받은 기관에서 사용하는 비밀관리기록부에 의거 관리번호를 부여한다.

제52조(비밀관리기록부) ①규칙 제30조제1항에 의한 비밀관리기록부는 비밀보관 담당과(실·부)에 비치하여 다음과 같이 사용하여야 한다.
1. 생산 또는 접수한 비밀은 비밀등급별로 구분하여 그 순서에 따라 기록 유지하고, 관리번호를 부여할 때에는 규칙 제31조제3항에 의한 관리번호 표시를 하여야 한다.
2. 관리번호 부여는 접수문서일 때에는 접수순위에 의하여 부여하고 생산문서일 때에는 최종 결재권자의 결재를 받은 후 내용이 확정된 때에 부여하여야 한다.
3. 동일 건의 비밀을 2부이상 접수 또는 보관하고자 할 때에는 매 건마다 관리번호를 부여하여야 한다.
4. 비밀을 파기, 이송 또는 일반문서로 재분류하였을 때에는 비밀관리기록부의 비밀등급란부터 사본란까지 2개의 붉은 선을 그어 표시하되 원문을 해독할 수 있도록 하여야 한다.<개정 2002.10.8.>
②비밀관리기록부를 갱신하고자 할 때에는 구 관리기록부 끝 부분란 및 신규 관리기록부 첫머리에 등급별 건수, 옮겨 쓴 연·월·일을 기재하고 보관책임자의 서명날인과 보안담당관의 확인 서명날인을 받아야 한다.<개정 2002.10.8.>
③신규 관리기록부에 이기하는 비밀은 관리번호를 새로이 부여하되, 구 관리기록부 근거란에 새로이 부여한 관리번호와 옮겨 쓴 연·월·일을 기재하고 옮겨 쓴 자가 날인하되 제1항제4호와 같이 처리한다.

제53조(안전지출 및 파기계획) 비밀의 안전지출 및 파기5계획은 각 기관에 따라 실정에 부합되도록 작성하여야 하며 규칙 제40조의 필요사항을 포함시켜야 한다.

제54조(비밀의 파기시설) 각 기관은 비밀의 파기시설을 갖추어 이용하여야 한다.

제55조(비밀관리부철의 보존) ①규칙 제68조 및 다음에 정하는 각 부철 보존기간은 그 사용기간이 끝난 다음 해 1월 1일부터 기산하여 해당 연도의 12월31일까지로 하며 보존기간중에 폐기하고자 할 때에는 농림수산식품부장관의 승인을 받아야 한다.<개정 2002. 10.8.>

1. 신원대장	5 년
2. 신원특이자 명부	영 구
3. 신원조사관계철	5 년
4. 신원특이자 동향기록부	5 년
5. 비밀취급인가증 교부대장	5 년
6. 비밀취급인가관계철	3 년
7. 비밀소유현황 및 비밀취급인가자 현황	3 년
8. 음어자재관리기록부	5 년
9. 음어자재점검관계철	5 년
10. 음어자재증명서철	5 년
11. 보안감사관계철	5 년
12. 비밀발간·작업일지	5 년
13. 비밀발간·복사승인관계철	5 년
14. 비밀문서 수발대장 및 영수증	5 년
15. 보안교육관계철	3 년
16. 보안업무 서무관계철	3 년

②제1항에서 정한 부철 이외의 비밀관리부철은 공공기관의기록물관리에관한법률에 따른다.<개정 2004.6.19.>

제5절 시설보안

제56조(보호구역) ①각 기관의 장은 국가비밀의 보호와 중요시설·장비·자재 및 정부재산의 보호를 위하여 규정 제30조 및 규칙 제42조 내지 제44조에 의한 보호구역을 설정하여야 한다.

②소속기관 및 산하단체의 장은 제1항에 의하여 보호구역을 설정, 변경 또는 폐지하였을 때에는 즉시 농림수산식품부장관에게 보고하여야 한다.<개정 2001. 6.23.>

③농림수산식품부 보호구역은 다음과 같다.<개정 2001.6.23.>

1. 제한구역 : 종합상황실, 통신실, 전산실
2. 통제구역 : 전시종합상황실, 국가지도통신실, 국협외교전문실, 암호장비실, 변전실, 저유탱크 또는 위험물 저장소, 보안장비가 설치된 장소 <개정 2001.6.23.>

제57조(보호구역의 책임관리) ①제한 및 통제구역의 각종 재산에 대한 책임은 기관의 장이 지며 보관단위별 책임자는 해당 과장, 부책임자는 그 하위직에 있는 (보호구역관리담당)자가 된다.
②보호구역의 총괄통제는 소속 보안담당관이 담당한다.
③보호구역 방호는 각 기관별 방호계획에 의하여 시행한다.

제58조(보호구역의 보안대책) ①보호구역의 출입문은 단일로 하고 외부로부터 투시가 불가능(다만, 전산실 등 통제구역 안에 설치된 경우 제외)하도록 하는 동시에 도청 및 파괴물질의 투척 등을 방지할 수 있도록 철망·철격자 또는 이와 같은 수준의 성능이 있는 시설물을 설치하여야 한다.<개정 2004.6. 19.>
②통제구역은 관계자 외의 접근을 막기 위하여 출입문 적절한 곳이나 해당 주무과 또는 수위실·경비실 및 당직실 간에 경보장치를 설치하여야 한다.<개정 2004.6.19.>
③보호구역에는 소화전, 방화수, 방화사 등 화재예방 기구를 비치하여야 한다.

제59조(보호구역 출입자 통제) ①제한구역에 근무하는 자와 담당자는 당해 구역의 출입을 인가한 것으로 보며, 그밖의 구역에 출입하고자 할 때에는 그 구역 책임자의 승인을 받아야 한다. 다만, 통제구역은 농림수산식품부의 경우 당해 구역의 실·국장의, 소속기관은 기관장의, 산하단체는 당해 구역의 실·처장의 승인을 받아 출입하여야 한다.<개정 2002.10.8.>
②외부인은 보호구역을 출입할 수 없도록 통제하여야 하며, 출입이 필요하다고 인정되는 경우에는 해당 책임자의 승인을 받아 관계직원이 같이 다녀야 하며, 통제구역은 소속 보안담당관을 거쳐 농림수산식품부는 당해 구역의 실·국장의, 소속기관은 기관장의, 산하단체는 당해 구역의 실·처장의 승인을 받아 출입하되 관계직원이 같이 다녀야 한다.<개정 2002.10.8.>
③제55조에 의한 보호구역 관리책임자는 별지 제16호서식에 의한 보호구역 출입자 통제대장을 비치하고, 관리책임자의 사전승인을 받은 후 출입하도록 한다.

제60조(일반출입자 단속) 시설의 안전보호를 위하여 보안담당관은 다음 사항을 담당한다.
1. 공무이외의 청사 내 출입을 최대한으로 제한하여야 하며 잡상인의 출입은 억제하여야 한다.
2. 일과중에는 보안담당부서에서 출입자를 확인하고(정문 또는 현관에서 별지 제17호서식에 의한 방문기록부에 기록한 후) 주민등록증 등 신원을 증명하는 증서와 별지 제18호서식의 방문증을 교환하여 달게한 후 출입하도록 하여야 하며, 일과 후의 내방자는 당직책임자가 신원을 확인한 후 당직일지에 기록하여 다음 날 보안담당부서장에게 보고하여야 한다.<개정 2002.10. 8.>
3. 각과 최종퇴청자는 퇴근시 사무실의 보안상태를 확인하고 별지 제19호서식의 보안점검표 또는 전산장비에 점검결과를 기록유지 하여야 한다.

제61조(당직자의 유의사항) ①당직자는 당직 규정(각 기관의 규정)을 준수하고 일과근무시간 종료 30분 전에 보안담당부서장에게 당직신고를 하여야 하며, 보안담당부서장은 매일 당직책임자에게 당직자의 준수사항을 지시하여야 한다.
②당직근무중에 비상사태나 보안사고가 발생하였을 때에는 비상연락계통도에 의거 기관장 및 보안담당관에게 보고하고 기관장 및 보안담당관의 명령에 의거 처리할 것이며, 명령을 기다릴 수 없는 긴박한 사태에 처하였을 때에는 당직함에 비치된 안전지출 및 파기계획에 의거 비밀을 처리하고 그 결과를 소속기관의 장 또는 보안담당관에게 보고하여야 한다.

제62조(보안 및 화기단속) ①각종 시설물 또는 각 사무실에는 보안 및 화기단속책임자를 둔다.
②보안 및 화기단속책임자는 해당 시설이나 사무실의 주무과장이 되고 부책임자는 그 하위직자가 되며 사무실 및 시설물의 출입문 눈 높이에 다음과 같은 관리책임자 표지를 부착한다.

16cm

보안 및 화기 단속책임자		4cm
정		3.5cm
부		3.5cm

11cm

제63조(보호구역의 표시) 보호구역에는 별지 제20호서식의 표지를 각 구역출입문 중앙부 눈높이에 부착 유지한다. 다만, 통제구역은 보안상 불이익하다고 인정할 때에는 부착하지 아니할 수 있다.

제6절 보안조사

제64조(보안사고) 보안사고의 범위를 다음과 같이 한다.
1. 암호·음어자재의 오인 소각·소실·분실·누설
2. 암호·음어자재 오손
3. 비밀문서 분실 및 도난과 누설
4. 비밀문서의 오손 및 부당 파기
5. 재해(화재·수해)에 의한 비밀문서의 소실 및 유실
6. 무기 및 탄약분실 또는 도난
7. 중요 기자재 및 시설의 파괴
8. 비밀문서 또는 암호(음어자재)영수증 분실 및 오손

제65조(보안사고 보고) ①보안사고를 발견하거나 알게 된 자는 즉시 관계 담당자 또는 보안담당관에게 보고하고, 보고를 받은 자는 제64조제1항제1호 및 제2호의 사고를 제외하고는

1차적으로 소속기관의 장에게 보고하여야 하며, 그 기관의 장은 농림수산식품부장관에게 보고하여야 한다.<개정 2002.10.8.>
②제64조제1호 및 제2호의 사고가 발생하였을 때에는 발견과 동시에 규칙 제51조에 의한 조치를 하여야 한다.
③보안사고는 전말조사가 종결될 때까지 외부에 누설 또는 감지되지 않도록 보안조치를 하여야 한다.
④보안사고를 보고하지 아니하거나 은익한 자는 관계법규에 의하여 징계 조치한다.
⑤비밀을 분실하였거나 누설하였을 때에는 그 비밀의 발행기관 및 배포기관에 통보하여야 한다.
⑥보안사고 보고시에는 기관명, 사고내용, 사고전말, 조치사항, 기타 참고사항 등이 포함되어야 한다.

제7절 통신보안

제66조(음어자재 수령 및 배부) ①음어자재는 농림수산식품부장관이 국가정보원장으로부터 수령하여 농림수산식품부 각 실·국 및 각 기관에 배부한다.<개정 2001.6.23.>
②음어자재를 배부받은 기관은 사용기간 만료일로부터 3일째 되는 날(공휴일인 경우에는 그 다음날)에 농림수산식품부장관에게 반납한다.<개정 2001.6.23.>

제67조(음어자재 운영) 음어자재는 비밀취급인가를 받은 자는 누구나 취급할 수 있으나 해독·조립한 음어문은 원문과 같이 보관할 수 없으며, 사용 즉시 소속 과장 또는 해당 보관책임자의 입회하에 파기하여야 한다.

제68조(음어자재 보관관리) 음어자재는 각 기관 실정에 맞는 보관함을 별도로 제작하여 비밀문서보관함에 보관하되 현재용은 서류 편철지에, 미래용 및 과거용은 각각 포장 봉인하여 보관하여야 하며, 일반문서 보관함에 보관하여서는 아니된다.

제8절 보칙

제69조(보안감사) ①보안업무의 지도와 효율적인 운용개선을 위하여 농림수산식품부장관은 보안담당관으로 하여금 연 1회이상 각 기관에 대하여 보안감사를 실시한다. 다만, 보안감사의 내실화를 도모하기 위하여 감사대상 전 기관을 반으로 나누어 격년제로 실시할 수 있으며, 필요하다고 인정할 때에는 수시로 보안감사를 실시할 수 있다.<개정 2002.10.8.>
②소속기관 및 산하단체의 장은 연 1회 자체보안감사(제1차 및 제2차 소속기관 포함)를 실시하

고 감사 종료 후 20일 이내에 그 결과를 농림수산식품부장관에게 보고하여야 한다.<개정 2001.6.23.>
③감사반의 편성은 보안담당 부서에서 Ⅱ급이상 비밀취급인가를 받은 자로 편성하되, 필요한 경우에는 관계직원을 차출할 수 있다.<개정 2001.6.23.>
④자체감사 결과 지적된 사항에 대하여는 20일 이내에 시정 조치하여야 한다.<개정 2002.10.8.>

제70조(보안교육) ①규칙 제67조에 의하여 각 기관의 보안담당관(분임보안담당관)은 소속직원 전원에 대하여 연 1회 이상 정규 및 수시교육을 실시하여야 하며, 특히 신규임용자 및 전입자에 대하여는 임용과 동시 다음 사항의 보안교육을 실시하여야 한다.<개정 2002.10.8.>
1. 보안업무규정
2. 보안업무규정 시행규칙
3. 보안업무시행세칙
4. 정보통신보안 기본지침<개정 2001.6.23.>
5. 국가지리정보 보안관리규정<신설 2001.6.23.>
②각 기관의 보안담당관은 해외여행자에 대하여 사전에 보안 교육을 시켜야 한다. 다만, 필요하다고 인정할 때에는 관계공무원 또는 전문가에게 위탁할 수 있다.

제71조(해외주재관에 관한 보안업무 지침) ①해외에 공무로 일정기간 상주하여 근무하는 농림수산식품부 주재관과 소속기관 및 산하단체에 이에 준한 직원은 외교통상부장관이 정한 지침 이외의 모든 비밀 및 대외비 문서를 처리함에 있어서는 이 내규의 정하는 바에 의한다.<개정 2001.6.23.>
②제1항의 해외 상주자는 출국 전 소속기관장으로부터 Ⅱ급 비밀취급인가를 받아야 하며, 소속기관 보안담당관의 보안교육(규정·규칙 및 세칙)을 받아야 한다.
③국제농업국장은 보직과 동시 농림수산식부품부 국외정보업무 조정담당관이 되며, 담당관은 국외정보업무 조정규정에 관한 업무를 담당한다.<개정 2001.6.23.>

제72조(국회 등 대외기관에 대한 자료 제출) ①국회 및 다른 기관으로부터 비밀문서의 내용이 포함된 자료의 제출을 요구받았을 경우에는 미리 보안성 검토를 실시하고, 최소 부수만을 제공하되, 열람 후 회수 또는 반납일자를 분명하게 기록하여야 한다. 이 경우 자료제출 창구는 국회담당부서로 일원화 하고 정식 공문으로 접수·제출하여야 한다.<신설 2004.6.19.>

②외국인 또는 외국기관에 자료를 제공하고자 할 경우에는 비밀보관 정책임자는 심사위원회의 토의에 부치어 그 자료에 대한 사전 보안성 검토, 제공 목적과 용도, 외국인 국적과 지위 등을 세밀히 검토한 후 승인하여야 하며, 제공된 자료의 목록을 자세히 기록·유지하여야 한다.<신설 2004.6.19.>
③제1항 및 제2항에서 정하지 아니한 사항은 "농림수산식품부 외국기관(인원)면담및자료제공 지침"에 따른다.<신설 2004.6.19.>

제73조(보안업무 세부시행계획 수립 및 집행) ①농림수산식품부 보안담당관은 국가정보원으로부터 통보받은 보안지침에 의거 자체보안실무지침을 작성하여 각 실·국, 소속기관 및 산하단체에 시달하여야 한다.<개정 2001.6.23.>
②제1항의 보안지침에 의하여 각 실·국 및 분임보안담당관은 자체보안업무 세부시행계획을 별지 제21호서식에 따라 작성하여 보안담당관에게 제출하고, 소속기관 및 산하단체는 자체실정에 맞는 보안업무 세부시행계획을 수립하여 시행하여야 하며, 농림수산식품부장관에게 제출하여야 한다.<개정 2001.6.23.>

제74조(자체보안진단) ①각 기관의 보안담당관은 매월 세째주 수요일을 사이버·보안 진단의 날로 정하여 자체보안진단을 실시하여야 한다.(단, 매월 세째주 수요일에 보안진단이 불가능할 때에는 화요일에 실시한다.)<개정 2009.4.3.>
②보안진단의 날에 구체적으로 시행하고 확인할 사항은 다음과 같다.
1. 보안교육 실시
2. 비밀취급인가자 현황파악 및 조정 필요성 검토
3. 비밀소유현황조사 및 재분류 검토
4. 음어자재·암호장비 보유 및 관리 상태 <개정 2009.4.3.>
5. 외래 출입통제 강화(공무 외 출입금지)
6. 출입증 발급현황과 소유실태조사(공무원·민간인 등)
7. 경비·수위요원에 대한 교육훈련 실시
8. 비상연락망 정비
9. 공무통화의 음어화 조치와 사용통화 제한
10. 실내단속 상태
   가. 창문·출입문·캐비넷·책상 고장여부
   나. 소화기 사용 가능여부
11. 정보보안 관리실태 <개정 2009.4.3.>
12. 기타 분야별 요소별 보안관리상태 전반

③보안진단 결과 나타난 문제점은 즉각 시정하고 관계기관의 협조가 필요할 때에는 관계기관에 통보 또는 협조요청을 하여야 한다.
④보안담당관은 기관 내 보안진단 결과를 종합하고 문제점에 대한 해결요청이 있을 때에는 이를 해결하여야 한다.

제75조(보안업무 심사분석) ①보안담당관은 보안업무의 효율적인 관리를 위하여 보안업무 심사분석을 실시하여야 한다.<개정 2001.6.23.>
②보안업무 심사분석은 각 기관의 보안담당관 책임하에 실시하고 다음 사항에 대한 실적을 파악, 문제점을 발굴하고 이에 대한 시정책을 강구한다.
1. 연간 보안업무 및 세부시행계획에 대한 구체적 시행 사항
2. 자체 보안교육 및 보안감사 점검에 관한 사항
3. 보안심사위원회 개최와 실적에 관한 사항
4. 비밀소유현황 및 비밀취급인가자 증감에 관한 사항
5. 부서별 업무분야별 보안대책에 관한 사항
6. 기타 보안활동 전반에 관한 사항
③농림수산식품부 각 실·국 및 분임보안담당관, 소속기관 및 산하단체는 제2항의 보안업무 심사분석 결과를 매년 보안업무 추진계획에 따라 농림수산식품부 보안담당관에게 제출하여야 한다.<개정 2001.6.23.>

부 칙 (2001. 6. 23.)
이 훈령은 발령한 날로부터 시행한다.

부 칙 (2002. 10. 8.)
이 훈령은 발령한 날부터 시행한다.

부 칙 (2004. 6. 19.)
이 훈령은 발령한 날부터 시행한다.

부 칙 (2008. 5. 20.)
이 훈령은 발령한 날부터 시행한다.

부 칙 (2009. 4. 3.)
이 훈령은 발령한 날부터 시행한다.

【별지 제1호서식】

보안심사위원회 심의 의결서

– 년도 제 차 심의회 –

년도 (안건내용) 심의 안건에 대하여 붙임 의결주문과 같이 의결한다.

20 . . .

농림수산식품부보안심사위원장

구 분	직 위	성 명	심의의견		서 명	비고
			가(可)	부(否)		
위원장						
부위원장						
위원						
간사						

의결 년월일	. . .

의결사항

농림수산식품부 보안심사위원회 안건

- 안 건 내 용 -

제 출 자
농림수산식품부 보안심사위원회 위원장

보안심사위원회 심의 의결서

1. 의결 주문

2. 제안 사유

3. 근　거

4. 그 밖의 필요사항

【별지 제2호서식】

보안심사위원회 회의록

1. 일시 및 장소 :

2. 참 석 위 원 :

3. 안　　건 :

4. 의 결 내 용 :

5. 발 언 요 지 :

○ 00위원 :

○ 00위원 :

위와 같이 기록함

년　월　일

운영지원과장(간사)　　서명

[별지 제3호서식]

신 원 대 장

연번	직 급	직 위	성 명	신 원 조 사			임용 또는 전입 일자	비고
				목 적	의뢰 일자	회보 일자		

[별지 제4호서식]

비밀취급(인가, 등급변경, 해제)신청서

분류기호 : 20 . . .

수 신 : 운영지원과장 발신 : 실·국장 (인)

아래와 같이 비밀취급인가를 (인가, 등급변경, 재발급, 해제) 신청하오니 조치하여 주시기 바랍니다.

<table>
<tr><td rowspan="2">인 적
사 항</td><td>소 속</td><td></td><td>직 급</td><td colspan="2"></td></tr>
<tr><td>성 명</td><td></td><td>주민등록번호</td><td colspan="2"></td></tr>
<tr><td>담당직무</td><td colspan="2"></td><td>인가등급</td><td colspan="2">급</td></tr>
<tr><td>사 유</td><td colspan="5">※ 구체적으로 기재</td></tr>
<tr><td rowspan="2">기타
사항</td><td rowspan="2">비밀취급
인가경력</td><td>급수 : 급</td><td rowspan="2">과내 비밀취급
인가자 현황</td><td>Ⅱ급 명</td><td>Ⅲ급 명</td></tr>
<tr><td>기간 :</td><td colspan="2">암호자재 명</td></tr>
<tr><td rowspan="3">심 사</td><td colspan="2">신원조회결과</td><td colspan="3"></td></tr>
<tr><td colspan="2">보안담당관 의견</td><td colspan="3"></td></tr>
<tr><td colspan="2">심사결과</td><td colspan="3"></td></tr>
</table>

년 월 일

조 사 자 : 직/성명 (인)

보안담당관 : (인)

첨부 1. 서약서 1부.(규칙 별지 제1호서식)

2. 신원조사회보서.(해당자에 한함)

3. 암호자재인 경우 암호의 종류 등 인가권자가 알아야 할 사항

제2편

[별지 제5호서식]

서 약 서

본인은 년 월 일자로 퇴직함에 있어 재직 중 지득한 일체의 비밀(대외비 포함) 또는 중요정보 사항이 국가안전보장에 중대한 사항임을 명심하고 이를 누설하지 아니할 것이며, 이를 위반했을 때에는 동기여하를 막론하고 그 결과가 이적 또는 반국가적 행위임을 자인하여 어떠한 처벌도 감수 할 것을 서약합니다.

년 월 일

서약자 소 속 : 직 급 :

성 명 : (인)

귀하

[별지 제6호서식]

비밀취급인가(해제)대장

소 속 :

연번	인가 번호	발 급 년월일	소속	직급	성명	주민등록 번 호	비밀 등급	발급 구분	해 제		수령 자인	결 재	
									일자	사유		담당	과장

[별지 제7호서식]

기 관 명

수 신 : 농림수산식품부장관 20 . . .

참 조 : 운영지원과장

제 목 : 비밀취급인가특례보고

농림수산식품부 보안업무시행지침 제24조제2항에 의거 아래와 같이 비밀취급을 인가하였기 보고합니다

소 속	직 위	성 명	인가등급	인가일자	인가의 필요성	비 고

끝.

(발 신 기 관 명)

[별지 제8호서식]

비밀취급인가자현황 조사서

(　　년　　월　　일 현재)

기 관 명	비 밀 등 급				비 고
	Ⅰ 급	Ⅱ 급	Ⅲ 급	계	

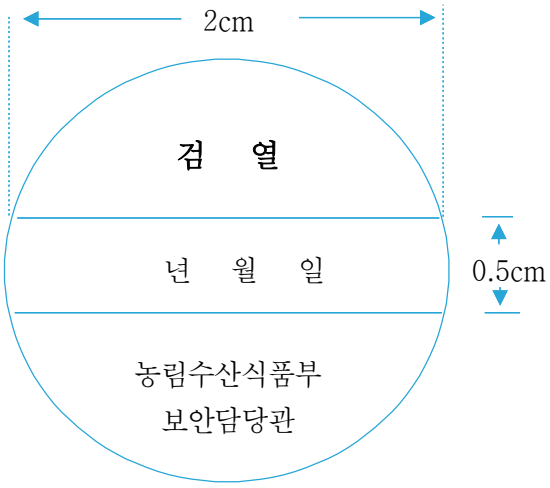
[별지 제9호서식]

비밀소유 및 취급인가자 현황 조사서

월일	조자사 서 명	확인자 서 명	Ⅱ급				Ⅲ급				계				인 가 자			
			이월	생산 접수	파기 (이송)	현보 유량	이월	생산 접수	파기 (이송)	현보 유량	이월	생산 접수	파기 (이송)	현보 유량	Ⅰ급	Ⅱ급	Ⅲ급	계

[별지 제10호서식]

비밀문서통제관인



[별지 제11호서식]

대외비문서 수발대장

번호	년 월 일	분류번호	발 신	수 신	제 목	수량	원 본 인수자	수령자 (인)

[별지 제12호서식]

비밀(대외비) 문서 발간(복사) 승인신청서

분류번호 :

수 신 : 20 . . .

아래와 같이 비밀(대외비)문서 발간(복사)코자 하오니 승인하여 주시기 바랍니다

발간(복사) 장 소	명 칭	(전화 :)			대 표 자	
	주 소				비밀취급	
제 목					비밀등급	
발간(복사) 일 시	20 . . . ~ 20 . . .(일간)					
발 간(복사) 수 량	신청	면~ 면 매 부	사정	면~ 면 매 부	구분	프린터, 공판, 인쇄, 복사, 기타( )
자 체 보안대책						
입 회 자	비밀취급 인가등급	급	직 급		성 명	(인)
배 포 선						

신 청 자 직/성명 (인)

보관책임자 과장(담당관) (인)

위의 비밀(대외비) 문서의 발간(복사)을 승인 함.

20 . . .

농림수산식품부 보안담당관 (인)

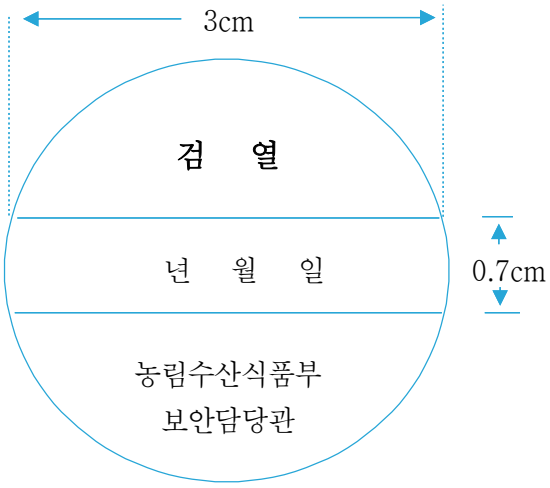
[별지 제13호서식]

비밀(대외비) 문서 발간(복사) 통제부

일련 번호	년월일	문서번호	제 목	등급	발간 종별	수량	발간 장소	의뢰과	입회자

[별지 제14호서식]

비밀문서통제관인



[별지 제15호서식]

비밀(대외비) 문서 발간(복사) 작업일지

구분 / 월일	발간대상 비밀				발간 또는 작업자			원지 및 파지처리(입회자)				비고
	제 목	등급	작업 종별	수량	소속	성명	비취인가 등 급	소속	성명	비취인가 등 급	처리수량 및 방법	

※ 작업종별은 타자, 필경, 복사, 프린트, 공판 등으로 구분

[별지 제16호서식]

보호구역(제한·통제) 출입자 통제대장

□ 보호구역명 :

연월일	출 입 자			출입시간 부터~까지	용 무	입 회 자			결 재
	소속	직급	성명			소속	성명	서명	
				: ~ :					
				: ~ :					
				: ~ :					
				: ~ :					
				: ~ :					
				: ~ :					
				: ~ :					

[별지 제17호서식]

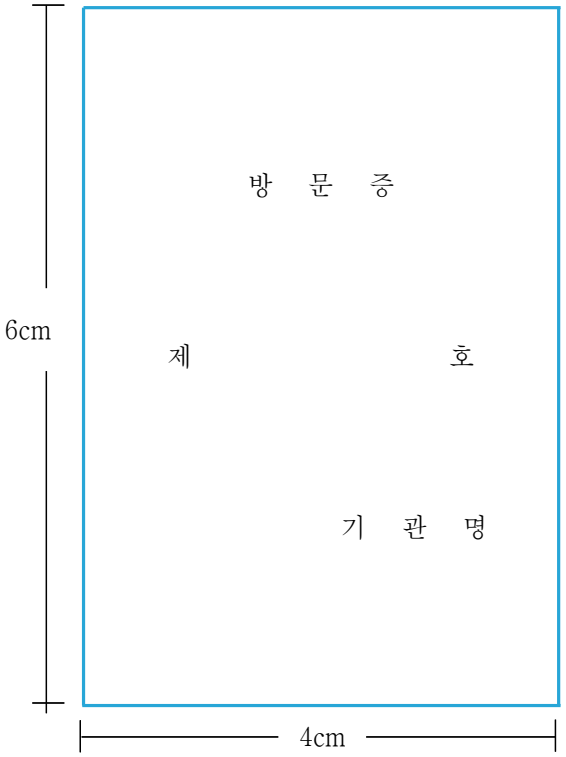
방 문 기 록 부

년 월 일	성 명	주민등록번호	방문 부서	용 무	방문시간	방 문 자 전화번호	출입증 번호	결 재 서 무 담 당
					시 분부터 시 분까지			
					시 분부터 시 분까지			
					시 분부터 시 분까지			
					시 분부터 시 분까지			
					시 분부터 시 분까지			
					시 분부터 시 분까지			
					시 분부터 시 분까지			
					시 분부터 시 분까지			
					시 분부터 시 분까지			
					시 분부터 시 분까지			

[별지 제18호서식]

방 문 증

(전 면)



(후 면)

준 수 사 항

1. 본 증을 패용할 것.
2. 퇴청시 반납할 것.
3. 당일에 한하여 유효함.
4. 타인에게 대여하지 못함.

기관장명

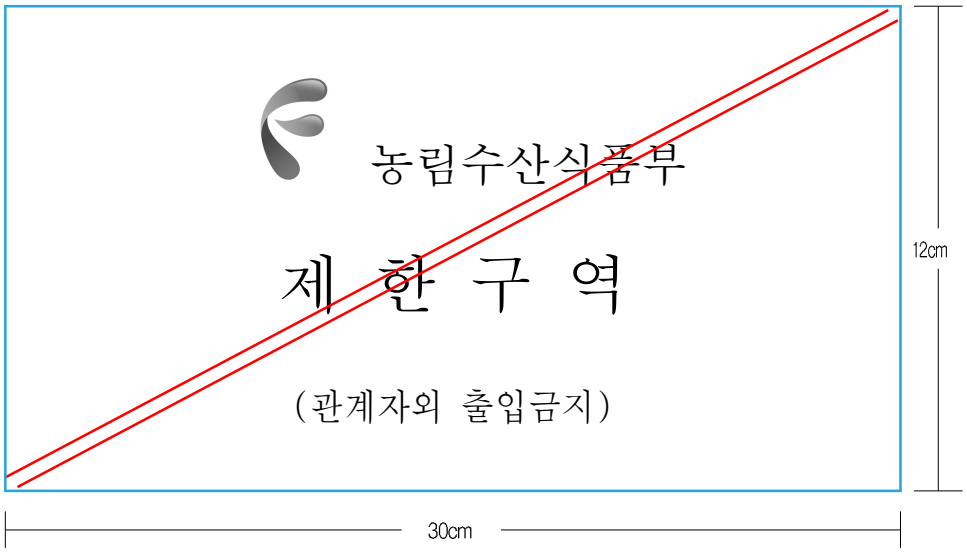
[별지 제19호서식]

보호구역(제한·통제) 출입자 통제대장

실·과명 :

구분 / 점검일	①서류보관상태		②청소상태		③소등상태		④화기단속상태		⑤문단속상태		⑥비고	점검시각 및 점검자				결재
												최종퇴청자		당직근무자		
	최종퇴청자	당직근무자	최종퇴청자	당직근무자	최종퇴청자	당직근무자	최종퇴청자	당직근무자	최종퇴청자	당직근무자		점검시각	성명	점검시각	성명	

[별지 제20호서식]



※ 제한구역(통제구역)에 비인가자 출입시는 보안담당관이 지정하는 안내원 입회

[별지 제21호서식]

년 보안업무 세부시행계획

Ⅰ. 목표(기관별 실정에 부합되는 보안활동 기본목표)

Ⅱ. 기본방침(연간 실시할 주요업무의 기본방침 제시)

Ⅲ. 세부지침

Ⅳ. 세부활동계획

분 야 별	사 업 명	세부추진내용	주관 및 관련부서

② 농림수산식품부 정보보안지침

제정 1997. 3. 5. 농 림 부 훈령 제 891 호
전문개정 2000. 2.26. 농 림 부 훈령 제1018호
전문개정 2007. 2.21. 농 림 부 훈령 제1264호
전문개정 2008. 4.29. 농림수산식품부 훈령 제 5 호

제1장 총 칙

제1조(목적) 이 지침은 보안업무규정 및 동 시행규칙과 농림수산식품부 보안업무내규, 국가정보원의 관련 지침에 의거 정보보안 활동에 필요한 세부사항 규정을 목적으로 한다.

제2조(적용범위) 이 지침은 농림수산식품부 본부 및 소속기관·산하단체(이하 '각급기관'이라 한다)에 적용한다.

제3조(정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다

1. "정보통신망"이라 함은 유·무선을 매개로 하는 다양한 정보통신 수단에 의하여 부호·문자·음향·영상 등의 정보를 수집·가공·저장·검색·송수신하는 정보 통신체제를 말한다.
2. "정보보안" 또는 "정보보호"라 함은 정보통신수단으로 수집·가공·저장·검색·송수신되는 정보의 유출·위변조·훼손 등을 방지하거나 정보통신망을 보호하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위를 말한다.
3. "국가용 정보보안시스템(이하 '보안시스템'이라 한다)"이라 함은 국가정보원장(이하 '국정원장'이라 한다)이 기밀 등 중요자료를 보호하기 위하여 승인한 암호장비·암호자재 또는 암호논리·사이버안전기술이 적용된 프로그램이나 장치 등을 말한다.
4. "보안적합성 검증필 정보보호시스템(이하 '검증필 정보보호시스템'이라 한다)"이라 함은 상용 정보보호시스템 중 국정원장이 각급기관에서 사용하는 것이 적합하다고 승인한 것을 말한다.
5. "암호논리"라 함은 자료의 누설, 위·변조, 훼손방지를 위하여 기밀성·무결성·인증·부인봉쇄 등의 기능을 제공하는 프로그램을 말한다.
6. "암호장비"라 함은 정보통신수단으로 처리·저장·송수신되는 정보를 보호할 목적으로 암호논리를 내장하여 제작된 장비나 장치를 말한다.
7. "암호자재"라 함은 Ⅱ급비밀 이하의 통신내용 및 정보자료를 비닉할 목적으로 사용하는 문자·숫자·기호 등으로 구성된 환자표와 난수 또는 암호논리 등을 저장한 문서나 도구를 말한다.

8. “음어자재”라 함은 Ⅲ급비밀 이하의 통신내용 및 정보자료를 비닉할 목적으로 사용하는 문자·숫자·기호 등으로 구성된 환자표와 난수 또는 암호논리 등을 저장한 문서나 도구를 말한다.
9. “약호자재”라 함은 대외비 이하의 통신내용을 비닉할 목적으로 특정 용어를 문자·숫자·기호 등으로 변환하여 수록한 문서나 도구를 말한다.
10. “암호취급자”라 함은 암호취급인가를 받아 암호체계를 연구·제작·수발하거나 국가용 보안시스템을 취급 관리하는 자를 말한다.
11. “정보통신실”이라 함은 서버·PC 등 전산장비와 스위치·교환기·라우터 등 통신 및 전송장비 등이 설치 운용되는 장소를 말하며, 전산실·통신실 및 전산자료 보관실 등을 말한다.
12. “전산자료”라 함은 전산장비에 의하여 전자기적인 형태로 입력·보관되어 있는 각종 정보(data)를 말하며, 그 자료가 입력되어 있는 자기테이프, 디스크 등 보조기억매체를 포함한다.
13. “정보보안측정”이라 함은 해킹·컴퓨터바이러스, 도청 등 각종 위협요소로부터 정보통신망에 대한 정보보안 취약성을 진단하기 위한 제반활동을 말하며, 대도청(對盜聽)측정 활동을 포함한다.
14. “대도청측정”이라 함은 도청탐색장비 등을 이용하여 은닉된 도청장치 색출 등 각종 도청 위해요소를 제거하는 보안활동을 말한다.
15. “국가용 보안시스템 제작업체(이하 ‘제작업체’라 한다)”라 함은 국가용 보안시스템의 제작권을 획득한 업체를 말한다.
16. “현장시험”이라 함은 개발 중인 국가용 보안시스템을 일정기간 동안 실제 운용중인 정보통신시스템 또는 정보통신망에 설치하여 미비점을 보완하기 위한 시험을 말한다.
17. “보조기억매체”라 함은 디스켓·CD·하드디스크·USB 메모리 등 자료를 저장할 수 있는 것으로 정보통신시스템과 분리할 수 있는 기억장치를 말한다.
18. “사이버공격”이라 함은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법 침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 말한다.
19. “사이버안전”이라 함은 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 말한다.
20. “보조기억매체 관리책임자”라 함은 각 팀 또는 과별 보조기억매체 관리상의 책임을 맡은 그 팀장·과장·담당관을 말한다.
21. “보조기억매체 취급자”라 함은 해당 보조기억매체를 사용하는 자를 말한다.
22. “보조기억매체 관리시스템”이라 함은 보조기억매체의 등록, 파기, 재사용, 반출·입, 불용처리 현황 등에 관하여 전자적으로 처리하는 시스템을 말한다

23. '보조기억매체 관리번호'라 함은 사용 중인 보조기억매체의 식별 및 관리를 용이하게 하기 위하여 부여한 번호를 말한다.
24. 공인인증서보관용 보조기억매체 중 '업무용' 이라 함은 업무와 관련 하여 신분확인 등에 활용되는 것을 말한다.
25. 공인인증서보관용 보조기억매체 중 '개인용' 이라 함은 인터넷 뱅킹 등 사적인 목적으로 활용되는 것을 말한다.
26. "저장매체"란 자기저장장치 · 광 저장장치 · 반도체 저장장치 등 자료 기록이 가능한 전자장치를 말한다.
27. "정보시스템"이라 함은 정보의 수집 · 가공 · 저장 · 검색 · 송신 · 수신에 활용되는 전자기기와 소프트웨어의 조직화된 체계를 말하며, 저장매체를 내장한 복사기 · 팩스 등 사무용 기기를 포함한다.
28. "소자(消磁)"란 저장매체에 역자기장을 이용해 매체의 자화값을 "0" 으로 만들어 저장자료의 복원이 불가능하게 만드는 것을 말한다.
29. "완전포맷"이라 함은 저장매체 전체의 자료저장 위치에 새로운 자료(0 또는 1)를 중복하여 저장하는 것을 말한다

제2장 정보보안 기본활동

제4조(기본목표) 정보보안의 기본목표는 각종 전자적 수단에 의한 국가안보 및 국가이익 관련 정보의 기밀성 · 무결성 · 가용성을 확보하고 정보통신망을 보호하는데 있다.

제5조(활동방향) 각급기관의 장은 정보보안을 위하여 다음 각 호의 기본활동을 수행하여야 한다.

1. 정보보안 정책 및 활동 세부계획 수립 · 시행
2. 정보보안 감사 · 지도점검 실시
3. 취약 정보통신망 보안대책 수립 추진
4. 정보보안 위규 적발 강화 및 사고조사 처리
5. 산하기관에 대한 정보보안 업무조정 및 감독
6. 사이버위협정보 수집 · 분석 및 보안관제
7. 사이버공격 관련 경보 발령시 대응활동
8. 침해사고 대응 · 복구
9. 정보보안수준 평가 · 관리
10. 정보보안 교육계획 수립 · 시행

11. 정보보안업무 심사분석 시행
12. 도청 위해요소 제거
13. 정보보안 관련 규정·지침 등 제·개정
14. 기타 정보보안 관련 사항

제6조(정보보안 책임) 각급기관의 정보보안에 관한 책임은 각급기관의 장에게 있다.

제7조(정보보안담당관 제도운영) ① 각급기관의 장은 효율적인 정보보안업무를 수행하기 위하여 정보통신분임 보안담당관(이하 '정보보안담당관'이라 한다)을 임명 운영하여야 한다.
② 다음에 정하는 자는 보직과 동시에 당해기관의 정보보안담당관이 된다.
1. 본부 : 정보화지원팀장이 정보보안담당관이 되며, 정보통신보안 업무중 일반통신은 보안담당관(총무과장)이 담당한다.
2. 소속기관 및 산하단체 : 각 기관의 장이 지정하는 자가 된다.
③ 농림수산식품부 정보보안담당관을 임명한 경우에는 3일 이내에 소속·직책·직급·성명·연락처(전자우편 주소 포함) 등을 국정원장에게 통보하여야 한다.
④ 농림수산식품부 정보보안담당관은 본부 및 소속기관·산하단체 등에 대한 정보보안업무를 총괄한다.
⑤ 각급기관의 정보보안담당관 임무는 다음과 같다.
1. 정보보안 정책 및 활동 세부계획 수립
2. 정보통신망 신·증설시 보안대책 수립
3. 정보통신실, 정보통신망 및 정보자료 등의 보안관리
4. 정보보안업무 지도·감독 및 교육
5. 정보보안 사고조사·복구 및 처리
6. 국가용 보안시스템의 운용·보안관리
7. 사이버위협정보 수집·분석 및 보안관제
8. 사이버공격 관련 경보 발령시 대응활동
9. 「국가 사이버안전 매뉴얼」 운용 등 사이버안전활동
10. 정보보안업무 심사분석 관장
11. 자체 정보보안관련 지침 등 제도 개선
12. 정보통신망 취약성 진단
13. 대도청 보안업무
14. 검증필 정보보호시스템의 운용·보안관리
15. 기타 정보보안 관련 업무

제8조(활동계획 수립 및 심사분석) ① 각급기관의 장은 제5조의 규정에 의거 정보보안업무 세부 추진계획(「국가 사이버안전 관리규정」에 따른 사이버안전대책을 포함한다)을 수립·시행하고 이에 대한 심사분석을 실시하여야 한다.

② 각급기관의 장은 정보보안업무 세부 추진계획 및 심사분석을 별지 제1호 및 제2호 서식에 의거 다음 각 호의 기한 내에 농림수산식품부장관에게 제출하여야 한다.

1. 연간 정보보안업무 세부 추진계획 : 당해년도 1월15일까지
2. 정보보안업무 심사분석 : 당해년도 10월15일까지

③ 농림수산식품부장관은 제2항의 보고서를 취합하여 '연간정보보안업무세부추진계획'은 당해년도 1.31까지, '정보보안업무심사분석'은 10.31까지 국정원장에게 제출하여야 한다. 다만, '연간 정보보안업무세부추진계획'은 '연간 보안업무추진계획'에, '정보보안업무심사분석'은 '보안업무심사분석'에 각각 포함하여 제출할 수 있다.

제9조(정보보안감사) ① 각급기관의 장은 제5조의 규정에 따라 연1회 이상 정보보안감사를 실시하여야 한다.

② 정보보안감사는 일반보안감사와 병행하여 실시한다. 다만, 필요하다고 인정할 때에는 별도로 감사를 실시할 수 있다.

③ 농림수산식품부장관은 국정원장에게 정보보안감사 실시계획과 감사결과를 다음 각 호의 기한 내에 제출하여야 한다.

1. 연도 정보보안감사 실시계획 : 당해년도 1.31까지
2. 정보보안감사 결과 : 감사결과 강평서 완료시

④ 농림수산식품부장관은 정보보안감사의 효율적 수행을 위하여 국정원장에게 감사방향, 감사중점사항, 감사관 지원 등 업무협조를 요청할 수 있다.

제10조(정보보안 지도방문) ① 각급기관의 장은 정보통신시스템 운용관리에 따른 보안취약성 개선을 위하여 정보보안 지도방문(이하 '지도방문'이라 한다)을 실시하여야 한다.

② 산하기관 및 소속부서에 지도방문을 실시할 경우에는 「국가 사이버안전 매뉴얼」의 점검항목을 적극 활용한다.

③ 지도방문 실시결과는 제8조의 정보보안업무 심사분석에 포함시켜야 한다.

제11조(보안성 검토) ① 각급기관의 장은 다음 각 호의 경우에 대하여는 자체 보안대책을 강구하고 이를 바탕으로 사업 계획단계에서 국정원장과 협의를 거쳐 보안성 검토를 의뢰하여야 한다. 다만, 사안이 경미할 경우 국정원장과 사전협의만으로 보안성 검토를 생략할 수 있다.

1. 정보통신망을 신·증설하거나 서버 등 정보통신시스템을 교체하는 경우
2. 내부 정보통신망을 외부망과 연결하고자 하는 경우
3. 정보보안 관련법규 제정 또는 개정하고자 할 경우
4. 국가용 보안시스템 또는 검증필 정보보호시스템을 도입 운용하고자 할 경우
5. 외부기관 및 업체의 보안감리 또는 보안컨설팅(보안취약성 분석·평가 포함)을 받거나 정보처리·보안관제 등의 업무를 위탁할 경우
6. 무선랜 등 무선망을 사용하여 업무를 처리하거나 원격근무 지원 등을 위해 시스템을 도입하는 경우
7. 기타 정보통신 운용환경 변화로 인하여 보안성 검토가 필요하다고 인정되는 경우

② 보안성 검토 업무절차는 다음과 같다.

1. 정보통신망 신·증설 또는 정보화 용역개발 등 추진하고자 하는 사업계획에 대하여 자체 보안심사위원회 심의를 거친 후 보안성 검토를 요청한다.
2. 계획수립 단계에서 보안대책을 판단하기가 곤란한 경우에는 미리 국정원장과 사전 협의한 후 보안성 검토를 요청한다.
3. 농림수산식품부장관은 국정원장에게 보안성 검토를 요청하고 각급기관의 장은 농림수산식품부장관을 경유하여 국정원장에게 보안성 검토를 요청한다.

③ 각급기관의 장은 보안성 검토를 요청할 경우 다음 각 호의 서류를 제출 하여야 한다. 다만, 암호논리를 지원 요청할 경우에는 제78조제2항에 근거한 자료를 제출하여야 하고 상용 정보보호시스템의 보안적합성 검증을 병행하고자 할 경우에는 제84조제3항에 근거한 자료를 함께 제출하여야 한다.

1. 사업목적 및 추진계획
2. 사업계획서(신규사업에만 적용)
3. 기술제안요구서
4. 정보통신망 구성도
5. 자체 보안대책 강구사항

④ 제3항제5호의 자체 보안대책 강구사항은 다음 각 호를 포함하여야 한다.

1. 보안관리 수행체계(조직, 인원) 등 관리적 보안대책
2. 정보통신시스템 설치장소에 대한 보안관리방안 등 물리적 보안대책
3. 국가용 보안시스템 또는 검증필 정보보호시스템 도입 및 운용계획
4. 국가기관간 망 연동시 해당 기관간 보안관리 협의사항
5. 서버, 단말기, 네트워크 등 정보통신시스템의 요소별 기술적 보안대책
6. 전산자료 보호대책
7. 재난복구계획 또는 상시 운용계획

제12조(정보보안 교육) ① 각급기관의 장은 정보보안 교육계획을 수립하고 년2회 이상 교육을 시행하여야 한다. 다만, 공무원 연수기관에서는 매 교육과정 1회 이상을 시행하여야 한다.
② 각급기관의 장은 정보보안교육의 효율성을 제고시키기 위하여 기관별 자체 실정에 맞는 정보보안 교안을 작성 활용하여야 하며, 필요시 국정원장에게 전문인력 및 자료 지원을 요청할 수 있다.
③ 제1항에 의한 교육계획 수립시 정보보안담당관이 최신 정보보안 정책 및 기술 등을 습득하기 위하여 국가정보대학원에 개설된 정보보안 관련 교육과정을 이수하는 내용을 포함할 수 있다.

제13조(비상통신 보안대책) 전시 또는 비상사태 발생에 대비하여 비상통신망을 운용하고 있거나 중요한 정보통신시설을 관리 감독하는 기관의 장은 평상시 이에 대한 정보통신보안 대책을 강구하여야 한다.

제3장 정보보안 관리

제14조(무선통신 보안관리) 무선통신망(이하 '무선망'이라 한다) 운용에 따른 보안관리 방침은 다음과 같다.
1. 보안상 취약한 무선망의 시설 또는 증설 억제
2. 무선망으로 중요자료를 소통할 경우 국가용 보안시스템 사용
3. 공중통신망 이용시 국가용 보안시스템 활용
4. 무선망을 신규도입하거나 운용환경을 변경하고자 할 때에는 국가용 보안시스템을 개발 적용할 수 있도록 입찰조건에 명시
5. 도서 무선망의 보안대책 수립추진

제15조(외교정보통신 보안관리) ① 각급기관의 장은 해외공관과 비밀 등 중요자료를 소통하고자 할 때에는 국정원장이 승인한 보안대책을 시행하여야 한다.
② 각급기관의 장은 해외공관에 직원을 파견하고자 할 경우에는 파견 직원에 대하여 정보통신시스템 운용시 보안관리방안 등 정보보안교육을 실시하여야 하며, 정보보안업무에 대하여 인계인수를 철저히 하여야 한다.

제16조(국제통신 보안관리) ① 각급기관의 장은 국제통신망에 의한 국가기밀 및 중요자료의 누설방지를 위하여 다음 각 호의 보안대책을 강구하여야 한다.
1. 비밀 및 중요사항에 대한 통신내용 보호대책

2. 보안성, 안전성을 고려한 정보통신망 활용

② 국제통신망으로 업무와 관련된 사항을 송수신 하고자 할 경우에는 자료 및 소통내용에 대한 보안통제를 실시하여야 한다.

제17조(남북통신 보안관리) ① 각급기관의 장은 남북회담 및 남북경협사업 등을 위하여 북한지역에 정보통신시스템을 반출하거나 정보통신망을 구축할 경우 국정원장과 사전 협의하여 보안대책을 강구하여야 한다.

② 남북경협사업 등에 참가한 사업자를 관할하는 각급기관의 장은 사업자가 북한 현지에서 운영하는 정보통신시스템이 도청 등에 악용되지 않도록 주기적인 정보보안교육 등 보안지도 활동을 강화하여야 한다.

③ 제1항에 따라 남·북한 지역간 정보통신망을 연결할 경우에는 통신경로를 임의로 변경하거나 인가받지 않은 다른 망과 연결하지 말아야 한다.

제18조(중요 정보통신시설 보안관리) ①각급기관의 장은 다음 각 호의 중요 정보통신시설 및 지역을 보호구역으로 설정 관리하여야 한다.

1. 암호실
2. 정보통신실(통합전산센터 포함)
3. 전산자료 보관실
4. 국가용 보안시스템 설치 장소
5. 국가비상통신 등 중요통신망의 교환국, 회선집중국 또는 중계국
6. 백업센터 및 중요한 정보통신시설을 집중 제어하는 국소
7. 기타 보안관리가 필요하다고 인정되는 정보통신시스템 설치 장소

②제1항에 의거 지정된 보호구역에 대해서는 「보안업무규정」에 의하여 보안대책을 강구하여야 한다.

③각급기관의 장은 중요 정보통신시설의 보안취약요인을 발굴 개선하거나 외부의 위협요소로부터 보호대책을 강구하기 위하여 정기적으로 보안점검을 실시하여야 한다.

제19조(대도청 측정활동) ① 각급기관의 장은 청사를 신설·이전 또는 증·개축하고자 할 때에는 도청방지 대책을 강구하여야 한다.

② 각급기관의 장은 중요한 협상이나 회의 또는 회담을 개최하는 장소 및 공사가 진행중인 주요시설 등에 대하여 도청으로부터 위해요소 제거를 위하여 국정원장에게 대도청 측정을 요청할 수 있다.

③ 각급기관의 장은 카메라 장착 휴대폰 등을 이용하여 불법적으로 내부 중요자료나 제18조제1

항의 중요시설에 대한 사진촬영을 금지토록 하는 등 보안대책을 강구하여야 한다.
④ 디지털·레이저 등 첨단도청장치에 의한 불법도청을 방어하기 위한 시스템 도입 운용시 국정원장과 사전 협의하여 성능이 검증된 제품을 사용하여야 한다.
⑤ 정보통신시스템 사용시 비의도적인 전자파 발생에 의한 기밀유출 방지를 위해 전자파 차폐실을 구축하거나 관련장비를 사용하고자 할 경우에는 국정원장이 제정한 「전자파 차폐실 구축 및 측정기준」(대외비)에 따라서 보안성 검토를 의뢰하여야 한다.
⑥ 주요 사무실에 차폐유리·도료 등 차폐재료 설치를 권장하고 정보통신시스템은 전자파장애(EMI)·전자파적합성(EMC) 검증을 받은 제품을 사용하여야 한다.
⑦ 각급기관의 장은 대도청 보안활동의 중요성과 전자파보안 의식제고 등을 위하여 국정원장에게 관련사항의 시연 및 보안교육을 요청할 수 있다.

제20조(대도청 측정결과 조치) ① 대도청측정 결과를 통보받은 각급기관의 장은 도출된 문제점에 대하여 국정원장과 협의하여 필요한 보안방책을 수립·시행하여야 한다.
② 각급기관의 장은 대도청측정 계획 및 결과에 관한 내용을 외부에 공개하여서는 아니 된다.

제21조(정보통신실 보안관리) ① 정보통신실을 운용하는 각급기관의 장은 다음 각 호에 정하는 보호대책을 강구하여야 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. 보조기억매체에 대한 안전지출 및 긴급파기 계획 수립
6. 관리책임자 및 자료·장비별 취급자 지정 운용
7. 비인가자에 대한 출입을 기록 유지
② 정보통신실의 관리책임자는 자료보호를 위하여 다음 각 호와 같은 보안대책을 강구하여야 한다.
1. 자료별로 접근권한을 제한
2. 작업은 소관업무에 따라 입력·출력·열람 등으로 제한
3. 열람은 필요에 따라 기본항목·전항목 등으로 제한

제22조(전산자료 보안관리) ① 각급기관의 장은 전산자료에 대한 유출이나 파괴 또는 변조 등에 대비하여 다음 각 호에 정하는 보호대책을 강구하여야 한다.
1. 자료복사본(예비) 확보 및 안전지역 별도 보관

2. 전산자료(보조기억매체) 보유현황 관리
3. 전산자료 및 장비의 반출 또는 반입 통제
4. 불법접근 및 컴퓨터바이러스(이하 '악성코드'라 한다) 피해 예방
5. 전산자료 접근권한 구분·통제
6. 예비(Back up)체계 수립·시행

② 전산자료를 입력 저장하기 위한 보조기억매체는 각 매체별로 별개의 관리번호를 부여 관리하여야 하며, 비밀 등 중요자료가 입력된 보조기억매체는 제29조를 준용 관리하여야 한다.

③ 보조기억매체를 활용하는 부서의 보안담당자는 월1회 이상 보유현황 및 관리실태를 점검하고 관리책임자의 확인을 받아야 한다.

④ 비밀로 분류하지 않더라도 민감한 보고서나 자료에 대해서는 자료별 접근 비밀번호를 사용하고, 보조기억매체를 적극 활용하여야 한다.

제23조(정보통신망 관련자료 관리) ① 각급기관의 장은 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 운용현황
3. 보안취약성 분석·평가 결과물
4. 기타 보호할 필요가 있는 정보통신망 관련 자료

② 제1항의 명시되지 않은 정보통신망 관련 자료의 분류 관리는 국정원장이 제정한 「비밀 세부분류지침」(대외비)을 따른다.

제24조(비공개자료 보호) ① 각급기관의 장은 정보보안과 관련된 행정정보를 비공개로 분류·관리해야 한다.

② 각급기관의 장은 소속직원 중 비밀 및 중요업무 담당자의 인적사항, 세부 담당업무와 전자우편 주소 등을 인터넷 등에 공개하여서는 아니 된다.

③ 제1항 및 제2항의 경우에도 불구하고 각급기관의 장은 국정원장과 공개범위·요건 등을 사전 협의하여 관련내용을 공개할 수 있다.

제25조(전산자료 보호등급 분류) ① 각급기관의 장은 전산자료의 효율적 보호를 위하여 다음 각 호에 해당하는 경우에는 자체 실정에 맞는 전산자료 보호등급을 분류하여야 한다.

1. 최초로 정보통신망을 신설하여 전산자료의 보호등급 구분이 필요한 경우
2. 현재 운용중인 정보통신망을 재구성할 경우

3. 각급기관의 장이 필요하다고 인정하는 경우

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

1. "가"급 보호등급 자료
   유출 또는 손상되는 경우 각급기관의 업무수행에 중대한 장애를 초래하거나 개인 신상에 심각한 영향을 줄 수 있는 전산자료
2. "나"급 보호등급 자료
   유출 또는 손상되는 경우 각급기관의 업무수행에 장애를 초래하거나 개인 신상에 영향을 줄 수 있는 전산자료
3. "다"급 보호등급 자료
   유출 또는 손상되는 경우 각급기관의 업무수행 및 기관의 신뢰도에 경미한 영향을 줄 수 있는 전산자료

제26조(전산자료 보호등급 분류기준) ① 각급기관의 장은 제25조의 규정에 따라 전산자료 보호등급을 분류하기 위한 자체 기준을 수립하여야 하며, 이를 수립한 경우에는 국정원장과 협의한 후 시행하여야 한다. 다만, 소속기관 및 산하단체에 대한 기준 수립은 농림수산식품부장관이 시행할 수 있다.

② 각급기관의 장이 전산자료의 보호등급 기준을 정하고자 할 경우에는 「국가 정보보안 기본지침」 부록1의 전산자료 보호등급 세부 분류기준을 참고할 수 있다.

제27조(보호등급별 보안대책) ① 각급기관의 장은 "가"급 보호등급으로 분류된 전산자료를 보호하기 위해서는 다음 각 호의 보안대책을 강구하여야 한다.

1. K4등급 또는 EAL4 등급 이상의 인증을 받고 국정원장이 국가기관용으로 보안적합성을 검증한 정보보호시스템을 설치 사용
2. 자료별 비밀번호의 사용과 시스템 접근권한을 설정 관리

② "나"급 보호등급으로 분류된 전산자료를 보호하기 위해서는 다음 각 호의 보안대책을 강구하여야 한다.

1. K3등급 또는 EAL3 등급 이상의 인증을 받고 국정원장이 국가기관용으로 보안적합성을 검증한 정보보호시스템을 설치 사용
2. 시스템 접근권한을 설정 관리

③ "다"급 보호등급 자료를 보호하기 위해서는 K2등급 또는 EAL2 등급 이상의 인증을 받고 국정원장이 국가기관용으로 보안적합성을 검증한 정보보호시스템을 설치 사용하여야 한다.

④ 서로 다른 보호등급의 전산자료를 보호하고자 할 경우에는 가장 높은 보호등급에 따른 보안대책을 강구하여야 한다.

⑤ 제1항 내지 제3항에서 언급되지 않은 사항은 제22조(전산자료 보안관리)의 보안대책을 준용한다.

제28조(비밀자료 등의 전자적 처리) ① 비밀 등 중요자료를 정보통신수단을 이용하여 생산·보관·분류·열람·출력·송수신·이관하는 등 전자적으로 처리하기 위해서는 국가용 보안시스템을 사용하여 암호화하는 등 국정원장이 안전성을 확인한 보안조치를 수행하여야 한다.

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

③ 비밀자료 생산을 완료한 경우에는 PC에 입력된 비밀내용을 삭제하여야 한다. 다만, 업무상 계속 보관이 필요한 경우에는 관리책임자의 승인 하에 삭제하지 아니할 수 있다. 이 경우에는 비밀자료를 저장할 보조기억매체를 별도로 지정 사용하거나 PC 내에 독립된 폴더를 지정, 국가용 보안시스템을 사용하여 암호화하는 등 적절한 보안대책을 강구하여야 한다.

④ 비밀자료를 전자적으로 생산·열람·출력·송수신·이관 시에는 작업 내용을 전자적으로 기록 유지하여야 하며, 송수신시에는 정당성 확인 및 부인을 봉쇄하기 위하여 전자적으로 생성된 영수증을 사용하여야 한다.

⑤ 전자적으로 처리된 비밀자료를 종이문서로 출력한 이후의 취급 관리는 「보안업무규정」을 따른다.

⑥ 제1항에 의한 보안조치 중 이 지침에 명시되지 않은 세부사항은 국정원장이 제정한 「전자문서 보안조치 수행지침」을 따른다.

제29조(중요자료 저장 보조기억매체 관리) ① 비밀 등 중요자료가 평문 또는 암호화 저장되어 있는 보조기억매체를 사용하고자 할 경우에는 유출, 훼손, 비인가자 접근 및 내용 위변조 등에 대비한 보안대책을 강구하여 정보보안담당관의 승인을 받아야 한다.

② 비밀자료가 저장된 보조기억매체는 매체별로 해당 비밀등급 및 관리번호를 부여하고 비밀관리기록부에 등재하여 이중캐비닛 또는 금고에 보관하여야 한다. 이 경우에는 매체 전면에 비밀등급 및 관리번호가 표시되도록 하여야 한다. 다만, 비밀자료가 국가용 보안시스템으로 암호화 저장된 보조기억매체는 그러하지 아니할 수 있다.

③ 제2항에 규정된 보조기억매체가 국가용 보안시스템에 해당될 경우에는 국가용 보안시스템 관리기록부(별지 제9호서식)에 등재하고 해당 국가용 보안시스템 운용·관리체계에 따라 관리하여야 한다.

④ 각급기관에서는 보조기억매체를 사용할 경우, 각 부서장의 승인 하에 사용하여야 하며 USB 메모리 등 보조기억매체 보안관리지침을 준용하여야 한다.

제30조(정보통신시스템 보안관리) ① 각급기관의 장은 정보통신시스템(정보통신망 포함)의 효율적인 보안관리를 위하여 정보통신시스템별로 관리책임자(이하 '시스템관리자'라 한다)를 지정·운영하여야 한다.

② 시스템관리자는 각종서버·PC·정보통신장비 등 정보통신시스템이 비인가자에게 불필요한 서비스를 허용하지 않도록 보안기능을 설정하여야 한다.

③ 시스템관리자는 보안도구를 이용하여 정보통신시스템의 보안취약성을 진단하여야 하며, 시스템 접속시 다음 각 호 사항이 자동 수록되도록 하여야 한다.

1. 서버 접속일시, 접속자 및 접속방법 등 전산망 접근기록(1차)
2. 전산자료 열람·출력 등에 대한 사용자, 일시, 자료제목 등 접근기록(2차)

④ 시스템관리자는 다음 각 호와 같이 자동 수록된 접근자료(Log Data)를 관리하여야 한다.

1. 접근자료는 접속의 성공여부와 무관하게 기록 유지
2. 시스템 접근기록은 매일 점검하고 분석내용을 월1회 관리책임자에게 보고
3. 자동 수록된 자료는 정보보안사고 발생시 확인 등을 위하여 3개월 이상 보관(백업자료 포함) 및 외부유출 방지를 위한 보호대책 강구
4. 3회 이상 접속시도의 오류가 발생하는 경우 경보 발생 및 시스템 관리자에 통보기능 부여

⑤ 시스템관리자는 각종 서버의 보유자료에 대해 업무별, 자료별 중요도에 따라 접근권한을 차등 부여하여야 한다.

⑥ 시스템관리자가 비인가자의 정보통신시스템 침입 사실을 인지한 경우에는 시스템 보호를 위한 접속차단 등 초동조치를 취하고 지체 없이 정보보안담당관에게 보고하여야 하며, 즉시 국정원장에게 관련내용을 통보하여야 한다.

⑦ 사용자별 자료 접근범위는 서버에 등록하여 인가여부를 식별토록 하고 인가된 범위 이외의 자료접근을 통제하여야 한다.

⑧ 정보보안담당관은 정보통신시스템에 대하여 외부업체의 원격 유지보수 작업을 허용하여서는 아니 된다. 다만, 부득이한 경우에는 필요한 보안대책을 강구한 후 허용할 수 있으며, 이 때에도 원격 유지보수 내용을 확인 감독하여 반드시 기록을 남겨야 한다.

제31조(정보통신시스템 감리) ① 각급기관의 장은 정보통신시스템에 대한 감리를 감리인에게 의뢰하고자 할 때에는 비밀 및 중요자료의 유출방지를 위하여 다음 각 호의 사항을 미리 농림수산식품부장관을 경유하여 국정원장과 협의하여야 한다.

1. 감리인 및 투입인원
2. 감리 일정 및 감리 대상·영역
3. 감리 중점사항 및 보안점검 대상항목
4. 비밀 및 중요자료 보호대책 등

② 다만, 보안 관련 사항을 감리할 경우에는 제11조에 의거 국정원장에게 보안성검토를 의뢰하여 감리계획 및 결과의 적절성 여부를 확인하여야 한다.

제32조(재난복구 대책) ① 각급기관의 장은 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애 발생에 대비하여 시스템 이원화, 백업관리, 복구 등 종합적인 재난복구 대책을 수립·시행하여야 한다.
② 각급기관의 장은 재난복구 대책을 정기적으로 시험하고 검토해야 하며 업무 연속성에 대한 영향평가를 실시하여야 한다.
③ 각급기관의 장은 정보통신망 장애에 대비한 백업시설을 확보하고 정기적으로 백업을 수행하여야 한다.
④ 제3항에 의거 백업시설을 설치할 경우에는 정보통신실과 물리적으로 일정거리 이상 위치한 안전한 장소에 설치하여 재난에 대비하여야 한다.
⑤ 해당기관의 장이 제1항 내지 제4항에 의하여 별도의 백업시설을 구축 운영하고자 할 경우에는 제11조에 의거 국정원장에게 사전 보안성 검토를 의뢰하여야 한다.

제33조(PC 보안관리) ① 단말기를 포함한 PC 등을 사용하고자 할 경우에는 사용자 및 관리책임자를 지정하여야 한다. 이 경우에 관리책임자는 사용자를 제4호서식(전산장비관리대장)에 등재하여 관리하여야 한다.
② 각급기관의 장은 비인가자가 PC를 무단으로 조작하여 전산자료를 유출, 위·변조 및 훼손시키지 못하도록 다음 각 호에 정한 보호대책을 강구하여야 한다.
1. 장비별·자료별·사용자별 비밀번호 사용
2. 10분 이상 PC 작업 중단시 화면보호 조치
3. 백신 및 PC용 침입차단시스템 등 운용
4. P2P 등 업무와 무관하거나 보안에 취약한 프로그램의 사용 금지
③ 해당부서 장은 PC를 교체·반납·폐기하거나 고장으로 외부에 수리를 의뢰하고자 할 경우에는 하드디스크에 수록된 자료가 유출, 훼손되지 않도록 보안조치를 하여야 한다.
④ PC에 적용되는 사용자계정(ID) 및 비밀번호의 취급관리는 제34조(사용자계정 관리)와 제35조(비밀번호 관리)의 규정을 준용한다.
⑤ 정보보안담당관은 해당기관의 업무용 노트북 PC, PDA 등 휴대용 단말기의 운용현황을 파악하여 관리하고, 해당부서 장은 반출 또는 반입시 최신 백신을 활용하여 해킹프로그램 및 웜·바이러스 감염여부를 점검하여야 한다.
⑥ 개인소유의 PC(노트북 PC 등)는 각급기관 내부로 반출 또는 반입하여 사용하여서는 아니된다. 다만, 부득이한 경우에는 해당부서 장의 책임 하에 보안조치를 한 후 반출·반입할 수 있으며, 정보보안담당관에게 통보하여야 한다.

제34조(사용자계정 관리) ① 사용자계정(ID)은 비인가자 도용 및 정보통신시스템 불법접속에 대비하여 다음 각 호의 사항을 반영하여 관리하여야 한다.

1. 사용자별 또는 그룹별로 접근 권한 부여
2. 외부 사용자의 계정부여는 불허하되 부득이한 경우에는 각급기관 장의 책임 하에 유효기간을 설정하는 등 보안조치 강구한 후 허용
3. 비밀번호가 없는 사용자계정은 사용 금지

② 시스템관리자는 사용자계정의 등록·변경·폐기시 정보보안담당관에 그 결과를 보고하여야 한다.

③ 3회에 걸쳐 사용자인증 실패시 정보통신시스템 접속을 중지시키고 비인가자 침입 여부를 확인 점검하여야 한다.

④ 퇴직 또는 보직변경 발생시 시스템관리자는 사용하지 않는 사용자 계정 및 비밀번호를 신속히 삭제하여야 한다.

제35조(비밀번호 관리) ① 비밀번호는 정보통신시스템의 무단사용 방지를 위하여 다음과 같이 구분 사용하여야 한다.

1. 비인가자의 정보통신시스템 접근방지를 위한 장비 접근용 비밀번호(1차)
2. 정보통신시스템 사용자가 서버 등 정보통신망 접속시 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 반드시 자료별 비밀번호를 부여하되, 공개 또는 열람 자료에 대해서는 부여하지 아니할 수 있다.

③ 비밀번호는 다음 각 호 사항을 반영하여 숫자와 문자, 특수문자 등으로 8자리 이상으로 정하고 분기1회 이상 주기적으로 변경 사용하여야 한다.

1. 사용자계정(ID)과 동일하지 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. 이미 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 등록되어 있는 비밀번호는 암호화하여 보관하여야 하고, 단말기·PC 등의 비밀번호를 종합기록 관리하고자 할 경우에는 전산장비 관리대장(별지 제4호서식)에 등재하여 대외비 이상으로 분류 관리하여야 한다.

제36조(악성코드 방지대책) ① 각급기관의 장은 웜·바이러스, 해킹프로그램, 스파이웨어 등 악성코드 감염을 방지하기 위하여 다음 각 호에 따라 정보통신시스템을 운영 관리하여야 한다.

1. 출처, 유통경로 및 제작자가 명확하지 않은 응용프로그램은 사용을 자제하고 불가피한 경우에는 백신 등 관련 검색프로그램으로 진단 후 사용
2. 업무상 불필요한 서비스를 제한
3. 실행파일은 읽기 전용으로 속성 변경
4. 인터넷 등 상용망으로 입수한 자료는 필히 악성코드 검색 후 사용
5. 악성코드 조기 발견을 위하여 최신 백신프로그램 활용 및 보안업데이트 실행
6. 시스템이 작동할 때마다 컴퓨터 하드디스크의 부트섹터 및 메모리 등에 악성코드가 감염되었는지 점검

② 악성코드 감염이 발견되었을 경우, 시스템관리자 또는 PC 사용자는 다음 각 호의 조치를 하여야 한다.

1. 악성코드 감염 피해를 최소화하기 위하여 감염된 시스템 사용 중지
2. 최신 백신 등 악성코드 제거 프로그램을 이용하여 퇴치
3. 악성코드 감염확산 방지를 위하여 정보보안담당관에게 관련내용 및 보안조치 사항을 즉시 보고
4. 악성코드 감염의 재발을 방지하기 위하여 원인 분석 및 예방조치 수행

③ 각급기관의 장은 바이러스가 신종이거나 감염피해가 심각하다고 판단될 경우에는 관련사항을 국정원장 및 관계기관에 신속히 통보하여야 한다.

④ 각급기관의 장은 국정원장이 악성코드 감염사실을 확인하여 조치를 권고할 경우 즉시 이해하여야 한다.

제37조(전자우편 등 보안관리) ① 전자우편 사용자는 보안조치 없이 전자우편을 이용한 비밀 및 중요자료 전송을 금지하고 출처가 불분명한 전자우편의 경우 열람하지 말고 삭제한다.

② 인터넷을 통한 불법 프로그램 다운로드를 금지한다.

③ 각급기관의 장은 PC 등에서 음란·도박·증권 등 업무와 무관한 인터넷 사이트 접근에 대한 통제대책을 강구하여야 한다.

제38조('정보보안진단의 날' 운영) ① 각급기관의 장은 매월 '정보보안진단의 날'을 지정·운용하여야 하며, 이는 '보안진단의날'과 병행하여 지정·운용할 수 있다.

② 정보보안담당관은 '정보보안진단의 날'에 소관 정보통신망을 대상으로 악성코드 감염여부와 정보통신시스템의 보안 취약여부 등을 진단, 문제점을 발굴 개선하여야 한다.

③ 각급기관의 장은 제1항 및 제2항에 따라 보안취약성을 발굴·개선한 실적을 제8조의 규정에 의한 정보보안업무 심사분석에 포함시켜야 한다.

제39조(상용망 등 외부망 연동) ① 각급기관의 장은 중앙행정부처와 소속기관·산하단체 또는 다른 기관과의 정보통신망과 연결 사용하고자 할 경우에는 보안관리의 책임한계를 설정하고 보안대책을 수립·시행하여야 한다.
② 외부망과 접속하는 경우에는 전산자료 제공범위 및 이용자의 접근 제한 등에 대해 보안심사위원회 심의를 거쳐 결정하여야 한다.
③ 외부망 연결에 따른 보안취약성 해소를 위하여 접속자료를 주기적으로 분석하고 보안도구를 이용하여 정보통신망의 취약성을 수시 점검하여야 한다.
④ 각급기관의 장은 정보통신망을 상용망 등 외부망과 접속하고자 할 경우에는 비인가자의 무단침입을 방지하기 보안적합성이 검증된 침입차단·탐지시스템 설치 운용 등 보안대책을 강구하여야 한다.
⑤ 보안적합성이 검증된 정보보호시스템의 설치 및 운용관리에 대해서는 제5장의 규정에 따른다.
⑥ 인터넷 등 상용망 및 타 기관과의 정보통신망 연동시 불법침입(해킹)을 방지하고 효율적인 보안관리를 위하여 연결지점을 지정 운용함으로써 임의 접속을 차단하여야 한다.
⑦ 각급기관의 장은 정보통신망에 사용되는 'IP 주소'를 체계적으로 관리하여야 하며, 내부정보통신망을 보호하기 위하여 가급적 사설주소체계(NAT : Network Address Translation)를 사용한다.

제40조(웹서버 등 공개서버 관리) ① 외부인에게 공개할 목적으로 설치되는 웹서버 등 각종 공개서버는 내부망과 분리하여 운영하고 보안적합성이 검증된 침입차단·탐지시스템을 설치하는 등 보안대책을 강구하여야 한다.
② 서버에 접근할 수 있는 사용자계정을 제한하며 불필요한 계정은 삭제하여야 한다.
③ 홈페이지 게재내용은 자체 보안심사위원회의 심의를 거쳐 비밀내용 등 비공개 자료가 포함되지 않도록 하여야 한다. 다만, 수치변경 등 동일제목의 내용수정은 정보보안담당관의 보안성 검토로 갈음할 수 있다.
④ 공개서버는 업무서비스를 제외한 모든 서비스 및 시험·개발도구 등의 사용을 제한하도록 보안기능을 설정하여야 한다.
⑤ 공개서버의 보안취약성을 수시로 점검하고, 자료의 위·변조, 훼손 여부를 확인하여야 한다.
⑥ 보안사고에 대비하여 서버에 저장된 자료의 철저한 백업체계를 수립·시행하여야 한다.
⑦공개서버를 통해 개인정보가 유출, 위·변조 되지 않도록 보안조치를 하여야 한다.

제41조(원격근무 보안관리) 각급기관의 장은 재택·파견·이동근무 등 원격근무를 지원하기 위한 시스템을 도입·운영할 경우 「원격근무 보안관리방안」(국가 정보보안 기본지침, 부록 2)을 참고하여 보안대책을 수립·시행하여야 한다.

제42조(정보보안관리 수준 평가) ① 각급기관의 장은 「국가 사이버안전 매뉴얼」을 참고하여 매년 자체 정보보안관리 수준을 평가하여야 한다.
② 각급기관의 장은 제1항에 의해 평가한 결과를 매년 10.31일까지 국정원장에게 통보하여야 한다.

제43조(외부 용역사업 보안관리) ① 각급기관의 장은 정보화사업 및 보안컨설팅 수행 등 외부 용역사업을 추진할 경우, 제11조에 근거하여 국정원장에게 보안성 검토를 의뢰하여야 한다.
② 각급기관의 장은 제1항에 의한 용역사업 계약시 계약서에 용역사업 참여직원의 보안준수사항과 위반시 손해배상 책임 등을 명시하여야 한다.
③ 각급기관의 장은 비밀 관련 용역사업을 수행할 경우, 외부인원에 대한 비밀취급인가 등 보안조치를 수행하고 국정원장에게 정보보안측정을 요청한다.
④ 정보통신망도·IP현황 등 용역업체에 제공할 자료는 자료 인계인수대장을 비치, 보안조치 후 인계인수하고 무단 복사·외부반출을 금지한다.
⑤ 정보보안담당관은 용역 참여직원을 대상으로 보안교육 및 보안점검을 실시하여야 하며, 필요시 국정원장에게 지원을 요청할 수 있다.
⑥ 정보보안담당관은 용역 참여직원이 노트북 등 관련장비를 반출 또는 반입할 때마다 악성코드 감염여부, 자료 무단반출 여부를 확인하는 등 보안조치를 하여야 한다.
⑦ 정보보안담당관은 용역사업 종료시 외부업체의 노트북·보조기억매체 등을 통해 기관 내부 자료 및 용역 결과물이 유출되는 것을 방지하기 위하여 복구가 불가능하도록 완전 소거하는 등 보안조치를 하여야 한다.
⑧ 각급기관의 장은 용역업체로부터 용역 결과물을 전량 회수하고 비인가자에게 제공·대여·열람을 금지하는 등 관리를 철저히 한다.

제44조(정보통신 운용현황 통보) 각급기관의 장은 다음 각 호에 해당하는 정보통신 운용현황을 관리하여야 하며, 제8조의 규정에 의한 심사분석에 첨부하거나 별도로 제출하여야 한다. 다만, 이미 제출한 경우에는 변동사항에 한하여 제출할 수 있다.
1. 정보통신시스템 운용현황
2. 정보통신망 세부 구성도
3. IP 할당현황
4. 주요 정보화사업 추진현황

제4장 국가용 보안시스템

제1절 공 통

제45조(사용) 각급기관의 장이 보안시스템을 사용하고자 할 때에는 국정원장이 개발·제작하거나 국정원장이 검토·승인된 제품을 사용하여야 한다.

제46조(정·부 책임자 운영) 각급기관의 장은 국가용 보안시스템을 운용하거나 관리를 담당하는 정·부 책임자를 임명하여야 한다.

제47조(암호문 보안관리) ① 암호전문은 일반으로 분류한다. 다만, 암호문을 복호화 하였을 경우 복호화된 평문은 해당 비밀등급으로 분류 관리하여야 한다.
② 암호문과 평문은 분리 보관하여야 한다.
③ 동일내용을 암호문과 평문으로 이중 송신하거나, 암호문을 전송한 후 이를 다시 평문으로 문의할 수 없으며 암호문과 평문을 혼용하여서는 아니 된다.

제48조(국가용 보안시스템 실태점검) ① 국정원장은 각급기관의 장과 협조하여 해당기관의 국가용 보안시스템 관리실태 등을 점검할 수 있다.
② 국정원장은 제1항에 의한 점검결과 드러나 문제점을 해당기관에 통보하고, 해당기관의 장은 이에 대한 보안대책을 강구하여야 한다.

제49조(복제·복사 금지) 국가용 보안시스템은 복제·복사할 수 없으며 다른 기관이나 개인에게 임의 대여할 수 없다.

제50조(사용 제한) ① 각급기관의 장은 국정원장이 승인하지 않은 보안시스템이나 외국에서 생산한 보안시스템을 무단으로 사용하여서는 아니 된다.
② 국가용 보안시스템은 주한 외국인 및 주한 외국기관(대사관, 외국군 등)에 제공할 수 없으며, 외국으로 무단 반출하여서는 아니 된다.
③ 제1항 및 제2항의 규정에도 불구하고 부득이하다고 판단되는 경우에는 사전에 국정원장의 승인을 받아 사용하거나 제공 또는 반출할 수 있다.

제51조(국가암호체계 보안관리) ① 암호개발 업무를 수행하는 자는 이를 비인가자에게 공개하거나, 비인가자에게 노출된 장소에서 국가 암호체계 및 운용 등에 대한 토의를 하여서는

아니 된다.

② 제1항의 규정에도 불구하고, 국정원장의 승인 하에 서약서(별지 제7호) 징구 등 보안조치를 한 경우에는 그러하지 아니한다.

③ 국가 암호체계와 관련된 사항을 알고 있는 자는 이를 학술·논문지, 간행물, 전시회 및 공개된 정보통신망 등을 통해 공개하여서는 아니 된다. 다만, 국정원장의 승인을 받은 내용은 공개할 수 있다.

제2절 암호장비

제52조(사용승인 요청) 각급기관의 장이 암호장비를 사용하고자 할 경우에는 다음 각 호에 정하는 사항을 구비하여 국정원장에게 제출하고 승인을 받아야 한다.

1. 사용목적
2. 사용기관
3. 암호장비의 종류, 소요량 및 산출근거
4. 관련 정보통신시스템 제원
5. 대상 정보통신망 구성도
6. 보안대책
7. 기타 참고자료

제53조(제작) ① 암호장비는 지정된 암호장비 제작업체에서 제작하여야 한다.

② 암호장비의 외부에는 일반적인 운용상의 기능, 형식승인번호, 기관번호 및 일련번호를 제외한 어떠한 표지도 하여서는 아니 된다.

③ 제작된 암호장비의 검사는 제작 의뢰한 기관장 책임 하에 행하여야 한다. 다만, 비닉 부분에 대한 검사는 국정원장에게 요청하여 실시하여야 한다.

제54조(설치) 암호장비 설치장소는 보안사고(분실, 도난, 피탈 등)의 방지를 위하여 다음 각 호의 제반 보안대책을 강구하여야 하며, 부득이한 경우에는 국정원장과 협의하여 조정할 수 있다. 다만, 암호장비에 대한 별도 운영체계가 수립된 경우에는 이를 따른다.

1. 보호구역 설정 운영
2. 이중 잠금장치가 된 보관함 설치 운용
3. 사진 촬영금지
4. 비인가자 출입통제
5. 화재예방 대책 등

제55조(등록) 암호장비 사용기관의 장은 암호장비를 설치한 후 30일 이내에 국정원장에게 별지 제8호 서식(암호장비 운용관리현황)에 의거 등록하여야 한다.

제56조(성능개선 등) 암호장비 사용기관의 장은 암호장비의 성능개선이나 운용 편의성 제고 등이 필요하다고 판단되는 경우에는 그 사유서를 작성하여 국정원장에게 요청하여야 한다.

제57조(운용 관리) ① 암호장비를 설치 운용하고 있는 각급기관의 장은 국가용 보안시스템 관리기록부(별지 제9호 서식)를 비치, 기록 유지하여야 한다.
② 암호장비의 비닉체계 및 키 운용체계와 관련된 서류 등 결과물(암호논리, 보안모듈, 키 주입기 등)은 비밀로 분류하여야 한다.
③ 암호장비의 고유명칭, 제원, 대상국소 및 수량 등 운용현황이 기록된 문서는 대외비 이상으로 분류하여야 한다.
④ 암호장비 취급책임자는 설치 운용중인 암호장비의 보관상태 및 정상 작동여부 등 이상 유무를 수시 점검하고, 그 결과를 국가용 보안시스템 점검기록부(별지 제10호 서식)에 월1회 기록 유지하여야 하며, 정보보안담당관은 점검여부를 확인하여야 한다.

제58조(비밀소통 기준) 암호장비의 비밀소통 기준은 기종 및 운용하고자 하는 정보통신망의 특성을 고려하여 장비 개발완료시 기종별로 국정원장이 정한다.

제59조(운반 및 전시) ① 암호장비는 취급책임자가 직접 운반하여야 하며, 이를 확인하기 위하여 국가용 보안시스템 증명서(별지 제11호 서식)를 사용한다.
② 암호장비를 운송하거나 전시하고자 할 경우에는 분실·피탈 등 사고를 방지하기 위한 보안대책을 강구하여야 한다.
③ 운송도중 보안조치가 필요할 경우에는 가까운 경찰서나 군부대에 암호장비의 보호를 요청할 수 있으며, 요청받은 기관은 필요한 조치를 지원하여야 한다.
④ 암호장비의 운반이나 전시 중에 사고가 발생한 경우에는 즉시 국정원장에게 통보하여 필요한 후속조치를 행할 수 있도록 하여야 한다.

제60조(정비) ① 암호장비 사용기관에서의 정비는 비닉부분을 제외한 일반부분으로 제한하며, 비닉부분의 정비는 암호장비 제작업체에서 행하여야 한다. 단, 비닉부분이 완전 밀폐된 별개의 구성품으로 되어 있을 경우에는 사용기관에서 예비용과 교체할 수 있다.
② 암호장비 정비장소는 보호구역으로 설정하여야 하며, 정비절차는 사용기관의 장이 정한다.
③ 사용기관의 정비요원은 암호취급인가를 받아야 한다.

제61조(파기) ① 암호장비 사용기관의 장이 암호장비를 파기하고자 할 때에는 다음 각 호에 정하는 사항을 국정원장에게 제출하고 승인을 받아야 한다.

1. 파기사유
2. 장비명칭, 수량 및 등록번호
3. 파기일시 및 장소
4. 파기방법
5. 파기자

② 암호장비 사용기관의 장은 긴급사태 발생 등으로 암호장비를 안전하게 보호할 수 없을 때에는 긴급 파기할 수 있으며, 파기 후 제1항 각 호의 사항을 국정원장에게 통보하여야 한다.

제62조(현황통보) 암호장비 사용기관의 장은 암호장비 운용관리 현황(별지 제8호 서식)을 작성, 익년도 6.30까지 국정원장에게 제출하여야 한다.

제63조(인계인수) ① 암호장비 운용관리 정·부 책임자 교체시에는 인계인수를 실시하여야 하며, 국가용 보안시스템 관리기록부(별지 제9호 서식)의 최종 기록 여백에 인계인수 사항을 기록 유지하여야 한다.

② 인계인수를 할 경우에는 다음 각 호 사항을 확인하여야 한다.

1. 암호장비의 종류와 수량
2. 납봉 또는 봉인표지의 이상유무
3. 암호장비의 정상 작동여부
4. 암호논리·키 수록매체(메모리카드 포함) 및 운용법 등 관련자료 이상 유무

제3절 암호 및 음어·약호자재

제64조(제작) ① 국정원장은 암호자재를 제작하여 필요한 기관에 배포한다. 다만, 필요시 사용기관에 제작을 위임할 수 있다.

② 국정원장은 각급기관이 공통으로 사용하는 음어자재를 제작 배부한다. 다만, 자체용 음어 및 약호자재는 국정원장의 인가를 받아 당해기관의 장이 제작 배부한다.

제65조(사용 신청) ① 암호 및 음어자재를 사용하고자 하는 각급기관의 장은 익년도 연간 암호자재 소요량(산하기관용 포함)을 파악, 매년 10.31한 암호 및 음어자재 신청서(별지 제12호 서식)에 의거 신청하여야 한다.

② 직제개편 및 특별한 요인발생 등으로 암호자재가 추가 소요되는 각급 기관의 장은 다음

각 호의 사항을 반영하여 즉시 국정원장에게 신청 하여야 한다.

1. 사용대상 및 용도
2. 자재명 및 수량
3. 자재형태 및 사용주기
4. 정보통신망도
5. 암호실 설치여부

제66조(등록 및 관리) ① 각급기관의 장은 자체 제작한 암호 및 음어·약호자재(이하 '암호자재 등'이라 한다)를 국정원장에게 등록하여야 한다.

② 암호자재등을 보유하고 있는 각급기관의 장은 별지 제9호 서식에 의한 국가용 보안시스템 관리기록부를 비치하고 용도별로 구분하여 기록 관리하여야 하며, 비밀관리기록부에는 등재하지 아니한다.

③ 암호자재등은 사용완료(이하 '반납용'이라 한다)·현용·미래용으로 구분하여 보관하되, 현용을 제외하고는 이를 포장한 후 봉인하여 보관함에 보관하여야 한다.

④ 암호자재는 암호실내 금고에 보관하고 음어·약호자재는 평시 상용이 가능하도록 별도 관리하되 일과 후에는 이중캐비닛 또는 금고에 보관하여야 한다.

⑤ 암호자재등의 보관함에는 암호자재등 이외의 비밀 또는 문건을 혼합 보관하여서는 아니된다.

⑥ 암호자재 취급자는 암호자재등에 대해 수시 점검하고 국가용 보안시스템 점검기록부(별지 제10호 서식)에 월1회 기록 유지하여야 하며, 정보보안담당관은 점검사항을 확인하여야 한다.

제67조(배부 또는 회수) ① 국정원장은 암호 및 음어자재를 정기적으로 각급기관에 배부하되 별지 제13호서식에 의한 인감등록이 되어 있는 자 또는 「국가기관 음어자재 운용매뉴얼」에 규정된 체계에 의해 신분확인이 가능한 자에 한하여 직접 배부하거나 회수한다. 다만, 직접 배부 또는 회수가 불가능할 때에는 비밀취급인가를 받은 사람 중 정책임자의 위임장을 소지한 자에게 배부 또는 회수할 수 있다.

② 각급기관이 소관분야에 대해 암호자재등을 배부 또는 회수하는 경우에는 인감등록이 되어 있는 자 또는 각급기관이 규정한 체계에 의해 신분확인이 가능한 자에 한하여 직접 배부 또는 회수하여야 한다.

③외교정보통신용 암호자재는 직접 배부 또는 회신하여야 한다. 다만,부득이한 경우는 국정원장이 지정하는 계통에 의하여 배부 또는 회수한다.

④ 암호자재등을 배부 또는 회수할 경우에는 등록번호와 국가용 보안시스템 증명서(별지 제11호 서식)의 기재내용과 일치여부 등을 확인하여야 하며, 제59조(운반 및 전시)의 제2항 내지 제4항

의 보안조치를 하여야 한다.
⑤ 사용기간이 만료된 암호자재 등은 지체 없이 배부기관의 장에게 반납한다.

제68조(취급 및 운용) ① 각급기관의 장은 암호자재 취급 필요성이 있는 자에 대하여 암호취급을 인가한 후 취급하도록 하여야 한다.
② 암호취급인가는 대한민국 국적소유자로서 비밀취급인가를 받은 자에 한하여 별도로 임명하여야 한다.
③ 암호자재등의 변경 운용지시는 제작기관의 장이 대외비로 하달한다.
④ 외교정보통신용 암호자재 중 공통용 암호자재는 본부 송신과 산하부서(해외공관 포함) 수신전용으로만 사용하여야 한다.
⑤ 지편식 암호자재 사용시 사용현황을 별지 제14호 서식(지편자재 사용기록부)에 기록하여 이중 또는 미사용이 발생하지 않도록 하여야 한다.

제69조(소통 기준) ① 암호자재는 Ⅱ급비밀 이하의 내용을 소통하는데 사용할 수 있다.
② 음어자재는 Ⅲ급비밀 이하의 내용을 소통하는데 사용할 수 있다.
③ 약호자재는 대외비 이하의 내용을 소통하는데 사용할 수 있다.
④ 암호자재등은 비밀이 아니더라도 국가이익을 해할 우려가 있는 내용을 정보통신수단으로 송수신할 경우에 사용할 수 있다.

제70조(암호실 설치 및 폐쇄) ①각급기관의 장은 암호자재를 활용하여 암호작업을 할 경우에는 다음 각 호의 구비요건을 갖춘 암호실을 설치 운용하여야 한다.
1. 통신소와 인접하고 비인가자 출입통제가 용이한 곳에 설치
2. 출입문 이중 잠금장치(자동잠금)와 창문에 철재 보호망 및 외부 투시 차단장치 설치
3. 출입문외 천장 등을 통한 외부통로 차단
4. 암호자재 보관용 금고 구비
5. CCTV, 지문인식기 등 과학보안장비 운용 등 경계 대책 및 안전지출 계획 수립
②암호실의 폐쇄는 각급기관의 장 책임 하에 행하고 암호실을 폐쇄할 경우에는 암호자재를 지체 없이 배부기관의 장에게 반납하여야 한다.
③각급기관의 장은 제1항 및 제2항에 의거 암호실을 설치하거나 폐쇄한 경우에는 농림수산식품부장관에게 그 내용을 통보하여야 한다.

제71조(암호실 출입통제) ① 암호실에는 해당기관의 장, 암호취급자 및 국정원장이 인가한 자 이외에는 출입할 수 없다.

② 암호실에는 별지 제5호서식(암호실 및 암호취급자 현황) 및 별지 제6호서식(암호실 출입자 기록부)에 의거 암호실 출입자를 통제하고 그 내용을 기록 유지하여야 한다.

제72조(암호실의 표지와 경비) ①암호실에는 출입제한표지 이외의 암호 취급을 나타내는 어떠한 표지도 하여서는 아니 된다.
②암호실은 무장 경비원에 의하여 경비되어야하며, 군(軍) 이외의 기관으로서 무장 경비원을 둘 수 없는 경우에는 이에 상당하는 특별 경비조치를 취하여야 한다.

제73조(암호실 검열) ①농림수산식품부장관이 임명한 암호실 검열관은 모든 암호취급기관에 대한 검열을 할 수 있다.
②암호실 검열관은 암호취급인가를 받은 자에 한하여 임명될 수 있으며, 검열관으로 임명된 자는 그 임무를 제 3자에게 위임하거나 대행하게 할 수 없다.

제74조(인계인수) ① 암호자재등을 취급하는 정·부 책임자가 교체되거나, 1개월 이상 부재중인 경우에는 암호자재등을 인계인수하여야 한다.
② 암호자재등을 인계인수할 때에는 국가용 보안시스템 관리기록부(별지 제9호 서식)의 최종기록 여백에 인계인수사항(명칭, 수량, 등록번호 등)을 기록 확인하여야 한다.

제75조(파기) ① 암호자재등의 파기는 일반파기와 긴급파기로 구분한다.
② 일반파기는 반납용 암호자재등을 파기하는 것으로서 회수한 자재는 제작기관의 장이 지정하는 자가 파기한다.
③ 긴급파기는 긴급사태 발생으로 암호자재의 보안관리가 곤란한 경우에 파기하는 것으로, 당해 사용기관의 장의 책임 하에 다음 각 호의 순서에 따라 파기한다.
1. 긴급한 사태가 발생하였을 때에는 상황 악화정도에 따라 반납용·미래용·현용 순으로 파기한다.
2. 현용 암호자재등을 계속 보유할 수 없을 때에는 공통용·단독용 순으로 파기한다.
3. 암호문과 평문 및 그 관련서류는 암호자재등의 파기에 앞서 파기하거나 이와 병행하여 파기한다.
④ 제2항 및 제3항에 따라 암호자재등을 파기한 경우에는 다음 각 호의 사항을 지체 없이 국정원장과 관계기관의 장에게 통보하여야 한다.
1. 파기일시 및 장소
2. 암호자재등의 수량 및 등록번호
3. 파기이유 및 방법
4. 파기자 및 참여자의 직책, 성명

제76조(현황통보) 각급기관의 장은 암호자재등의 운용결과 및 보유실태를 별지 제5호서식, 제14호 내지 제16호서식에 의거 종합 작성하여 익년도 1.31까지 국정원장에게 통보하여야 한다.

제4절 암호논리

제77조(개발) ① 각급기관이 사용하는 암호논리는 국정원장이 개발하여 보급한다. 다만, 각급기관의 장은 필요시 자체적으로 암호논리를 개발하여 사용할 수 있으며, 이 경우 국정원장의 안전성 평가·승인을 받아야 한다.

② 제1항의 규정에 의하여 암호논리를 개발하는 각급기관의 장은 개발실 보안대책을 강구 시행하여야 한다.

③ 암호논리를 개발하는 각급기관의 장이 국정원장에게 안전성 평가·승인을 요청하고자 할 경우에는 다음 각 호의 사항을 첨부하여야 한다.

1. 암호알고리즘, 소스코드 등 최종 비닉방식 및 체계 설명서
2. 안전성 평가 등 관련자료

제78조(요청) ① 암호논리를 제공받고자 하는 각급기관의 장은 운용하고 있는 정보통신시스템과의 적합성여부 검토와 키 관리방안 등 보안대책을 강구한 후 국정원장에게 암호논리를 요청하여야 한다.

② 암호논리를 요청할 경우에는 다음 각 호의 자료를 첨부하여야 한다.

1. 사용목적
2. 정보통신시스템 구성도 및 작동 프로토콜
3. 암호키 관리방안
4. 정보통신시스템 구성요소별 기능 및 제원
5. 보안서비스 요구사항

제79(설치 및 운용) ① 암호논리를 변경 운용하고자 하는 각급기관의 장은 국정원장의 안전성 평가·승인을 받은 후 사용하여야 한다.

② 암호논리를 운용하는 각급기관의 장은 암호논리와 키를 안전하게 관리하여야 하며, 주기적으로 키를 변경 운용하여야 한다.

제80조(보안관리) 승인된 암호논리의 세부구조를 알 수 있는 설계도, 소스코드 등은 비밀로 분류하고 암호논리를 개발하고자 하는 자는 제68조의 규정에 의거 암호취급인가를 받아야 한다.

제81조(반납 및 파기) 실용성이 상실되거나 유효기간이 만료된 암호논리는 국정원장에게 반납하거나 각급기관의 장의 책임 하에 파기(소자)하고 국정원장에게 그 결과를 통보하여야 한다.

제82조(현황통보) 암호논리를 사용하는 각급기관의 장은 매년말 기준으로 별지 제17호서식에 의거 암호논리 운용현황을 작성하여 익년도 6.30까지 국정원장에게 통보하여야 한다.

제5장 보안적합성 검증필 정보보호시스템

제83조(도입) 각급기관의 장은 소관 정보통신망을 보호하기 위하여 상용 정보보호시스템 또는 정보보호기능이 탑재된 정보통신시스템을 사용하고자 할 경우 '검증필 정보보호시스템'을 도입하여야 한다.

제84조(보안적합성 검증 요청) ① 각급기관의 장은 검증필 정보보호시스템으로 등재되지 아니한 제품을 도입할 경우 제11조제2항제3호에 따라 국정원장에게 보안적합성 검증을 요청하여야 한다.

② 보안적합성 검증 대상 상용 정보보호시스템은 「정보화촉진기본법」 또는 정보보호제품 국제상호인정협회(CCRA)에 의해 인증서가 발급된 것이어야 한다.

③ 각급기관의 장은 보안적합성 검증 요청시 다음 각 호의 자료를 국정원장에게 제출하여야 한다.

1. 별지 제18호 서식에 의거한 검증 신청서 1부
2. 별지 제19호 서식에 의거한 사용자 보안요구사항
3. 정보통신망 구성도 등 운용환경
4. 「정보화촉진기본법」 또는 국제상호인정협정(CCRA)에 의해 발행된 인증서 사본, 보안목표명세서, 평가보고서 각 1부
5. 암호논리가 포함된 경우 「암호모듈 시험 및 검증지침」에 의해 발행된 검증서 사본 1부 또는 암호기능 검증에 필요한 문서

제85조(보호시스템 관리자 지정) 각급기관의 장은 검증필 정보보호시스템 관리자(이하 '보호시스템 관리자'라 한다)를 임명 운용하여야 한다.

제86조(운용 및 보안관리) ① 검증필 정보보호시스템은 비인가자의 출입통제가 용이한 장소에 설치하여야 한다.

② 보호시스템 관리자는 정보보호시스템 설치시 요구되는 시험절차와 보안관리 기준을 사전에 수립·시행하고, 설치 결과에 대해서는 정보보안담당관의 승인을 받아야 한다.
③ 각급기관의 장은 운용요원에 대하여 다음 각 호의 사항에 대한 교육·훈련계획을 체계적으로 수립·시행하여야 한다.
1. 운용관리 직무지식
2. 시스템 취약성 분석 및 보안진단 방법
3. 보안사고 발생시 긴급 대응능력 등
④ 보호시스템 관리자는 검증필 정보보호시스템에서 P2P 등 업무에 불필요한 서비스 사용을 금지하고 관련서비스 포트를 차단하도록 패킷 필터링 정책을 설정하여야 한다.
⑤ 보호시스템 관리자는 주기적으로 다음 각 호의 사항을 점검하고, 월1회 정보보안담당관의 확인을 받아야 한다.
1. 검증필 정보보호시스템에 일반사용자 계정이 있는지 여부
2. 검증필 정보보호시스템 사용자 권한 설정의 적절성 여부
3. 검증필 정보보호시스템 기능에 영향을 줄 수 있는 프로그램 설치 및 은닉 여부
4. 검증필 정보보호시스템에 대한 비인가자의 물리적·기술적 접근 차단 대책
5. 주기적인 보안패치 및 업그레이드 여부
6. 비인가자의 침입여부를 확인하기 위한 시스템 접근기록 등
⑥ 각급기관의 장은 정보보호시스템을 설치할 때에 보안기능 설정을 위하여 국정원장에게 기술지원을 요청할 수 있다.

제87조(목적이외 사용제한) 각급기관의 장은 검증필 정보보호시스템을 사용할 경우, 설치목적 외 사용 및 보안기능의 임의변경 등을 하여서는 아니 된다.

제88조(원격관리 제한) ① 보호시스템 관리자는 검증필 정보보호시스템을 원격으로 관리하여서는 아니 된다. 다만, 부득이한 경우는 정보보안담당관의 승인 하에 원격으로 관리하되 다음 각 호의 사항을 준수하여야 한다.
1. 원격관리 시간을 최소화
2. 원격관리자의 접속비밀번호 임시 부여 및 소통내용 암호화 등 보안대책 적용
3. 인가되지 않은 원격관리가 수행되는지 주기적 확인 점검
② 정보보안담당관은 제1항에 의한 승인을 위하여 다음 각 호의 사항을 확인하는 등 보안조치를 수행하여야 한다.
1. 원격 접속할 사용자, 사용자계정, 비밀번호
2. 접속주소, 접속시간

3. 원격접속 사유(출장, 전산망 유지보수 등)
4. 원격접속 후 사용자계정 및 비밀번호 회수 등 조치사항

제89조(사용자 관리) 보호시스템 관리자는 복수의 사용자가 시스템을 공동 사용하는 경우 사용자에 대한 효율적 관리를 위하여 다음 각 호의 사항을 반영하여 사용자관리대장을 유지하여야 한다.
1. 사용자이름, 소속기관 및 부서, 사용자계정, 비밀번호
2. 사용자계정 부여일자 및 유효기간
3. 사용자의 현재상황(근무, 휴가, 출장, 사용중지 등)

제90조(긴급사태 관리) 보호시스템 관리자는 인위적·자연적으로 발생되는 시스템 장애, 가동중지 등 긴급사태에 대비하여 위하여 제32조를 참조하여 다음 각 호의 백업 및 복구절차 등을 수립·시행하여야 한다.
1. 긴급사태에 대비한 조직, 임무 및 업무처리 절차
2. 백업시설 구성, 백업방법 및 절차
3. 정상상태로의 복구절차
4. 긴급사태에 대비한 정기적 훈련과 교육실시 등

제91조(현황통보) 각급기관의 장은 별지 제21호서식에 의거 검증필 정보보호시스템 운용현황 등을 종합 작성하여 제8조에 규정한 정보보안업무 심사분석에 포함, 국정원장에게 통보하여야 한다.

제6장 사이버공격 대응

제92조(사이버공격 초동조치) ① 각급기관의 장은 소관 정보통신망에 대하여 해킹, 웜·바이러스 유포 등 사이버공격 인지시 피해실태를 파악하고 관련 로그자료 보존 및 필요시 전산망 분리 등 초동조치를 하여야 한다.
② 단순 웜·바이러스 감염 등 경미한 사항은 해당기관이 자체 처리 후 국정원장에게 관련사항을 통보하여야 한다.
③ 전산망 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 하여서는 아니 된다.

제93조(사이버공격 대응활동) ① 각급기관의 장은 소관분야의 사이버공격 대응절차를 수립·시행하고 이행실태를 지속 확인 점검하여야 한다.
② 각급기관의 장은 국정원장이 경보 발령시 소관분야 직원을 대상으로 관련사항을 전파하고 대응조치를 이행하며 진행상황을 예의주시하는 등 대응절차에 따라 신속하게 대처하여야 한다.
③ 각급기관의 장은 제2항에 따른 경보 단계별 조치사항을 국정원장에게 통보하여야 한다.
④ 국정원장은 제1항 및 제2항과 관련하여 정보통신망에 대한 안전성을 확인할 수 있다.
⑤ 제1항 내지 제4항에 구체적으로 명시되지 않은 사항은 「국가 사이버안전관리 규정」과 「국가 사이버안전 매뉴얼」에 따른다.

제7장 USB메모리 등 보조기억매체 보안관리

제94조(USB메모리 및 관리시스템 도입절차) ①보조기억매체 보안관리 해당기관의 장은 USB메모리를 도입할 경우 그 제품의 안전성을 검증하기위하여 『전자정부구현을위한행정업무등의전자화촉진에관한법률시행령』 제34조를 준용하여 농림수산식품부장관에게 보안 적합성 검증을 의뢰하여야 한다.
②국가정보원장은 보안적합성 검증시 다음 각 호에 해당하는 필수 보안기능의 유무를 검토한 후 그 결과를 적합성 검증결과에 반영한다.
1. 사용자 식별·인증기능
2. 지정데이터 암·복호화 기능
3. 저장된 자료의 임의 복제 방지기능
4. 분실시 저장데이터의 보호를 위한 삭제 기능
③제2항 제2호의 지정데이터 암·복호화 기능은 자료를 USB메모리에 보관하는 경우로 한하며, 비밀자료를 PC에 보관 하거나 소통하고자 할 경우에는 국가정보원이 개발·보급한 암호장비·자재 등 국가용 보안시스템을 사용하여야 한다.
④보조기억매체 보안관리 해당기관의 장은 운용중인 보조기억매체를 안전하게 관리하기 위하여 보조기억매체 관리시스템을 구축할 수 있다. 이 경우 별지 제22호 내지 별지 제28호 서식에 갈음할 수 있다.

제95조(보조기억매체 사용) ①보조기억매체 보안관리 해당기관은 보조기억매체를 등록한 후 사용하여야 한다.
②보조기억매체의 등록방법은 제97조의 규정에 따라 각급기관별 별지 제22호 내지 별지 제24호 서식을 이용하여 보조기억매체 관리대장에 등재하는 것을 말한다.

제96조(보조기억매체 사용제한) ①보조기억매체 보안관리 해당기관은 등록된 보조기억매체만 사용할 수 있으며 업무목적 이외 사적인 용도로 사용할 수 없다. 다만, 공인인증서용(업무용, 개인용)에 한하여 등록 후 개인소지 및 사용을 하게 할 수 있다.
②보조기억매체 보안관리 해당기관의 장은 그 소속직원에게 공지·교육을 통하여 보조기억매체의 임의 사용을 제한하여야 하고 이에 대하여 주기적인점검을 실시하여야 한다.

제97조(보조기억매체 관리책임자) ①보조기억매체 보안관리 해당기관의 보조기억매체는 각 팀장 또는 과장 책임하에 관리하는 것을 원칙으로 하며 그 팀장 또는 과장을 '보조기억매체 관리책임자'라 칭한다.
②보조기억매체 관리책임자는 별지 제22호 내지 별지 제24호 서식의 일반용, 비밀용 그리고 공인인증서용 보조기억매체 관리대장을 각각 비치하여야 한다.
③보조기억매체 관리책임자는 보조기억매체 관리대장에 최종 변경된 보조기억매체의 등록현황을 등재하여야 하며 사본 1부를 정보보안담당관에게 제출하여야한다.
④보조기억매체 관리책임자는 월 1회 이상 보조기억매체 수량 및 보관상태를 점검하고 별지 제25호 서식에 따라 확인·서명하여야 한다.
⑤보조기억매체 관리책임자는 보조기억매체의 반·출입을 통제하여야 하며 별지 제26호 서식에 따라 기록하여야 한다. 이때 반·출입은 업무상 목적(별지 제26호서식의 '용도'참조)에 한한다. 다만, 사적소지가 허용된 공인인증서용은 제외한다.
⑥보조기억매체 관리책임자는 소속직원이 미등록 보조기억매체를 사용하거나 공인인증서용 보조기억매체에 업무자료를 보관하지 않도록 감독하여야 하며 이를 위반한 사실을 발견 또는 확인하는 즉시 정보보안담당관에게 통지하여야 한다.

제98조(정보보안담당관의 책무) ①정보보안담당관은 소속기관 내에서 사용하는 보조기억매체 등록 현황을 파악하여야 한다. 이 경우 각 부서 팀·과별보조기억매체 관리대장 사본을 비치·관리하는 것으로 갈음할 수 있다.
②정보보안담당관은 각 팀·과별 보조기억매체 관리책임자가 별지 제27호 서식에 따라 보조기억매체 라벨 작성 및 별지 제28호 서식에 따라 불용처리확인을 요청하는 경우에는 확인한 후 날인 하여야 한다.
③정보보안담당관은 보조기억매체를 일괄 구입하여 필요한 부서에 보급할 수 있다.
④정보보안담당관은 미등록 또는 공인인증서용 보조기억 매체에 업무자료를 보관하는 것을 인지한 경우에는 수록된 자료현황을 파악하는 등의 경위조사를 실시하여야 한다.
⑤정보보안담당관은 대외비 이상 비밀이 보관된 보조기억매체를 무단 반출하거나 미등록 또는 공인인증서용 보조기억매체에 비밀을 보관하고 있는 경우에는 경위조사를 실시하여야 한다.

⑥정보보안담당관은 제5항에 따라 조사를 실시한 결과, 비밀 유출이 우려되거나 유출 징후가 있는 경우에는 지체 없이 농림수산식품부장관에게 보안사고 조사를 의뢰하여야 한다.

제99조(보조기억매체의 구분 및 관리요령) ①보조기억매체는 일반용, 비밀용(대외비 포함) 그리고 공인인증서보관용으로 구분한다.

②일반용 보조기억매체(이하 '일반용' 이라 한다)의 관리요령은 다음과 같다.

1. 일반용에는 일반자료만 보관하여야 하며 별지 제22호 서식의 보조기억 매체관리대장에 기록하여야 한다.
2. 일반용은 캐비넷 등에 안전하게 보관하여야 한다.
3. 일반용에는 별지 제27호 서식과 같이 기입·표시하여야 한다.
4. 보조기억매체 관리번호는 팀·과명, 일반, 연번으로 한다. 이 경우 팀·과명은 약칭을 사용할 수 있다.(예 : 총무과-일반-01, 총무과-일반-02, 총무-일반-03 등)

③대외비 이상 자료를 보관하는 비밀용 보조기억매체(이하 '비밀용'이라 한다) 관리요령은 다음과 같다.

1. 비밀용을 사용할 경우에는 별지 제23호 서식의 보조기억매체 관리대장에 기록하여야 하며 대외비 이상의 기밀자료가 수록되어 있는 경우에는 비밀관리기록부에도 등재·관리하여야 한다.
2. 비밀용은 비밀자료와 동일하게 이중캐비넷 또는 금고에 보관하여야 한다.
3. 비밀용에는 별지 제27호 서식과 같이 기입·표시하여야 한다.
4. 비밀용을 사용하여 비밀작업을 하는 경우 그 작업을 완료하거나 일시 중단할 때에는 PC에서 즉시 분리하여야 한다.
5. 비밀용은 해당 비밀을 생산하거나 보관할 필요가 있는 경우 비밀등급별로 각각 보조기억매체를 마련해야 하며, 하나의 보조기억매체에 등급이 다른 비밀 또는 대외비를 혼합 보관해서는 아니 된다.
6. 관리번호는 팀·과명, 비밀등급, 연번으로 한다. 이 경우 팀·과명은 약칭을 사용할 수 있다. (예 : 총무과-Ⅱ급-01, 총무과-Ⅲ급-01, 총무-대외비-01 등)

④공인인증서보관용 보조기억매체(이하 '공인인증서용' 이라 한다)의 관 리요령은 다음과 같다. 다만, 공인인증서를 CD-R 형태의 매체에 보관하고 있는 경우에는 아래의 관리요령 준수대상에서 제외할 수 있다.

1. 공인인증서용에는 공인인증서 이외의 자료를 저장할 수 없으며 별지 제24호서식의 보조기억매체 관리대장에 기록하여야 한다.
2. 공인인증서용은 소지·사용에 유의하여야 한다.

3. 공인인증서용에는 별지 제27호 서식과 같이 기입· 표시하여야 한다.
4. 보조기억매체 관리번호는 팀·과명, 인증, 연번으로 한다. 이 경우 팀·과명은 약칭을 사용할 수 있다.(예 : 총무과-인증-01, 총무과-인증-02, 총무-인증-03 등)

제100조(보조기억매체 불용처리 및 재사용) ①업무상 목적으로 사용한 보조기억매체는 불용처리시 물리적 파기를 원칙으로 하며 그 사실을 보조기억매체관리대장에 기록하여야 한다.
②일반용을 타부서 이전 또는 용도를 전환하여 사용하고자 할 경우에는 수록된 자료를 완전히 삭제·포맷 후 사용하여야 한다.
③비밀용을 일반용 또는 다른 등급의 비밀용으로 전환하여 사용할 경우 또는 일반용을 외부기관에 이전하여 사용하는 경우에는 파일 삭제·포맷 및 필요한 경우 자성소거 등의 파일복원 방지대책을 강구하여야 한다.
④공인인증서용을 타부서 이전 또는 퇴직 후 사용하고자 할 경우 업무용은 그 기록의 삭제·변경 등 적절한 조치 후 사용할 수 있고 개인용은 그 등록의 해지를 요한다.
⑤보조기억매체를 불용처리하거나 재사용하는 경우에는 별지 제28호 서식에따라 정보보안담당관의 확인을 받아야 하며 확인서를 보관하여야 한다.

제101조(보조기억매체의 분실, 소각시 대처방안) ①보조기억매체 취급자는 보조기억매체의 분실 또는 소각 등의 사유가 발생한 즉시 관리책임자에게 그 사실을 보고하여야 한다.
②관리책임자는 보조기억매체의 분실 또는 소각사실을 보고받은 즉시 정보보안담당관에게 통지하여야 한다. 다만, 공인 인증서용은 등록을 해지하고 보조기억매체 취급자에게 사용상의 주의를 환기시켜야 한다.
③정보보안담당관은 일반용의 분실 또는 소각 사실을 통지받거나 인지한 경우에는 자체 조사를 실시하고 재발방지 대책을 강구하여야 한다.
④정보보안담당관은 비밀용의 분실 또는 소각 사실을 통지 받거나 인지한 경우에는 지체 없이 농림수산식품부장관에게 그 사실을 통보하여야 한다.

제102조(보조기억매체 고장·훼손, 오인 삭제·포맷시 대처방안) ①보조기억매체의 고장, 자료의 훼손 또는 자료의 오인삭제, 포맷시 제100조의 규정에의거 불용처리를 원칙으로 한다. 다만, 자료의 복구가 필요한 경우 상용 소프트웨어 활용 및 민간업체에 의뢰할 수 있다.
②제1항에 따라 민간업체에 의뢰하는 경우에는 정보보안담당관과 협조하여 보안서약서 징구 등 적절한 보안대책을 강구하여야 한다. 다만, 비밀자료가 포함된 경우에는 우선 정보보안담당관을 경유하여 농림수산식품부장관에게 통보하여야 한다.

제8장 정보시스템 저장매체 불용처리

제103조(정보시스템 저장자료 보안조치책임) 정보시스템을 폐기·양여·교체·반납하거나 외부수리(이하 '불용처리'라 한다)를 위하여 당해 기관 외부로 반출할 경우 저장매체에 저장된 자료의 보안조치책임은 당해 기관의 장이 진다.

제104조(정보시스템 저장자료 삭제) 정보시스템 저장매체에 저장된 자료를 삭제할 경우는 다음과 같다.

1. 정보시스템의 사용연한이 경과하여 폐기 또는 양여할 경우
2. 정보시스템 무상 보증기간중 저장매체 또는 저장매체를 포함한 정보시스템을 교체할 경우
3. 정보시스템의 임대기간이 만료되어 반납할 경우
4. 고장 수리를 위한 외부 반출 등 당해 기관이 정보시스템 저장매체를 보안통제 할 수 없는 환경으로 이동이 필요한 경우
5. 기타 정보시스템 사용자 변경 등으로 저장자료 삭제가 필요하다고 판단되는 경우

제105조(저장자료 삭제책임) ①개인에게 지급된 정보시스템의 저장자료는 사용자 본인 책임하에 삭제하여야 한다.

②홈페이지 등 각 부서가 공통적으로 사용하는 정보시스템은 정보보안담당관 책임하에 저장자료를 삭제하여야 한다.

제106조(저장자료 삭제방법의 지정) ①각급기관의 정보보안담당관은 별지 제29호를 준용하여 당해 기관의 실정에 맞게 정보시스템별 저장자료 삭제방법을 사전 지정하여야 한다.

②당해 기관내에서 정보시스템의 사용자가 변경된 경우, 비밀처리에 사용한 정보시스템은 완전포맷 3회 이상, 그 외의 정보시스템은 완전포맷 1회 이상으로 저장자료를 삭제하여야 한다.

③본 지침에서 정한 별표와 다른 방법으로 저장자료를 삭제하고자 할 때에는 사전 농림수산식품부장관과 협의하여야 한다.

제107조(저장자료 삭제확인) ①각급기관의 정보보안담당관은 정보시스템을 불용 처리할 경우 사전 저장자료 삭제여부를 확인하여야 한다.

②정보시스템에 저장된 자료의 삭제를 외부업체에 의뢰할 때에는 정보보안담당관이 입회하여 삭제 절차·방법 준수여부 등을 확인 감독하여야 한다.

제108조(정보시스템 도입시 보안조치) ①각급기관의 장은 정보시스템의 도입시 고장수리 등을

위해 공급업체가 저장매체를 교환·반출해 갈 경우에 대비, 저장자료 삭제방법 등 저장매체 보안조치 방안을 계약서상에 포함하여야 한다.
②정보시스템을 임차 사용할 때에는 임차기간 만료후 반납시 당해 시스템의 저장자료 삭제방법 등 저장매체 보안조치 방안을 임차계약서상에 포함하여야한다.

제109조(정보시스템 외부반출시 보안조치) ①불용처리 등을 위해 정보시스템을 외부로 반출할 경우 사전 정보보안담당관의 통제를 받아야 하며 정보보안담당관은 그 현황을 기록 유지하여야 한다.
②각급기관의 장은 저장매체의 고장수리·저장자료 복구 등을 외부에 의뢰할 경우 저장매체에 저장된 자료의 유출 방지를 위해 수리 또는 복구 참여자에 대해 보안서약서 집행·교육 등 필요한 보안조치를 하여야 한다.
③각급기관의 장은 정보시스템을 불용 처리할 경우 당해 시스템의 사용기관·부서·사용자 등을 인식할 수 있는 표시를 모두 제거하여야 한다.

제110조(소자장비 등의 적합성 검증) 각급기관의 장은 정보시스템의 저장자료를 삭제하는 장비나 소프트웨어를 도입할 경우 사전 국가정보원에 제품성능에 대한 적합성 검증을 의뢰하여야 한다.

제111조(삭제방법의 지속 개선) 각급기관의 장은 농림수산식품부를 경유하여 국가정보원과 긴밀히 협의하여 정보시스템에 저장된 자료의 삭제방법·절차 등을 지속 개선하여야 한다.

제9장 정보보안측정 및 사고처리

제112조(정보보안측정) ① 국정원장은 정보통신망에 대한 보안취약성을 진단하기 위하여 정보보안측정을 실시한다.
② 정보보안측정은 다음 각 호의 경우에 실시한다.
1. 정보보안 사고가 발생하여 정보통신망의 보안취약성 진단이 요구될 때
2. 국가 중요 정보통신기반시설에 대한 사이버공격이나 도청 등으로부터의 보호대책이 필요한 경우
3. 정보통신수단에 의하여 국가기밀 유출 및 암호체계의 누설 우려가 있는 경우
4. 정보통신시스템에 대한 보안성 검토와 국가용 보안시스템 설치 등과 관련하여 국정원장의

보안대책 확인이 요구되는 경우

5. 각급기관의 장이 정보통신망에 관한 보안취약성 점검 또는 종합 진단이 필요하다고 판단하여 요청할 경우
6. 기타 국가안보상 필요하다고 판단되는 경우

제113조(정보보안 위규) ① 정보보안 위규사항은 별표1과 같다.

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

제114조(정보보안사고 처리 및 조사) ① 각급기관의 장은 별표2의 정보 보안사고가 발생한 때에는 즉시 피해를 최소화하도록 조치를 취하고 다음 각 호의 사항을 국정원장에게 통보하여야 한다.

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

② 국정원장은 사고조사를 실시하고 동일유형의 사고가 발생하지 않도록 제반 보안조치를 권고할 수 있다.

③ 각급기관의 장은 정보보안사고 관련자를 관련규정의 징계기준에 의거 처벌하고 사고조사 및 징계결과에 대해 국정원장에게 통보하여야 한다.

제10장 보 칙

제115조(시행세칙) 각급기관의 장은 정보보안 업무수행을 위하여 이 지침에 반하지 아니하는 범위 내에서 자체적으로 세부규칙을 정할 수 있다.

제116조(준용) 이 지침에 명시되지 않은 사항은 다음 각 호의 관련규정 및 지침에 따른다.

1. 정보 및 보안업무 기획·조정 규정
2. 보안업무규정
3. 보안업무규정 시행규칙
4. 국가 사이버안전 관리규정
5. 전자문서 보안조치 수행지침

6. 국가 정보보안기술 연구개발 지침
7. 연도 보안업무 수행지침
8. 국가 사이버안전 매뉴얼
9. 정보시스템 저장매체 불용처리지침
10. USB메모리 등 보조기억매체 보안관리지침
11. 국가 정보보안 기본지침
12. 기타 관련법령

부 칙

①(시행일) 이 지침은 발령일부터 시행한다.
②(지침 등의 폐지) 본 지침의 시행과 동시에 「각급기관 도입을 위한 상용 정보보호시스템 보안성 검토 지침」은 폐지한다.
③(준용규정의변경) 제94조 제1항의 『전자정부구현을위한행정업무등의전자화촉진에관한법률시행령』 제34조를 2007년 7월 1일부터 『전자정부법』 제27조로 대체한다

【별 표 1】

정보보안 위규사항

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

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

【별 표 2】

정보보안사고 유형

조	내 용	항	세 부 내 용
1	정보통신시스템 및 정보통신실	(1)	정보통신망에 대한 해킹·악성코드의 유포
		(2)	비밀이 저장된 PC 분실
		(3)	승인 없이 정보통신시스템내 비밀 저장
		(4)	정보통신시스템 및 정보통신실 파괴
2	암호장비	(1)	암호장비 분실 및 피탈
		(2)	암호장비 파손 및 임의파기
		(3)	암호장비의 복제·복사
		(4)	비인가 암호장비 사용
		(5)	암호장비 비닉체계 특성 및 제원 노출
		(6)	암호장비 키 운용체계 노출
3	암호 및 음어·약호자재	(1)	암호·음어·약호자재의 분실 및 누설
		(2)	암호·음어·약호자재의 파손 및 임의파기
		(3)	암호·음어·약호자재의 임의제작 사용
		(4)	세부 비닉체계 노출
4	정보자료	(1)	주전산기·대용량 전자기록(DB) 손괴
		(2)	비밀자료의 유출·파괴·변조 및 평문 소통
		(3)	전자공문서 위조

【별지 제1호 서식】

정보보안업무 세부 추진계획

1. 활동목표

2. 기본방침

3. 세부 추진계획

분야별	사 업 명	세 부 추 진 계 획	주 관· 관련부서	비 고

4. 전년도 보안감사·지도방문시 도출내용과 조치계획

도 출 내 용	조 치 계 획	담당부서

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

제2편

【별지 제2호 서식】

정보보안업무 심사분석

1. 총 평

2. 주요성과 및 추진사항

3. 세부 사업별 실적분석

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

지 적 상 항	조치계획	담당부서

5. 애로 및 건의사항

6. 첨부(정보통신망 및 검증필 정보보호시스템 운용현황 등)

【별지 제3호 서식】

전파측정 활동 결과보고

1. 활동 목표

○ 측정기간 및 지역

○ 측정장비

○ 참여기관 및 인원

2. 측정결과 내용

기간	측정지점	통신구간	주파수 (MHz)	신호세기 (dBM)	취약여부	비 고
						* 디지털, 아날로그 구분

3. 분석 및 평가

4. 조치 및 대책

【별지 제4호 서식】

전산장비 관리대장

연번	소 속	취급자(성명)	단말기·PC 및 서버		비 밀 번 호				부여일자	해제일자
			관리번호	기종·성능	장비별	파일별	망접속시 취급자			
							사용자계정	비밀번호		

【별지 제5호 서식】

암호실 및 암호취급자 현황

구분 / 부서	암 호 실				암 호 취 급 자				비 고
	인가	운용	과부족	변동 내용	인가	운용	과부족	변동 내용	
총 계									

【별지 제6호 서식】

암호실 출입자 기록부

소 속	직 급	성 명	직 책	용 무	출입 일시	서 명	인가자인	비고

【별지 제7호 서식】

서 약 서

본인은 년 월 일부로 국가용 보안시스템과 관련한 업무(연구개발, 제작, 입찰, 기타)를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 나는 국가용 보안시스템과 관련된 소관업무가 국가기밀 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. 국가보안법 제4조 제1항제2호·제5호(국가기밀 누설 등)
   나. 형법 제99조(일반이적) 및 제127조(공무상 비밀의 누설)
   다. 군형법 제80조(군사기밀 누설)
   라. 군사기밀보호법 제9조(누설) 및 제13조(업무상 누설)

년 월 일

서약자 소속 직급 주민등록번호
직위 성 명 인

서 약 소속 직급 주민등록번호
집행자 직위 성 명 인

【별지 제8호 서식】

암호장비 운용관리현황

기관명 :　　년　월　일 현재

순위	시스템명	등록번호	설치장소	상대국소	회선 및 방식	설치일자	비고

【별지 제9호 서식】

국가용 보안시스템 관리기록부

<암호장비용>

장비명	배부(수령)					회수(반납)				변동사항				비고
	일시	수량	등록번호	대상기관	증빙번호	일시	수량	등록번호	증빙번호	일시	근거	수량	확인	

<암호 및 음어·약어자재용>

자재명칭	수령(제작)				배부				회수		변동사항				비고
	일시	수량	등록번호	발행처	일시	수량	등록번호	발행처	일시	수량	일시	수량	반납처	확인	

* 국가용 보안시스템 관리기록부는 한권으로 만들고 암호장비, 암호자재 등 용도별로 색인 구분하여 사용

【별지 제10호 서식】

국가용 보안시스템 점검기록부

<암호장비용>

점검일시	장비명칭	점 검 사 항				점 검 관	
		납 봉	암호화	회 선	작 동	성 명	서 명

※ 점검요령

- ○ 납봉상태 : 암호장비 외장 불법개봉 여부 점검
- ○ 암호화상태 : 암호화 또는 비화상태 점검
- ○ 회선상태 : 암호장비와 정보통신장비간 접속코드 등 연결상태 점검
- ○ 동작상태 : 암호장비의 성능저하 고장여부 등 정상작동 여부 점검

<암호 및 음어·약호자재용>

점검일시	자재명칭	부 수	보관상태	점 검 관		비 고
				성 명	서 명	

* 국가용 보안시스템 점검기록부는 필요에 따라 암호장비, 암호 및 음어·약호자재 등 용도별로 분류 또는 통합권으로 사용

【별지 제11호 서식】

국가용 보안시스템 증명서

<암호장비용>

○ 증명서 번호 :		구 분 : (배부, 반납, 파기, 장비)		
발 신 :		수 신 :		
아래 암호장비 및 부품(대)를 (배부, 반납, 폐기, 정비의뢰)하였음		아래 암호장비 및 부품(대)를 (수령, 회수, 폐기, 정비)하였음		
일 자 : 년 월 일		일 자 : 년 월 일		
소 속 :		소 속 :		
성 명 : (인)		성 명 : (인)		
구 분	암호장비 명칭	구 분	등 록 번 호	비 고

<암호 및 음어·약호자재용>

○ 증명서 번호 :		구 분 : (배부, 반납, 파기, 정비)		
발 신 :		수 신 :		
아래 기록된 (암호, 음어, 약호) 자재 (부)를 (배부, 반납, 파기) 하였음		아래 기록된 (암호, 음어, 약호) 자재 (부)를 (수령, 회수, 파기) 하였음		
일 자 : 년 월 일		일 자 : 년 월 일		
소 속 :		소 속 :		
성 명 : (인)		성 명 : (인)		
구 분	자재 명칭	수 량	등 록 번 호	비 고

【별지 제12호 서식】

암호 및 음어자재 신청서

자재명	수령 지역	실수령 기 관	소요 부수	산 출 내 역	보유 부수	과부족	비고

<작성요령>

- ○ 수령지역 : 중앙청사, 과천청사, 대전청사, 지자체별
- ○ 소요부수 : 소요자재 부수기준 산출
- ○ 산출내역 : 세부 운용부서 및 소요부수
- ○ 보유부수 : 현용 자재기준 산출
- ○ 과 부 족 : 소요부수 - 현재 보유부수
- ○ 비 고 : 조직 신설·증편·통합 등 참고사항 기재

【별지 제13호 서식】

암호취급자 인감등록서

1. 기 관 명 :

2. 변동 및 등록일자 : 년 월 일

가. 정 책임자

인 적 사 항		인 감	서 명
직급 및 성명			
직 책			
주민등록번호			
비밀취급등급			

나. 부 책임자

인 적 사 항		인 감	서 명
직급 및 성명			
직 책			
주민등록번호			
비밀취급등급			

다. 실무자

인 적 사 항		인 감	서 명
직급 및 성명			
직 책			
주민등록번호			
비밀취급등급			

【별지 제14호 서식】

지편자재 사용기록부

장비명	관리번호	일시	전 문 액 표			난 수 사 용				소자일시	소자자	비고
			번호	송수구분	조수	부터		까지				
						쪽	행	쪽	행			

<작성요령>

○ 전문액표

– 번호 : 암호전문 일련번호

– 송수구분 : 수발신으로 구분

– 조　　수 : 암호전문 조수

【별지 제15호 서식】

암호 개발요원 현황

구 분	인 가	운 용	과 부 족	변 동 내 용	비 고
총 계					

【별지 제16호 서식】

암호 및 음어·약호자재 보유현황

기 관 명	자 재 명 칭	수 량	등 록 번 호	비 고

【별지 제17호 서식】

암호논리 운용현황

기관명	운용부서	운용시스템	수량	설치일	비 고

【별지 제18호 서식】

보안적합성 검증 신청서

신청기관	기 관 명		담당부서	
	도입목적			
	운용환경	□유선망 □무선망 □유·무선통합망	운용기관	
	주요 보안기능 요구사항			
대상 시스템	개발사 (판매사)	* 개발사와 판매사가 사이한 경우 판권소유자 기재	대 표 자	
	주 소		전화번호	
	시스템명		평가등급	
	평가기관		인증기관	
	담당자		E-mail	
비 고				

* 복수의 시스템을 신청하는 경우, 별도 출력하여 대상시스템란에만 기재

【별지 제19호 서식】

사용자 보안요구사항

1. 개 요
   ○ 목 적

2. 정보보호시스템 운영환경
   ○ 인가되어야 할 최대 사용자
   ○ 정보통신망 환경
      – 속도
      – 통신규약
      – 유·무선 연동

3. 보안기능 요구사항
   ○ 형상(S/W 또는 H/W)
   ○ 보안감사기능
      – 기록방식
      – 저장방식 및 보존기간
      – 출력방식
   ○ 식별 및 인증기능
   ○ 정보보호시스템 접속방법
      – 접속경로
      – 통신규약
      – 암호화 방식
   ○ 내부 데이터 보호
   ○ 비인가자에 대한 접근통제

4. 활용 대상업무

【별지 제20호 서식】

정보통신시스템 보안적합성 검증 제출물 목록

문서분류	작 성 요 소	비 고
보안목표 명세	○ 보안 위협요소 및 보안 목적 ○ 보안 정책 ○ 운영환경 ○ 보안기능 목록	각 1부
기본 및 상세 설계	○ 보안기능 작동 및 외부 인터페이스 ○ 시스템 구조 및 인터페이스 ○ 시스템을 구성하는 보안 및 비보안 구성요소 ○ 보안기능 제공방법	
형상관리	○ 버전 부여방법 ○ 형상변경 통제 방법	
시스템 설명	○ 시스템 설치 절차 및 보안관리 방법 ○ 보안기능 운영 방법 ○ 사용자 인터페이스 등 사용방법 ○ 안전한 시동, 백업, 유지보수 및 운용 등의 절차 ○ 하드웨어 보안모듈의 자체진단 기능 및 진단결과 예시	
취약성 분석결과	○ 취약성 분석 및 대응방법	
시험결과	○ 개발과정 단계별 시험항목에 대한 시험목적, 절차 및 결과	
소스코드	○ 소스코드 또는 하드웨어 설계도	

【별지 제21호 서식】

검증필 정보보호시스템 운용현황

운용부서	제 품 명	수 량	설치일자	보호 대상망	보안기능	비고

【별지 제22호 서식】

보조기억매체 관리대장(일반용)

<관리책임자 : >

연번	관리번호 (S/N)	매체 형태	등록일자	취급자	불용 처리일자	불용처리방법 (재사용 용도)	비고
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

【별지 제23호 서식】

보조기억매체 관리대장(일반용)

<관리책임자 : >

연번	관리번호 (S/N)	등급	매체 형태	등록일자	취급자	불용처리일자	불용처리방법 (재사용 용도)	비고 (사유)
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								

【별지 제24호 서식】

보조기억매체 관리대장(공인인증서용)

<관리책임자 : >

연번	관리번호 (S/N)	형태	등록일자	취급자	용도	해지일자	해지사유
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

【별지 제25호 서식】

보조기억매체 점검대장

<관리책임자 : >

점검일시	현 보유수량					이상 유무	점검관		비고 (서명)
	Ⅱ급	Ⅲ급	대외비	일반	인증		성명	서명	

【별지 제26호 서식】

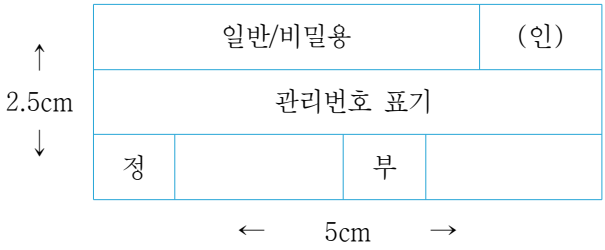
보조기억매체(전산장비 포함) 반출·입 대장

<관리책임자 : >

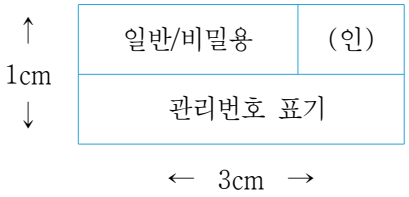
장비명	관리번호 (시리얼번호)	사용자	용도	전출입 일시 (입·출 구분)	확인

【별지 제27호 서식】

보조기억매체 라벨



< 디스켓, 이동형 HDD 서식 >



< USB · CD 등 서식 >

가. 同 서식을 만들어 보조기억매체 중앙의 적절한 위치에 부착

나. 첫 번째 줄에는 일반/비밀용은 정보보안담당관의 직인을 날인하고 공인인증서용은 관리책임자의 직인을 날인

다. 두 번째 줄에는 보조기억매체 관리번호 표기

라. 세 번째 줄의 '정'란에 관리책임자 · '부'란에 취급자 표기
(USB메모리 및 CD의 경우 생략 가능)

마. 보조기억매체의 크기를 고려하여 서식 · 글자 크기 조정 가능

【별지 제27호 서식 예시】

일반용			(인)
총무과-일반-01			
정	이순신	부	홍길동

대외비용			(인)
총무과-대외비-01			
정	이순신	부	홍길동

공인인증서용			(인)
총무과-인증-01			
정	이순신	부	홍길동

일반용	(인)
총무과-일반-01	

Ⅱ급비밀용	(인)
총무과-Ⅱ급-01	

공인인증서용	(인)
총무과-인증-01	

【별지 제28호 서식】

보조기억매체 불용처리 확인서

아래와 같이 보조기억매체(　종　점) 불용처리 및 보조기억매체(　종　점) 재사용에 대해 확인을 요청함

연번	관리번호 (S/N)	매체형태	사유	불용처리	재사용
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

확인일자 :　　년　월　일

요 청 자 :　소속·직책　　O급 성명 :　　(인)

확 인 자 : 정보보안담당관　O급 성명 :　　(인)

【별지 제29호 서식】

정보시스템 저장매체·자료별 삭제방법

저장자료 / 저장배체	공개자료	민간자료 (개인정보 등)	비밀자료 (대외비 포함)
플로피디스크	㉮	㉮	㉮
광디스크 (CD·DVD 등)	㉮	㉮	㉮
자기테이프	㉮·㉯중 택일	㉮·㉯중 택일	㉮
반도체메모리 (EEPROM 등)	㉮·㉯중 택일	㉮·㉰중 택일	㉮·㉰중 택일
	완전포맷이 되지 않는 저장매체는 ㉮ 방법 사용		
하드디스크	㉱	㉮·㉯·㉰중 택일	㉮·㉯중 택일

㉮ : 완전포맷(소각·파쇄·용해)

* 비밀이 저장된 플로피디스켓·광디스크 파쇄시에는 파쇄조각의 크기가 0.25mm 이하가 되도록 조치

㉯ : 전용 消磁장비 이용 저장자료 삭제

* 소자장비는 반드시 저장매체의 磁氣力보다 큰 磁氣力 보유

㉰ : 완전포맷 3회 수행

* 저장매체 전체를 '난수'·'0'·'1'로 각각 중복 저장하는 방식으로 삭제

㉱ : 완전포맷 1회 수행

* 저장매체 전체를 '난수'로 중복 저장하는 방식으로 삭제

❸ 농림수산식품부 당직 및 비상근무규칙

전문개정 1984. 7. 2. 농 수 산 부 훈령 제 582 호
개정 1985. 5. 1. 농 수 산 부 훈령 제 605 호
개정 1988. 1.13. 농 림 수 산 부 훈령 제 661 호
개정 1988. 5.20. 농 림 수 산 부 훈령 제 668 호
개정 1989. 8.25. 농 림 수 산 부 훈령 제 695 호
개정 1992. 7.22. 농 림 수 산 부 훈령 제 747 호
개정 1994. 2.21. 농 림 수 산 부 훈령 제 781 호
개정 1998. 3.17. 농 림 부 훈령 제 934 호
개정 1999.12.30. 농 림 부 훈령 제1009호
개정 2008. 5.20. 농림수산식품부 훈령 제 13 호

제1장 총 칙

제1조(목적) 이 규칙은 국가공무원 당직 및 비상근무규칙('08. 3. 4)의 규정에 의하여 농림수산식품부와 소속기관 및 단체의 당직 및 비상근무에 관한 사항을 규정함을 목적으로 한다.

제2장 당직근무

제1절 통 칙

제2조(당직의 구분) ①당직(재택당직을 포함한다. 이하 같다)은 일직과 숙직으로 구분한다.
②일직은 공휴일에 두며, 그 근무시간은 토요일이 아닌 정상 근무일의 근무시간에 준 한다.
③숙직근무시간은 정상근무시간 또는 일직근무시간이 종료된 때로부터 다음날의 정상근무 또는 일직근무가 개시될 때까지로 한다.

제3조(숙직근무자의 교대취침 등) ①각 기관의 장은 숙직근무자가 2인 이상인 때에는 일정한 시간을 정하여 교대로 취침하게 할 수 있고, 1인일 때에는 기관의 기능 및 성격 등을 고려하여 농림수산식품부장관의 승인을 얻어 제12조의 규정에 의한 당직임무를 수행한 후 일정한 시간을 정하여 취침하게 할 수 있다.
②각 기관의 장은 업무상 불가피한 경우를 제외하고 숙직근무자(재택근무자를 제외한다.)에 대하여 그 근무종료시각이 속하는 날의 근무시간의 일부를 휴무하게 하여야 한다.

제4조(당직명령 및 변경) ①당직명령은 당해 기관의 장이 근무예정일 7일전까지 하여야 한다.
②당직명령을 받은 자가 출장·휴가 기타 부득이한 사유로 당직근무를 할 수 없는 경우에는 지체 없이 당직명령자에게 신청하여 당직근무일의 변경·승인을 얻어야 한다.

제5조(당직신고 및 인계·인수) ①당직근무자는 당직근무 개시 시간 30분전에 당직명령권자에게 당직신고를 하여야 한다. 다만, 공휴일의 당직근무자는 그 전일인 정상근무일에 당직신고를 하여야 한다.
②당직근무자는 제1항의 당직신고 전에 당직 주무부서로부터 당직근무일지 기타 필요한 당직용 비품을 인수·확인하여야 하고, 당직근무를 마칠 때에는 이를 당직 주무부서에 인계하여야 한다. 다만, 공휴일인 경우에는 일직근무자와 숙직근무자간에 인계·인수한다.

제6조(당직자의 준수사항) ①당직근무자는 근무상의 공무 아닌 용무로 근무구역(재택당직근무처를 포함한다)을 이탈하여서는 아니 되며, 당직자로서의 품위를 손상하거나 당직근무에 지장이 있는 행위를 하여서는 아니 된다.
②당직근무자는 복장을 단정히 하여야 하고, 별표에 의한 당직근무표찰을 패용하여야 한다. 다만, 재택당직근무자는 그러하지 아니하다.

제7조(당직실의 위치) 각 기관의 장은 방범, 방호, 방화 등 당직근무수행에 가장 적당한 위치에 당직실을 설치·운영하여야 한다. 다만, 재택근무를 실시하거나 당직근무를 하지 아니하는 기관은 당직실을 설치·운영하지 아니할 수 있다.

제8조(당직실의 전화시설 등) 당직실에는 전화시설을 하고 그 전화번호를 관할 체신관서에 통보하여야 한다.

제9조(당직차량의 운영) 농림수산식품부장관이 필요하다고 인정하는 기관은 당직업무수행을 위한 당직차량을 운영하여야 한다. 다만, 운전원의 수가 부족하고, 당해 기관의 기능 및 성격상 당직차량이 크게 필요하지 아니하다고 판단되는 경우에는 그러하지 아니한다.

제2절 기관의 당직

제10조(당직의 편성) ①중앙행정기관의 당직근무자는 2인 이상으로 하고, 중앙행정기관이 아닌 기관의 당직근무자는 1인으로 한다. 다만 당해기관의 기능과 실정을 감안하여 필요한 경우에는 이를 조정하여 운영할 수 있다.

②2이상의 기관이 동일 건물 안에 위치하여 각 기관별로 당직근무를 운영 할 필요가 없는 때에는 상호 협의하여 당직근무를 통합 운영할 수 있으며, 이 경우에는 기관별 당직근무자를 1인으로 할 수 있다. 다만, 당해기관의 당직근무대상인원이 적어 기관별 당직근무자를 1인으로 하는 것이 곤란한 경우에는 상호 협의하여 통합된 기관의 당직근무자 총수를 최하 1인까지로 하여 운영할 수 있다.

③각 기관의 장은 다음 각호의 1에 해당하는 경우에는 별도의 당직근무를 실시하지 아니할 수 있다.

1. 당직근무대상인원이 극히 적어 1인이 당직근무를 하여도 1인당 2주 1회를 초과하여 당직근무를 하는 경우로서 근무시간 외에는 문서처리 및 업무연락 등의 필요성이 적은 경우에 한하여 당해 기관장이 제4항제1호 및 기타 필요한 보완대책을 강구한 경우
2. 당해 기관의 기능 또는 성격상 일정시간대별로 교대근무를 실시하는 등 정상근무가 상시 계속되는 경우
3. 상시 상황실을 운영하고 상황실에 당직임무를 부여한 경우

④각 기관의 장은 당해 기관의 기능 및 성격 등을 고려하여 다음 각호의 보완대책을 강구하고 당직근무자로 하여금 재택당직근무를 하게 할 수 있다. 이 경우 중앙행정기관의 경우에는 행정안전부장관과의 협의를 거쳐 실시하여야 하며, 소속기관은 기관별 보완대책내용과 시행일자 등을 농림수산식품부장관에게 보고하여야 한다.

1. 무인전자경비장치의 설치 또는 경비업체 등의 유인경비 실시
2. 당직용 이동전화의 확보와 착신통화전환조치 등 통신연락체계의 강구
3. 일과시간 종료시부터 일정시간 사무실 대기근무

제11조(당직책임자) ①당직근무자가 2인 이상인 경우에는 책임자 1인은 감독직위에 있는 자이어야 한다.

1. 농림수산식품부 본부 및 산하 외청 : 4~5급 공무원을 책임자로 한다.(이에 상당하는 특정직 또는 별정직 포함)
2. 소속관서 : 4~5급 공무원을 책임자로 한다. 다만, 4~5급 공무원의 수가 현저히 적을 때에는 6급이하 공무원을 책임자로 할 수 있다.
3. 소속단체 : 과장급을 책임자로 한다. 다만, 과장급 직원의 수가 현저히 적을 때에는 바로 하위직급의 자를 책임자로 할 수 있다.

제12조(당직근무자의 일반업무) ①당직근무자는 다음 각호의 사항을 성실히 이행함으로써 사고의 발생을 미연에 방지하여야 한다.

1. 방범·방호·방화 기타 보완상태의 순찰·점검

2. 경비원 기타 정상근무 시간외의 근무자에 대한 복무상태의 점검
3. 문서의 수발·인계 또는 관리
4. 전화민원의 응대

②각 기관의 장은 사무실 별로 별지 제1호 서식의 보완점검표를 작성·비치하고 최종퇴청자가 이를 점검하도록 하여야 하며, 당직근무자는 최종 퇴청자가 기록한 점검사항을 확인하여야 한다. 다만, 당직근무자는 무인전자경비장치 등 보안장비가 작동중인 보호구역안의 보완점검표 점검사항은 이를 확인하지 아니할 수 있다.

③당직근무자는 당직근무 중에 접수된 문서나 발생한 업무가 긴급한 처리를 요하는 사항일 때에는 이를 지체 없이 주무 부서에 연락하거나 소속 기관의 장에게 보고하고 필요한 조치를 하여야 한다.

제13조(당직근무자의 긴급사태시의 임무) ① 당직근무자는 청사에 화재가 발생한 때에는 지체 없이 다음 각 호의 조치를 하여야 한다.

1. 관할 소방관서에의 연락
2. 청사내의 화재경보
3. 자체 소화시설에 의한 진화작업

②당직근무자는 외부 침입자 등이 있을 때에는 지체 없이 다음 각 호의 조치를 하여야 한다.

1. 관할 경찰서에서의 연락
2. 무기고 등 중요시설의 경비강화

③당직근무자는 제1항, 제2항의 경우와 기타 긴급한 사태가 발생한 경우에는 그 상황에 따라 소속기관의 장이나 상급기관의 당직근무자·당직사령(당직사령을 둔 경우에 한한다)또는 당직총사령에게 지체 없이 이를 보고하고, 그의 지시를 받아 필요한 조치를 하여야 한다. 다만, 특히 긴급을 요하여 상급기관 당직근무자 등의 지시를 기다릴 시간적 여유가 없을 때에는 긴급사태발생보고와 함께 필요한 조치를 한 후 지체 없이 그 경과를 보고하여야 한다.

④당직근무자는 각급기관의 장이 당직실(당직실을 설치·운영하지 아니하는 경우에는 당직주무부서를 말한다. 이하 같다)에 비치하는 당직근무자의 긴급사태시 행동요령을 숙지하여야 한다.

제14조(당직실의 비품) ①당직실에는 다음 각호의 서류 및 물품을 비치하여야 한다.

1. 별지 제2호 서식의 당직근무일지
2. 기관 간 비상연락체계도
3. 직원 비상소집대장
4. 향토예비군 비상소집대장

5. 민방위대원 비상소집대장
6. 관계기관의 당직실 전화번호부
7. 비상열쇠 보관함
8. 농림수산식품부당직및비상근무규칙
9. 기타 당직근무에 필요한 물품

②제1항 제1호의 당직근무일지는 기관의 특수성에 따라 당해기관의 장이 그 서식의 내용을 변경하여 사용할 수 있다.

③제1항 제3호 내지 제5호의 각 소집대장에는 전화·도보·교통수단 등의 연락방법이 2가지 이상 기재되어야 한다.

제3절 기관의 당직

제15조(당직감사) ①농림수산식품부장관은 필요한 경우에 각 기관의 당직근무상태를 수시로 감사하거나 소속공무원으로 하여금 이를 감사하게 할 수 있다.

②각 기관의 장은 소속기관 및 피감독기관의 당직근무상태를 수시로 감사하거나 소속공무원으로 하여금 이를 감사하게 할 수 있다.

제16조(당직근무상태의 점검) ①기관별 당직근무자는 직근소속기관 및 피감독기관의 당직근무상태를 2회 이상 순찰 또는 전화 등에 의한 방법으로 확인·점검하여야 한다.

②기관별 당직근무자는 당직근무상태의 확인·점검 대상기관이 동일행정구역이 아닌 먼 거리에 위치하고, 상호간 전용 통신시설이 설치되어 있지 아니한 경우에는 제1항의 규정에 의한 당직근무상태의 확인·점검을 실시하지 아니할 수 있다. 다만, 비상시 또는 특이상황의 발생시에는 그러하지 아니한다.

③각 기관의 장은 자체실정에 맞게 당직 및 비상근무태세 점검계획을 수립, 매월 1회 이상 점검을 실시하여야 한다.

제17조(당직근무태만자 등에 대한 조치) 당직및비상근무규칙(행정안전부령 및 농림수산식품부령)을 위반한 당직근무자에 대하여는 특별한 사유가 없는 한 징계 또는 기타 필요한 조치를 하여야 한다.

제3장 비상근무

제1절 통 칙

제18조(비상근무의 목적) 비상근무는 비상사태 하에서 업무수행의 효율화를 도모하기 위하여 발령한다.

제19조(비상근무의 종류) 비상근무는 그 상황에 따라 다음과 같이 구분하여 발령한다.
1. 비상근무 제1호 : 전시·사변 또는 이에 준하는 비상사태 하에서 발령한다.
2. 비상근무 제2호 : 전시·사변 또는 이에 준하는 비상사태의 징후가 농후하거나 천재지변 기타 이에 준하는 사유로 사회불안이 조성되고 사회질서가 교란될 우려가 있는 경우에 발령한다.
3. 비상근무 제3호 : 제1호 및 제2호 이외의 비상근무가 필요하다고 인정되는 경우에 발령한다.

제20조(발령 및 해제) ①농림수산식품부장관은 행정안전부장관으로부터 비상근무의 발령을 통보받아 전국 또는 일정지역을 지정하여 별지3호 서식의 비상근무발령서에 의하여 발령하되, 신속히 소속직원을 비상근무에 임하도록 하여야 한다. 해제의 경우에도 또한 같다.
②농림수산식품부장관은 필요하다고 인정할 때에는 소속직원에 대하여 비상근무를 발령할 수 있으며, 소속기관의 장은 농림수산식품부장관의 승인을 얻어 비상근무를 발령할 수 있다. 다만, 특별히 긴급을 요하는 경우에는 비상근무를 발령하고 사후에 승인을 얻을 수 있다.
③제2항의 규정에 의하여 비상근무를 발령하거나 승인한 경우에는 지체없이 비상의 종류, 발령일시, 사유 등을 보고받아 행정안전부장관을 거쳐 국무총리에게 보고하여야 한다.

제21조(비상근무의 요령) ①비상근무의 발령 중에는 부득이한 경우를 제외하고는 출장을 억제하고 소속직원의 소재를 항상 파악하여야 하며, 비상근무의 종류별로 다음 기준에 따라 휴가를 제한하고 휴일과 야간에는 소속직원을 비상근무 하도록 하여야 한다.
1. 비상근무 제1호가 발령된 때에는 연가를 중지하고 소속직원의 3분의 1이상의 비상근무 한다.
2. 비상근무 제2호가 발령된 때에는 연가를 중지하고 소속직원의 5분의 1이상이 비상근무 한다.
3. 비상근무 제3호가 발령된 때에는 부득이한 경우를 제외하고는 연가를 억제하고 소속직원의 10분의 1이상이 비상근무 한다.
②각 기관의 장은 비상근무인원이 일부 부서 또는 일부 직급에 편중되지 않도록 부서별 인원, 직급, 업무의 성질 및 기관의 특수성을 감안하여 비상근무를 함으로써 비상근무 기간 중 업무수행의 계속성이 유지되고 비상근무의 목적이 달성될 수 있도록 하여야 한다. 이 경우 비상근무인원에는 문서보관자, 타자요원, 통신요원 등 사무보조에 필요한 인원이 포함되도록 하여야 한다.

제22조(비상연락체계) ①정상근무시간이 아닌 때에 제20조 제1항의 규정에 의하여 비상근무를 발령 또는 해제하고자 할 경우에는 이를 각 기관에 신속히 연락하여야 한다.
②정상근무시간이 아닌 때에 제20조 제2항의 규정에 의하여 비상근무를 발령 또는 해제하고자 하는 경우에는 각 기관의 당직체계에 따라 제1항내지 제3항의 규정에 준하여 조치하여야 한다.

제23조(비상소집) ①정상근무시간이 아닌 때에 제20조 제1항 및 제2항에 의한 비상근무가 발령된 경우에는 기관별 당직근무자는 지체 없이 소속기관의 장에게 제10 제1항의 규정에 의한 통합된 기관의 당직근무자는 해당기관의 장에게 이를 보고하고, 해당기관의 전직원이 비상소집이 되도록 연락하여야 한다. 다만, 비상근무 제3호가 발령된 경우에는 발령자 또는 소속기관의 장의 명에 따라 필요한 해당인원이 비상소집이 되도록 연락하여야 한다.
②각 기관의 장 또는 당직근무자는 당해기관의 비상소집결과를 별지 제3호 서식의 "비상소집결과보고서"에 의하여 제22조의 비상연락체계에 따라 보고하여야 하고, 소속기관의 장은 농림수산식품부장관에게, 농림수산식품부장관은 행정안전부장관을 거쳐 국무총리에게 보고하여야 한다.

제24조(비상근무기간 중의 당직) ①제20조제1항의 규정에 의하여 비상근무 중일 때에는 비상근무기관의 당직근무를 중지한다. 다만, 정상근무위치 외에서 비상근무를 하는 기관은 그러하지 아니하다.
②당직근무자가 당직근무 중 비상근무가 발령되어 제1항의 규정에 의하여 당직근무를 중지할 때에는 당직주무부서에 당직근무일지 등을 인계하여야 한다.
③당직 명령자는 정상근무시간 외에 비상근무가 해제된 때에는 지체 없이 당직근무를 하도록 조치하여야 한다.

제25조(연습상황의 부여금지 등) 비상근무기간 중에는 비상근무발령자의 지시 또는 승인 없이 연습상황을 부여하여서는 아니 된다.

제4장 연락체계의 유지

제26조(직원연락체계의 유지) ①농림수산식품부 소속직원은 근무시간이 아닌 때에도 항상 소재파악이 가능하도록 연락체계를 유지하여야 한다.
②소속직원은 주소·전화번호 등 연락체계의 유지를 위하여 필요한 사항의 변경이 있을 때에는 이를 즉시 소속기관의 장에게 신고하여야 한다.

제26조2(필수요원의 지정) ①각급 기관의 장은 정상근무시간이 아닌 때에 긴급사태가 발생할 경우에 대비하여 소속직원 중 일부를 미리 필수요원으로 지정하고, 긴급사태 발생시 신속히 필요한 조치를 하도록 하여야 한다.
②제1항의 필수요원은 비상소집시 1시간 이내에 응소 가능한 자를 우선적으로 지정하되, 문서보관자, 타자요원, 통신요원 등 사무보조에 필요한 인원이 포함되도록 하여야 한다.

제27조(직원비상소집대장의 정비·보완) ①각 기관의 장은 제26조의1 제1항의 규정에 의한 신고를 받은 때에는 제14조제1항 제3호에 규정된 직원 비상소집대장을 즉시 정비·보완하여야 하며, 월 1회 이상 이를 점검하여야 한다.
②각 기관의 장은 복무관계 업무를 담당하는 소속직원 중에서 직원 연락체계의 유지 및 직원비상소집대장의 정비·보완을 위한 책임자 및 보조자 각1인을 지정하여야 한다.

제5장 보 칙

제28조(위임규정) 이 규칙의 시행에 관하여 필요한 사항은 각 기관의 장이 정한다.

부 칙(1984. 7. 2. 훈령 제582호)

①(시행일) 이 규칙은 공포한 날로부터 시행한다.
②(훈령의 폐지) 농림부훈령 제 호('81. 12. 3)의 "농수산부당직및비상근무규칙"은 이 규칙 시행과 동시 폐지된다.

부 칙(1985. 5. 1. 훈령 제605호)

이 규칙은 1985년 5월 1일부터 시행한다.

부 칙(1988. 1. 13. 훈령 제601호)

이 규칙은 1988년 1월 20일부터 시행한다.

부 칙(1988. 5. 20. 훈령 제668호)

이 규칙은 1988년 5월 20일부터 시행한다.

부 칙(1989. 8. 25. 훈령 제695호)

이 규칙은 1989년 8월 25일부터 시행한다.

부 칙(1992. 7. 22. 훈령 제582호)

이 규칙은 1992년 7월 22일부터 시행한다.

부 칙(1994. 2. 21. 훈령 제781호)

이 규칙은 1994년 2월 21일부터 시행한다.

부 칙(1998. 3. 17. 훈령 제934호)

①(시행일) 이 규칙은 공포한 날로부터 시행한다.

②(훈령의 폐지) 농림수산부훈령 제781호('94. 2. 21)의 "농림수산부당직 및 비상근무규칙"은 이 규칙 시행과 동시 폐지된다.

부 칙(1999. 12. 30. 훈령 제1009호)

이 규칙은 2000. 1. 1부터 시행한다.

부 칙(2008. 5. 20. 훈령 제 13호)

이 규칙은 발령한 날부터 시행한다.

[별지 제1호서식] <개정 1999.12.21>

보안점검표

22㎜ ↓

7㎜ ↑

25㎜ ▶

년도

실·과명 :

구분 / 점검일	① 서류보관상태		② 청소상태		③ 소등상태		④ 화기단속상태		⑤ 문단속상태		⑥ 비고	점검시각 및 점검자				결재
												최종퇴청자		당직근무자		
	퇴청자 최종	근무자 당직	퇴청자 최종	근무자 당직	퇴청자 최종	근무자 당직	퇴청자 최종	근무자 당직	퇴청자 최종	근무자 당직		점검시각	성명	점검시각	성명	

28㎜ ▼ 9㎜ → 7㎜ ←

60㎜ ▼ ○ ▲ 70㎜ ▼ ○ ▲ 60㎜

14행

8㎜ ↑

비고 : 1. 서류보관상태 : 책상위 서류방치 여부와 캐비닛, 책상 등의 잠금여부
2. 화기단속상태 : 컴퓨터·프린터·복사기·선풍기 및 전열기(커피포트·전기히터 등)의 전원스위치의 차단여부와 배선주변에 인화물질이 있는지 여부

1203-12일(1)
83.6.17 승인

268㎜×190㎜
(신문용지(양면인쇄) 54g/㎡)

[별지 제2호서식]

당 직 근 무 일 지

20 . . .(요일 숙직)

결재		

당직자	①당직명	②소속	③직명	④성명	⑤서명	문서처리상황						
						⑥종류	⑦발송			⑧접수	⑨인계	⑩비고
							문서번호	수신처	제목			
⑭지은시사받항			⑮조사치항									
⑯지사시한항			⑰조과치확결인			특근자현황						
						⑪소속·실과	⑫인원수		⑬특근시간			
							외 명					
⑱보사고항			⑲인사계항	1. 물품 2. 문서 3. 기타			외 명					
							외 명					
							외 명					

0204-4-2C
72.4.24 승인

268mm×380mm
(백상지 70g/㎡)

청사내의순찰점검사항

①순찰시간	②발견사실 및 처리개요	③순찰자	④순찰시간	⑤발견사실 및 처리개요	⑥순찰자
시 분부터 시 분까지		㊞	시 분부터 시 분까지		㊞
시 분부터 시 분까지		㊞	시 분부터 시 분까지		㊞

⑦연락사항	⑧연락기관	⑨수화자 소속·직명	⑩수화자성명	⑪송화자성명	⑫이상유무

⑬비 고	

[별지 제3호서식]

비상소집결과보고서

1. 기관명 :
2. 비상근무발령 접수일시 : 년 월 일 시 분
3. 비상소집 응소현황

구분		총원	응소 대상 인원	응소 인원	응소율 (%)	시간별 응소현황			
						1시간 이내		1시간 후 2시간 이내	
						인원	비율	인원	비율
총계	계								
	필수요원								
	일반직원								
본부	계								
	필수요원								
	일반직원								
소속기관	계								
	필수요원								
	일반직원								

보고요령

1. 응소대상인원은 총원에서 교육·출장·휴가자 등을 제외한 인원을 말한다.
2. 응소현황보고
   중앙행정기관의 본부소속 응소현황은 시간별로 즉시 전화보고하고, 소속기관 응소현황은 집계와 동시에 본부를 포함하여 총괄 보고한다.
   (우선 전화보고 후 서면보고)
3. 삭제 <1998.2.2>

15011-13211보
87.10.29 승인

190mm×268mm
(신문용지 54g/㎡)

④ 외국기관(인원) 면담 및 자료제공 지침

(농림부 총무 07000-55 : 2001. 2. 23)

Ⅰ. **목 적** : 국제화·정보화 추세에 대비하여 농림부 관련 중요정보가 직원들의 외국기관(인원)과의 공·사적인 면담이나 자료제공을 통해서 흘러나가는 것을 막기 위해 이를 효율적으로 관리함으로써 국가 중요정보에 대한 경각심을 제고하고자 함.

Ⅱ. **근거 규정 : 보안업무내규 제68조(보안업무세부시행계획수립)**

Ⅲ. **적용 범위 : 농림부 각실국(과) 소속 직원**

Ⅳ. **세부 지침**

1. 외국기관(인원) 면담

가. 농림부 소속직원의 외국기관(인원) 면담을 효율적으로 관리하기 위해 **총무과를 외국기관(인원) 면담 전담부서로 지정**한다.

나. 농림부 소속직원(이하 직원이라 한다)은 외국기관(인원)으로부터 업무와 관련하여 개인적인 면담 요청을 받은 경우에는 사전에 **별첨1 양식**에 의거 **보안담당관(총무과장)을 경유하여 농림부장관의 승인**을 득하여야 하며, **별첨2 양식**에 의거 사후에 **결과보고**를 하여야 한다.

다. 직원이 외국기관(인원)을 면담할 경우에는 불가피한 경우를 제외하고는 **민원상담실을 이용**하여야 한다.

라. 직원은 외국정보기관(인원)의 의도적 접촉이나 특정분야 자료에 대해 지속적으로 요구받는 등 **보안상 특이사항**을 발견할 경우에는 **보안담당관을 경유하여 국정원에 통보**하여야 한다.

마. 직원은 주한 외국기관직원, 외국기자, 상사원 등을 회원으로 하는 **공·사적인 단체모임에 가입하는 경우**에는 사전에 **별첨3의 양식**에 의거, **보안담당관을 경유하여 농림부장관의 승인**을 받아야 한다.

2. 외국기관(인원) 자료제공

가. 외국기관(인원)의 자료제공 요구를 효율적으로 관리하기 위해 **농림부 국제농업국 국제협력과를 자료제공 전담부서로 지정**한다.

나. 각 처리과는 부서별 또는 개인별로 외국기관(인원)에 대하여 자료를 제공하거나 브리핑을 금지한다. 다만, 비밀보호협정이나 양해각서 등 관계법령에 의한 경우에는 그러하지 아니하다.

다. 처리과에서 외국기관(인원)으로부터 **자료제공 요구를 받은 경우**에는 **별첨4의 양식**에 의거하여 **국제협력과에 통보**한다.

라. **국제협력과**는 처리과의 통보사항에 대하여 요청기관, 요청목적, 타당성 등 제공자료의 **사전 보안성을 철저히 확인·검토**한 후 **농림부 장관의 승인을 득한후 제공 여부를 처리과에 통보**한다.

마. 국제협력과는 제공자료의 보안성검토를 함에 있어, 동자료의 제공으로 인하여 **국익을 저해하거나 국익에 민감한 영향**을 줄 수 있다고 판단되는 사항에 대해서는 **보안담당관에게 보안심사위원회 심의를 요청**할 수 있다.

<별첨1 양식>

외국기관(인원) 면담요청 신고서

소 속	직·성명	면담기관(인원)	면담내용	예상문제점

년 월 일

신고자 (인)

보안담당관 보안성 검토의견	장 관

<별첨2 양식>

외국기관(인원) 면담 결과 보고서

소 속	성 명	면담기관(인원)	면담 내용

<별첨3 양식>

외국기관(인원)이 포함된 단체가입 신청서

소 속	성 명	가입 단체	목적 및 주요활동내용

년 월 일

신청자 (인)

보안담당관 보안성 검토의견	장 관

<별첨4 양식>

외국기관(인원) 자료요청 신청서

소 속	성 명	요청기관(인원)	요청자료 내용

년 월 일

신고자 (인)

국제협력과장 보안성 검토의견	장 관

5 특정직위에 대한 비밀취급 인가 및 해제 처리 지침

1. 목 적

임무 및 직책상 보직과 동시에 비밀취급이 수반되는 직위에 대하여 별도의 비밀취급인가 절차를 정함으로써 신속한 업무처리와 보안업무의 효율을 기하고자 함.

2. 근거규정

농림수산식품부 보안업무시행세칙 제19조(훈령 제14호, 2008. 5. 20)

3. 세부지침

가. 특정직위의 범위(당연직 인가대상자)

○ 제1차관, 제2차관
○ 국·단·관장 등 고위공무원으로 보한 국장급 이상
○ 각 국(단, 관)의 주무과장
○ 각 국(단, 관)의 주무담당 및 주무서무
○ 운영지원과의 보안담당 사무관 및 주무관
○ 비상계획관실 소속 직원

나. 비밀취급인가 등급 : Ⅱ급 비밀

다. 비밀취급인가의 절차

특정직위 보직자는 보직과 동시에 「보안업무시행규칙」 제5조에 의한 별지 제1호서식의 서약서를 보안담당관에게 제출함으로써 비밀취급인가 절차에 갈음한다.

라. 비밀취급인가의 해제

특정직위 보직자 중 타 기관 전출이나 비밀 취급이 불필요한 직위에 보직 시에는 당연 해제된다. 이 경우 별도의 해제신청 없이 보안담당부서(운영지원과)에서 인사발령문서 등에 근거하여 해제 조치한다.

마. 특정직위 비밀취급인가자의 관리

특정직위 비밀취급인가자는 보안담당부서(운영지원과)에서 인가와 동시에 「특정직위비밀취급인가대장」에 등재하여 관리하고 보직변경 후에도 계속적인 비밀취급인가가 필요한 경우 별도의 비밀취급인가 신청절차 없이 「비밀 및 암호자재 취급인가대장」으로 이기하여 비밀취급의 자격을 계속 유지할 수 있도록 한다.

Ⅲ 기타 비밀관리에 관한 규정

❶ 정부비밀문서 발간관리지침

(조달청 자재 43161-58463, 2003. 10. 2)

1. 정부비밀문서 발간업체 관리기준

조달청이 관리하는 정부비밀문서 발간업체(이하 "비밀발간업체"라 한다)에 대한 관리요령은 본 기준에 의한다.

가. 적용범위

비밀발간업체(인쇄, 공판, 프린트)에 대한 시설기준, 인가요건, 인가취소 및 제재에 관하여 적용한다.

나. 시설기준

(1) 비밀발간업체의 시설기준은 다음과 같다.
다만, 사업수행을 위하여 특별한 사유로 정부기관의 청사를 사용하는 경우에는 예외로 할 수 있다.

㈎ 인쇄업체는 서울특별시인쇄공업협동조합에 가입된 업체로서 영업면적 165평방미터(50평)와 다음 각 호의 시설을 구비하여야 한다.
1) 전자조판기(입력기) 5대
2) 제판기(5절) 1대
3) 옵셋(또는 마스터) 인쇄기 2대
4) 재단기(반절) 1대

(2) 비밀발간업체로 인가되면 즉시 비밀보관용기(이중캐비넷 또는 대형금고) 3개 이상을 비치하여야 한다.

다. 인가기준

(1) 비밀발간업체에 대한 인가는 "나"항에 규정한 시설기준을 구비하고, 당청에 등록된 업체로서 다음사항 중 각호에 해당하는 업체를 대상으로 한다.

㈎ 중앙행정기관의 장이 추천한 업체, 다만 1개 기관이 추천한 업체수는 원칙적으로 1개 업체에 한한다.

㈏ 조달청장이 적합하다고 인정하는 업체

⑵ 제⑴호의 업체는 대표자 및 비밀발간 종사원의 신원조사에 결격사유가 없고, 비밀발간 작업에 충분한 인원을 확보하여야 한다.

라. 인가절차

⑴ 비밀발간의 인가대상으로 인정되는 업체가 "나"항 및 "다"항의 기준을 확인할 수 있는 서류를 첨부하여 인가신청을 하여야 한다.

⑵ 비밀발간 인가대상 업체는 "다'항 제⑵호에 해당하는 자로서 보안의식이 강하고 가급적 보안관계 종사경험이 있는 자 중에서 다음의 비밀보호 책임대상자 명단을 인가 전에 제출하여야 한다.

㈎ 비밀보호 정책임자는 대표자로 한다.

㈏ 비밀보호 부책임자는 실제작업에 있어서 비밀보호 정책임자를 대리할 수 있는 자로 한다.

⑶ 비밀반간의 인가대상 업체에 대하여는 국가정보원장의 보안측정 결과 적격판정이 있어야 한다.

⑷ 비밀발간업체의 인가 전에 대표자 및 비밀발간 작업종사원에 대한 신원조사 결과 결격사유가 없어야 한다.

마. 인가증 교부 및 회수

⑴ 비밀발간업체로 인가할 때에는 인가증 발급대장(별지1)에 기록하고, 인가증(별지2)을 교부한다.

⑵ 비밀발간업에의 인가를 취소할 때에는 인가증을 회수한다.

바. 인가취소

다음 각 호의 1에 해당할 때에는 비밀발간업체의 인가를 취소한다.

⑴ "나"항 및 "다"항 기준에 미달하는 때

⑵ 중앙행정기관의 장이 비밀반간업체 추천을 취소 요청할 때

(3) 개인업체인 경우에는 양도에 의하여 대표자의 명의가 변경된 때

(4) 법인인 경우에는 법인등기부상의 임원이 아닌 자 또는 종사원으로 신고되지 아니한 자가 대표자로 취임한 때

(5) 영업장소를 신고없이 이전하여 보안측정을 받지 아니하고, 영업을 하는 때

(6) 비밀의 누설 또는 분실 등 중대한 보안사고가 발생한 때

(7) 영업장소이전, 대표자 변경, 비밀관련 물품 도난 등의 주요 신고의무를 이행하지 아니한 때

(8) 3년 동안에 2회 이상 경고처분을 받은 때

(9) 비밀문서 발간업체로서 부적당하다고 인정되는 다음의 경우

㈎ 보안관리상태 부실

㈏ 보안조치 불이행

㈐ 연간비밀발간 실적이 없거나 극히 저조한 때

사. 보안업무 지도 감독

(1) 조달청장은 비밀발간업체를 대상으로 연 1회 이상 보안지도 감독 및 교육을 실시하여야 하며, 필요한 경우 수시로 할 수 있다.

(2) 지도점검반은 담당과장을 반장으로 하여 3~5명으로 평성한다.

(3) 보안지도 감독결과 보안시설 또는 보안관리가 미비하거나 보안상의 요 시정 및 보안관계 준수사항을 이행하지 아니한 때에는 주의 또는 경고 조치한다.

(4) 제3호의 주의 3회는 경고 1회로 한다.

(5) 조달청장은 제1호의 결과를 국가정보원원장에게 통보하여야 한다.

아. 경과조치

이 지침 개정 전에 인가된 업체는 이 지침에 의하여 인가된 업체로 본다.

2. 정부비밀문서 발간에 대한 준수사항

조달청장의 지정에 의한 정부의 비밀문서발간업체로서 이행 준수할 사항과 정부기관의 의뢰에 따라 정부의 비밀문서를 발간 납품할 때의 비밀문서의 발간작업과 취급요령은 본 준수사항에 의한다.

가. 정부비밀문서 발간의 우선

정부기간(이하 "수요기관"이라 한다)으로부터 정부비밀문서(이하 "비밀문서"라 한다)의 발간(수요기관이 제시한 원고나 지시에 따라 인쇄에 의하여 비밀문서를 생산하는 것을 말하여 이하 같다) 의뢰가 있을 때는 타 수요기관의 비밀문서작업에 지장이 없는 한 거부함이 없이 즉응하여야 하며 일반문서에 우선하여 발간하여야 한다.

나. 수요기관의 관계공무원의 입회 및 동행

(1) 비밀문서 원고의 수교시의 동행

㈎ 수요기관의 관계공무원이 직적 비밀발간업체에 방문하여 수교한다.

㈏ 비밀발간업체의 직원이 수요기관에 방문하여 원고를 수령할 때는 수령으로부터 발간업체 작업장까지 수요기관의 관계공무원이 동해하여야 한다.

(2) 비밀문서 발간작업시의 입회

발간작업의 전 과정에는 수요기관 관계공무원의 입회하에 작업하여야 하며 관계공무원의 입회없이 작업함을 금한다.

(3) 비밀문서 납품시의 동행

발간된 비밀문서를 납품할 때는 작업장으로부터 수요기관의 납품장소까지 수요기관의 관계공무원이 동행하여야 한다.

다. 비밀문서 발간작업 종사원

(1) 작업종사원의 등록

발간작업 시에는 소정의 절차에 의하여 조달청에 비밀문서 발간작업 종사원임을 등록하고 조달청장으로부터 종사원 등록증을 교부받은 자만이 종사할 수 있으며 전기이외의 여하한 자도 비밀문서의 발간작업에 종사하거나 비밀문서를 취급하여서는 아니된다.

(2) 작업종사인원의 제한
비밀문서의 발간작업에 종사할 인원은 등록된 종사원 중 작업량에 따라 필요한 최소한의 인원으로 제한하여야 한다.

(3) 작업중 종사원등록증의 패용
발간작업종사원은 작업중 조달청장이 발행한 종사원등록증을 반드시 패용하고 작업에 종사하여야 한다.

라. 비밀문서 발간작업장 및 기타 시설

(1) 작업장의 설치
비밀문서 발간작업장은 일반작업장과 완전히 구분하여 설치하고 작업장 창문에는 외부로부터의 침입을 방지할 수 있는 경고한 철책 또는 철망을 시설하고 출입문에는 시건장치를 하여야 한다.

(2) 통제구역의 표시
비밀문서 작업장 출입문 외부에는 통제구역의 표시(별지 3)를 하고 비밀문서 발간작업종사원 이외의 인원의 출입 또는 접근을 금하여야 한다.

(3) 작업단계별 작업장의 설치
작업단계의 특수성으로 인하여 비밀문서발간작업장(통제구역)을 종합 설치할 수 없을 때는 가능한한 통합된 최소의 작업단계별로 전기 "(1)", "(2)"에 준하여 비밀문서발간 작업장과 일반문서 작업장을 자바라, 커텐 등으로 구분 설치하고 비밀문서의 발간작업을 하여야 한다.

(4) 비밀문서 보관함의 비치
작업장에는 작업착수로부터 납품시까지에 일시 작업이 중단될 경우 비밀문서와 관련된 원고, 원지 등과 기타 작성된 비밀문서를 보관할 수 있는 시건장치가 된 철제함상(캐비넷 등)을 비치하고 비상시 제1차 지출순위임을 표시하여야 한다.

(5) 폐기물처리 대책 강구
작업장에는 문서 세절기를 비치하여 비밀문서와 관련된 파지 등 작업중 발생한 폐기물을 세절 처리하여야 한다. 단, 문서세절기를 구비치 않은 경우에는 방첩함(별지 4)를 비치하고 소각장을 설치하여야 한다.

마. 작업종사원과 작업장 비밀문서의 발간작업

(1) 작업종사원과 작업장
비밀문서의 발간작업을 전기 다항의 작업종사원이 라항의 작업장에서 작업하여야 하며 그 이외의 인원이 종사하게 하거나 작업장에서 작업하여서는 아니된다

(2) 수요기관의 관계공무원의 입회
작업의 전 과정은 수요기관 관계공무원의 입회하에 행하여야 한다.

(3) 작업장의 출입제한
비밀문서 발간작업장에는 발간작업관계공무원과 종사원 이외의 여하한 인원도 출입하게 하거나 접근하게 하여서는 아니된다.

(4) 비밀의 전파 등 금지
작업에 종사한자는 작업 중 알게된 비밀을 타인에게 전파, 누설, 공개 또는 타처에 유출시켜서는 아니되며 이를 위반하였을 때는 국가보안법에 의하여 처벌됨을 명심하여야 한다.

(5) 폐기물의 파기
발간작업중 비밀문서와 관련하여 발생한 원지, 파지등 (라항 (5)호의 방첩함에 투입된 내용물 포함)은 당일 작업 종류후 수요기관의 관계공무원의 지시와 그의 입회하에 전기 라항(5)호의 폐기물 소각장에서 소각 용행 등 멸소 종료후 수요기관의 관계공무원의 지시와 그의 입회하에 전기 라항(5)호의 폐기물 소각장에서 소각 용해 등 멸소처리를 하고 입회한 수요기관의 관계공무원의 확인을 받은 파기증명서(별지 5)를 작성 비치하여야 한다.

(6) 발간부수의 제한
비밀문서의 발간부수는 수요기관에서 요구하는 부수에 한하고 납품에서 제외된 불안전품은 입회중인 수요기관의 관계공무원의 지시에 따라 처리하여 하며 최종납품 이후에는 업체내의 비밀문서나 그와 관련된 비밀사항이 기재(표시)된 여하한 형태의 물건이라도 보유하여서는 아니된다.

(7) 비밀문서의 보관
작업이 일시 중단되거나 작업착수 당일에 완료하지 못하고 2일 이상의 작업시일이 소요되는 등으로 비밀문서와 그에 관련된 문서 등을 업체내에 보관하여야 할 때는 수요기관 입회공무원의 지시를 받아 전기 라항 (4)호의 비밀문서 보관함에 보관하고 시건하여야 한다.

(8) 납품

발간된 비밀문서를 수요기관에 납품할 때는 반드시 수요기관의 관계공무원과 동행 반송하여야 한다.

(9) 숙직자의 배치

비밀문서를 업체내에 보관하고 있을 때는 주간의 물론 야간에도 비밀문서의 안전보관을 위하여 비밀작업종사원으로 등록된 자를 숙직자로 배치하여 비밀문서의 보관보호에 만전을 기하여야 한다.

바. 돌발사태 등에 대한 대책

(1) 비밀문서의 분실 등

발간작업중 또는 보관중인 비밀문서와 그에 관련된 비밀사항이 기재(표시)된 물건을 도난당하거나 분실되었을 때는 즉시 수요기관과 최기의 경찰관서에 신고하고 그 지시에 따라야 한다.

(2) 비밀문서의 대피

화재 또는 기타 돌발적인 긴급사태의 발생으로 비밀문서의 보호가 극히 위태로울 때는 작업중인 경우에는 입회중인 수요기관의 관계공무원의 지시에 따라 최우선적으로 비밀문서를 보호, 대피책을 강구하고 작업의 일시 중단으로 보관중인 때는 비밀문서를 최기의 경찰관서에 긴급 대피시키고 즉시 수요기관에 연락하여 그의 지시에 따라야 한다.

사. 비밀보호책임자의 임명

(1) 비밀보호 정책임자와 부책임자의 임명

작업중이거나 보관중인 비밀문서의 비밀보호를 철저히 하기 위하여 비밀보호 정책임자와 부책임자를 임명하여야하며, 비밀보호 정책임자는 회사대표자가 되고 부책임자는 조달청에 등록된 종사원 중에서 비밀문서 실제작업에 있어 비밀보호 정책임자를 대리할 수 있는 자를 임명하여야 한다.

(2) 비밀보호자의 임무

(가) 비밀보호책임자는 대표자를 대리하여 비밀보호에 관한 책임을 진다.

(나) 비밀보호책임자는 비밀문서작업 또는 보관중에는 작업자 등 관계자를 사전에 지정하고 관계자 이외의 인원의 통제구역내 출입을 통제하여 실제 작업에 있어서 비밀보호에 필요한 제반조치를 지시 및 확인토록 한다.

㈐ 통제구역출입문과 비밀문서보관함의 자물쇠 암호와 열쇠를 보관 관리한다.

㈑ 자물쇠 암호와 열쇠는 비상시에 대비하여 밀봉한 후 비밀문서 보관 책임있는 숙직자에게 보관케하고 익일 이를 회수한다.

아. 영업장소의 이전과 대표자의 변경

(1) 이전 등의 신고

영업장소 이전, 대표자 변경, 비밀작업장 개조 등 보안여건을 변동하여야 할 시는 사전에 즉시 조달청장에게 신고하고 1개월 이내에 보안측정을 요청하여야 한다.

(2) 이전 등 이후의 비밀문서 발간 금지

영업장소 이전, 대표자 변경, 비밀작업장 개조 등 보안여건 변동후에는 보안측정을 받지 아니하고는 여하한 경우에도 비밀문서를 발간할 수 없다.

자. 광고선전 등의 금지

정부비밀문서발간업체는 대외적인 광고선전 등에 정부비밀문서발간업체임을 표시하여서는 아니되며 업체의 내외부에 정부비밀문서발간업체임을 인지할 수 있는 여하한 형태의 표시나 표기를 하여서는 아니된다.

차. 기록의 유지 및 보고사항 등

비밀문서발간업체는 다음과 같은 부책을 기록유지 비치하여야 하며 지정된 사항을 지체없이 조달청에 보고하여야 한다.

(1) 서약서

㈎ 정부비밀문서 발간업체로 지정되면 대표자를 포함한 조달청에 등록된 비밀문서 발간작업 종사원 전원의 서약서(별지 6) 2통을 징구하여 1통은 업체에 비치하고, 1통은 조달청에 제출하여야 한다.

㈏ 신규로 비밀문서 종사원으로 조달청에 등록을 필하였을 때도 전항과 같이 서약서를 징구하고 업체에 비치하는 한편 조달청에 제출하여야 한다.

(2) 종업원 명부

㈎ 대표자를 포함한 조달청에 등록된 정부비밀문서 발간작업 종사원명부(별지 7)를 2통 작성, 1통은 조달청에 제출하고 1통은 업체에 비치할 것이며 종사원이 이동이 있을

때마다 해당 종사원에 대한 명부상의 기재사항을 조달청에 보고하고 비치한 명부를 기록 유지하여야 한다.

㈏ 비밀보호 정책임자와 부책임자는 비고란에 그 뜻을 주서 하여야 한다.

(3) 종사원의 등록증

㈎ 업체의 종사원중 비밀문서 작업에 종사할 인원에 대하여는 조달청에 소정의 절차에 따라 등록을 필하고 별지8과 같은 종사원등록증을 발급받아야 한다.

㈏ 종사원 등록증은 비밀문서발간작업중 항시 패용하여야 한다.

㈐ 비밀문서 발간작업이 끝나면 대표자는 종사원 등록증을 회수하여 업체내에 보관 관리하여야 한다.

㈑ 등록된 종사원이 퇴직하거나 비밀문서발간작업 종사에서 이동되었을 때는 즉시 종사원 등록증을 조달청에 반환하여야 한다.

(4) 작업일지

수요기관으로부터 원고 수령후 납품까지의 매일의 작업상황을 별지9의 작업일지에 의하여 기록하고 수요기관 입회관의 확인을 받아 비치하여야 한다.

(4)-1 교육일지

비밀보호책임자는 비밀발간 종사원으로 등록된 자 전원을 대상으로 비밀문서발간 준수사항 등에 대하여 월 1회 이상 교육을 실시하고 교육일지를 비치 교육내용을 기록 유지하여야 한다.

(5) 비밀파기증명서

전기한 "다항(5호)"에 의하여 원지, 원판, 지형 기타 작업중 발생한 비밀사항과 관련된 폐기물을 파기 조치하였을 때 매일 작성한 비밀파기증명서(별지 5)는 일련번호 순위에 따라 이를 합철 비치하여야 한다.

(6) 숙직일지

작업기일이 2일 이상 소요되며 비밀문서를 작업장내에 보관하였을 때는 숙직을 실시하고 별지10의 숙직일지를 작성하고 수요기관 입회관의 검열을 받아 비치하여야 한다.

(7) 비밀문건 발간실적 보고

비밀문서발간업체는 매 분기별 비밀문건(문서 및 도면 등) 발간실적을 별지 11호 서식에 의거 작성하여 익월 15일까지 조달청에 제출하여야 한다.

카. 전산장비이용 비밀문서 발간작업

(1) 비밀문서를 발간할 때 이용하는 워드프로세서 등 전산장비(이하 "비밀발간전산장비"라 한다)는 자료를 무단 열람 또는 출력하지 못하도록 비밀번호(PASSWORD)를 사용하여야 한다.

(2) 비밀발간전산장비는 인터넷에 연결하여 사용할 수 없다.

(3) 비밀발간전산장비를 이용한 비밀문서 등 중요내용 발간작업은 프로피디스켈 등 보조기억장치를 이용하여 작업함을 원칙으로 한다. 다만, 부득이한 사정으로 전산장비 본체에서 작업한 경우에는 당일 작업종료시 작업한 내용을 본체에서 삭제하여야 한다.

(4) 비밀발간전산장비를 이용하여 비밀문서 등 중요내용의 발간작업을 한 경우에는 매일 작업일지를 작성·유지하여 비밀보호 정·부책임자가 (1), (2), (3)항의 내용을 확인하여야 한다.

타. 기타

(1) 이 지침은 2003년 10월 10일부터 시행한다.

(2) 이 지침에 명시되지 않은 사항으로서 비밀문서의 발간작업 또는 취급상의 의문이 있을 때는 당해 비밀문서의 발간을 의뢰한 수요기관 또는 조달청에 문의하여 그 지시에 따라야 한다.

(3) 인가취소 사유의 경고 및 주의를 받은 회수의 누계는 2003년도부터 계산한다.

[별지 1]

정부비밀문서 발간업체 인가증 발급대장

인가증 번 호	인 가 년월일	상 호	대표자	주 소	신규 및 발 급	계 인	비 고

[별지 2]

인 가 증

제 호 :

상 호 : (구분 :)

대표자성명 : (년 월 일생)

주 소 :

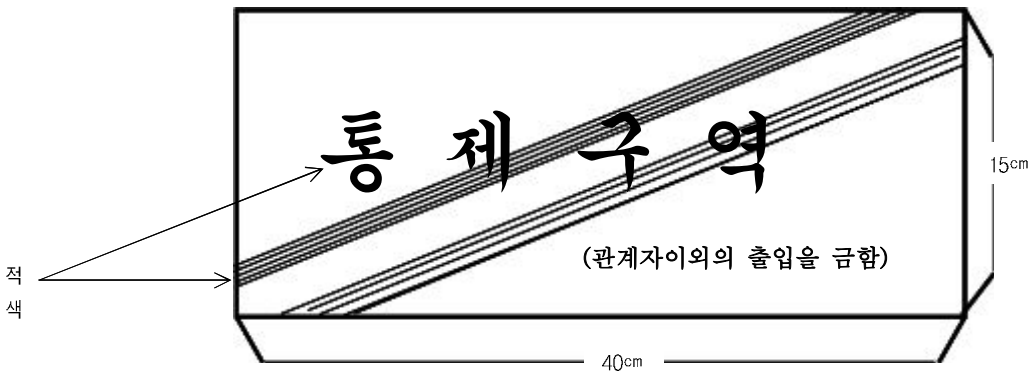
상기자를 정부비밀문서 발간업체로 인가함

200 년 월 일

조 달 청 장

[별지 3]

통 제 구 역 표 시

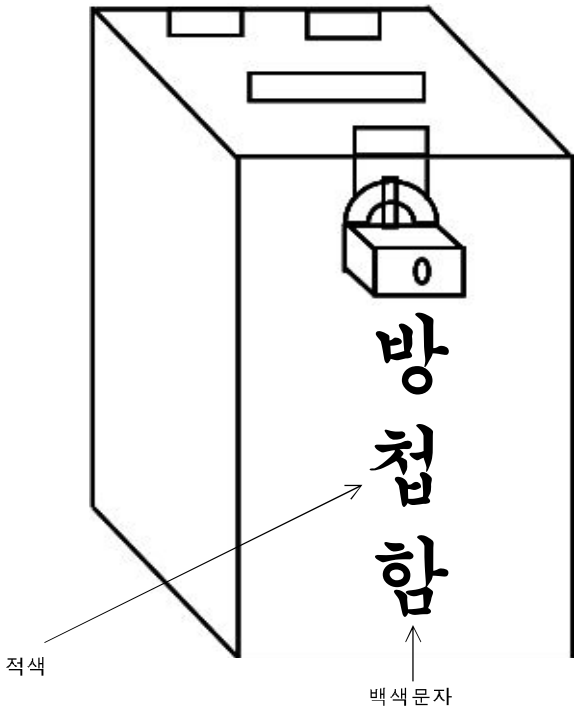


[별지 4]

방 첩 함 사 양

1. 높이 70cm
   가로 50cm
   세로 40cm

2. 재료는 1.2cm
   이상의 판자
   또는 2mm이상의
   철판으로 할 것



[별지 5]

비 밀 파 기 증 명 서

일련번호

수요기관의 비밀관리 번호	제목, 가제목 또는 품명	발행 또는 각성일자	비밀 등급	수 량	발기처	사본 번호	파기 번호	비 고

본인은 상기비밀(수요기관) 입회관의 지시에 의하여 파기하였음 200 년 월 일 상 호 : 파기자 : (대표자 또는 비밀책임자) 성 명 : ㊞	본인은 상기 비밀파기를 지시하고 파기에 입회 확인하였음 200 년 월 일 수요기관명 : 직 명 : 성 명 : ㊞

[별지 6]

서 약 서

본인은 200 년 월 일부터 으로 비밀을 취급함에 있어 다음 사항을 준수할 것을 엄숙히 서약한다.

1. 본인은 본인이 취급하던 비밀은 물론 기타 지득한 일체의 비밀이 국가안전보장에 관계되는 중대한 사항임을 명심한다.

2. 본인은 이 비밀을 누설함이 국가안전보장상 유해로운 결과를 초래한다는 것을 자각하고 제 보안 규정을 시간과 장소에 제한 없이 성실히 이행하며 재직중은 물론 퇴직후에도 누설하지 아니할 것이면 만일 누설하였을 때에는 동기여하를 막론하고 그 결과가 이적 또는 반국가적 행위임을 자인하고 하기 제법규에 의하여 엄중한 처벌을 감수할 것을 서약한다.

가. 국가안보법 제3조제1항 및 제4조(일반목적 수행)
나. 국가안보법 제7조(고무, 찬양등)
다. 형법 제99조(일반 이적)
라. 형법 제127조(공무상 비밀누설)
마. 형법 제14조(일반 이적)
바. 군형법 제47조(명령위반)
사. 군형법 제80조(군사기밀 누설)

좌수무인		200 년 월 일		우수무인
서약자	직책	직위	성명	㊞
서약자	직책	직위	성명	㊞

[별지 7]

종 사 원 명 부

일련번호	부서	성명	성별	생년월일	직책	본적	주소	입 직 년월일	퇴 직 년월일	비고

1. 부서 본인의 소속부서(예 : 인쇄부, 조판부 등)
2. 직책, 본인의 직무상의 직위(조판부장, 인쇄공등)
3. 본적, 주소는 (서울 종로 인의 123동으로 번지까지 기재함)
4. 종업원 이동(입직, 퇴직)이 있을 때마다 해당인의 명부만을 본 양식에 의하여 제출할 것
5. 비고란에는 민간인 신원진술서, 서약서 제출연월일을 기입

[별지 8]

(앞 면)

종 사 원 등 록 증

사 진

No.

성 명 :

주민등록번호 :

생 년 월 일 :

본 적 :

주 소 :

직 책 :

상기자는 정부간행물 종사원의 등록을 필하였음을 증명함

20 년 월 일

조 달 청 장

(뒷 면)

이 동 사 항		
년 월 일	근 무 처	검 인

[별지 9]

작 업 일 지

(전 면)

200 년 월 일 요일				대표자인			입회관 확인인		
수요부처	비밀문서의 제목 또는 가제목	비밀등급	발간요구부수	원고접수일자	납품요구일자	최초작업착수일자	인가등급	입회관 직명	입회관 성명

작 업 상 항

작업구분	작업인원수	작업시간 (부터~ 까지)	작업량	기타

기타사항(입회관, 지시사항)

(후 면)

작 업 종 사 자		계 명	
작업부서	성 명	작업부서	성 명

[별지 10]

숙 직 일 지

200 년 월 일	대표자인		입회관 사후검열인	
보관중인 비밀문서				
수요기관	제목 또는 가제목	비밀등급	수량	접수 또는 작성일시	보관장소	비 고
숙 직 사 항				
보관상태의 이상유무	확인시간	가	사	
기타사항				
숙 직 자	부서	직책		성명		인

[별지 11]

비 밀 발 간 실 적

(단위 : 천원)

구분	Ⅰ급		Ⅱ급		대외비		계	
	건 수	금 액	건 수	금 액	건 수	금 액	건 수	금 액
1/4분기								
2/4분기								
3/4분기								
4/4분기								
계								

[별지 12]

PC 비밀번호관리기록부

년 월 일	제품번호 (PC)	컴퓨터 관리자	비밀번호		결재		
			변경전	변경후	담당	부책임자	정책임자

※ 비밀번호는 영문포함 8자리 이상으로 설정

[별지 13]

비밀문서 PC작업일지

년월일	제품번호 (PC)	의뢰내용		작업자	작업 일시	삭제 일시	결재		
		기관명	의뢰자				담당	부책임자	정책임자

※ 작업일시는 시작부터 종료시까지 기록

② 특수자료취급지침

제정 70. 2. 16(중대보 020)
개정 77. 12. 30(중오보 020)
84. 6. 30(대 보 020)
88. 9. 1(대 보 020)
98. 9. 1(외보 97200)
2003. 7. 3(보안 97200)

제1조(목적) 이 지침은 정보 및 보안업무 기획조정규정(대통령령 제16211호) 제4조제6호 및 제5조에 의거 특수자료 취급 및 관리에 관한 사항을 규정함을 목적으로 한다.

제2조(용어의 정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.
①"특수자료"라 함은 간행물, 녹음테이프, 영상물, 전자출판물 등 일체의 대중전달 매개체로서 관련기관에서 비밀로 분류한 것을 제외한 다음 각호에 해당하는 자료를 말한다.
1. 북한 또는 반국가단체에서 제작, 발행한 정치적·이념적 자료
2. 북한 및 반국가단체와 그 구성원의 활동을 찬양, 선전하는 내용
3. 공산주의 이념이나 체제를 찬양, 선전하는 내용
4. 대한민국의 정통성을 부인하거나 자유민주주의 체제를 부정하는 내용 등
②"특수자료 취급기관"(이하 "취급기관"이라 한다)이라 함은 이 지침에 의거 특수자료의 취급인가를 받은 기관, 단체 및 업체를 말한다.

제3조(특수자료의 분류)
①특수자료 취급기관의 장은 수집한 자료 등에 대해 제2조 제1항에 정하는 기준에 의거 분류하여야 한다.
②특수자료 여부에 대한 판단이 어려울 때에는 감독부처를 경유하여 통일부에 문의하고 통일부에서는 필요시 국가정보원장(이하 "국정원장이라 한다)과 협의할 수 있다.

제4조(취급기관 인가 및 해제)
①특수자료를 취급하고자 하는 기관의 장은 별지 제1호 시석에 의거 해당 감독부처의 장에게 취급기관 인가를 신청하여야 한다.
②해당 감독부처의 장은 타당성과 보안요건을 판단하여 인가하되 미리 인가신청서 등 관련자료를 첨부하여 국정원장과 협의하여야 한다.

③국정원장은 관련자료를 검토하여 의견을 회신하되 필요한 경우 보안측정을 실시할 수 있다.
④취급기관의 장은 취급기관 인가를 해제하고자 할 때에는 사유, 보유자료 처리대책을 해당 감독부처의 장에게 보고하여야 한다.
⑤해당 감독부처의 장은 보유자료 처리를 확인한 후 인가를 해제하고 그 결과를 국정원장에게 통보하여야 한다.

제5조(특수자료의 관리)
①취급기관의 장은 특수자료 관리 및 취급을 위해 자체 내규를 수립·시행하는 등 전반적인 보안책임을 진다.
②취급기관의 장은 자료를 전담 관리할 정·부 책임자를 임명하여 다음 각 호의 임무를 수행하게 하여야 한다.
1. 특수자료의 보관관리 및 확인점검
2. 각종대장 기록유지 및 특수자료 관리에 필요한 사항
③취급기관장은 자료관리 정·부 책임자에 대해 신원조사를 실시하고, 보안서약서(별지 제2호 서식) 징구 및 교육 등 보안조치를 하여야 한다. 다만, 현직 공무원이거나 공공기관, 교육기관 종사자 등의 경우에는 임용시 신원조사로 대체 할 수 있다.
④특수자료는 등록대장(별지 제3호 서식)에 기록하고 관리번호(별지 제4호 서식)를 부여하여야 하며 경고문(별지 제5호 서식)을 여백에 표시하여야 한다.
⑤특수자료는 제한구역으로 설정한 보관실에 보관하여야 한다. 다만, 공간협소 등 부득이 한 경우에 한하여 별도 보관함에 보관할 수 있으며 이 경우 자료의 분실·유출 등 방지를 위한 보안대책을 철저히 강구하여야 한다.

제6조(자료의 열람·대출·양도)
①취급기관의 장은 특수자료 열람신청이 있을 때에는 신청자의 신분 및 열람목적을 확인한 후 지정된 장소에서 열람을 허가한다.
②취급기관의 장은 자료 대출 신청이 있을 때에는 신청자의 신분·목적을 확인하고 타당성이 인정된 자에 한하여 30일 이내에서 대출을 허가할 수 있다. 이 경우 취급기관의 장은 무단 복제·복사·유통 방지를 위해 서약서(별지 제6호 서식) 징구 등 보안대책을 강구하여야 한다.
③특수자료를 열람 또는 대출할 때에는 별지 제7호 서식에 의한 열람·대출대장에 기록하여야 한다.
④취급기관의 장이 특수자료를 복사 또는 취급기관에 양도할 때에는 복사·양도대장(별지 제8호 서식)에 기록하여야 한다.

제7조(특수자료의 공개활용)

①취급기관의 장은 국민의 안보의식 계도 및 학술연구 등 필요한 경우 해당 감독부처장의 승인을 받아 특수자료를 공개할 수 있다. 이 경우에는 공개할 자료의 내용, 활용목적, 공개시기 및 방법 등을 기재한 특수자료 공개활용 계획서를 제출하여야 한다.

②해당 감독부처의 장은 의견을 첨부하여 국정원장과 미리 협의하여야 한다.

③취급기관이 보유한 특수자료의 목록은 전항의 절차 없이 공개할 수 있다.

제8조(보고 및 통보)

①취급기관의 장은 특수자료 취급현황(별지 제9호 서식)을 연 1회 작성, 해당 감독부처의 장에게 보고하여야 한다.

②취급기관의 장은 특수자료의 분실, 유출 등 각종 보안사고와 특수자료실 이전시는 지체없이 해당 감독부처의 장에게 보고하여야 한다.

③해당 감독부처의 장은 제1항 및 제2항에 정한 사항을 국정원장에게 통보하여야 한다.

제9조(지도방문)

①해당 감독부터의 장은 연1회 이상 산하 취급기관에 대한 지도방문을 실시, 자료관리 및 활용실태를 점검한 후 국정원장에게 그 결과를 통보하여야 한다.

②국정원장은 필요시 감독부처와 합동으로 취급기관에 대한 지도방문을 실시할 수 있다.

제10조(행정제재) 해당 감독부처의 장은 산하 취급기관 및 관리 책임자가 이 지침에 정한 사항을 위반한 때에는 경고, 시정명령, 인가취소 등 행정제재 조치를 할 수 있다.

제11조(비상시 자료보호) 취급기관의 장은 천재지변, 화재 등 비상시 안전지출 또는 긴급파기계획 등 자료보호대책을 자체관리내규에 포함시켜야 한다.

부 칙

1. 이 지침은 2003년 7월 3일부터 시행한다.
2. 이 지침 시행전 특수자료 취급 인가자는 지침 제5조 제3항에서 정한 신원조사 대상으로부터 제외한다.
3. 1998년 9월 1일 시행한 특수자료 취급지침은 이 지침 시행과 동시에 폐지한다.

[별지 제1호 서식]

특수자료 취급기관 인가신청서

기관명		기관장	성 명	
			생년월일	
소재지			전화번호	
관 리 책임자	정	성명 : (. . 생) 소속 :		
	부	성명 : (. . 생) 소속 :		
특수자료 취급목적 및 필 요 성	※ 자료 확보방안 포함			
자료실 현황	※ 평(㎡)			
기 관 조직 및 인원				
시 설 현 황	※ 대지(평·㎡) 및 건물(층고·동수·연면적) 등 시설현황			

※ 자체 특수자료 취급관리 내규 (첨부)

[별지 제2호 서식]

서 약 서

수 신 :

1. 본인은 소속기관의 특수자료 관리책임자로서 자료취급에 관한 제반규정을 성실히 이행하여 자료 보호·관리에 만전을 기할 것이며

2. 만일 본인의 고의 또는 과실로 인하여 관련법규 및 제반규정에 위배되는 사례가 발생한 경우에는 어떠한 처벌도 감수할 것을 서약합니다.

20 . . .

소 속 :

연 락 처 :

주민등록번호 :

주 소 :

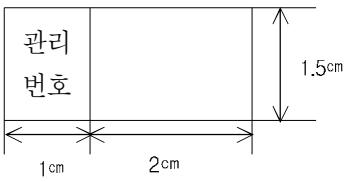
성 명 : ㊞

[별지 제3호 서식]

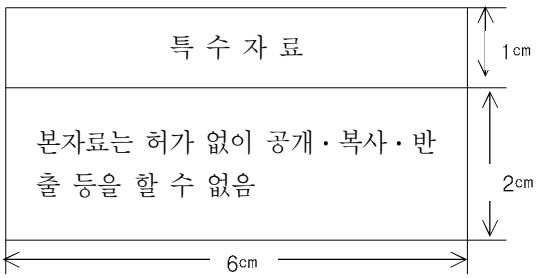
특수자료 등록대장

관리 번호	입수 일자	자 료 명	발행자	발 행 연월일	입수 경위	비고

[별지 제4호 서식]



[별지 제5호 서식]



[별지 제6호 서식]

서 약 서

수 신 :

1. 본인은 대출한 특수자료를 신청목적에 부합되게 활용할 것이며

2. 본인의 고의 또는 과실에 의해 대출자료가 무단 복제·복사·유통되어 국익에 위배되었을 때에는 동 행위가 관계법규에 위반된다는 것을 명심하고 특수자료 취급에 관한 제반규정을 성실히 준수할 것을 서약합니다.

20 . . .

소 속 :

연 락 처 :

주민등록번호 :

주 소 :

성 명 : ㊞

[별지 제7호 서식]

특수자료 열람·대출대장

일자	관리번호	자 료 명	목 적	열람·대출자				반 납		
				소속	연락처	주민번호	성명	일자	책임자	서명

[별지 제8호 서식]

특수자료 복사·양도대장

일자	관리번호	자료명	목적	인계(복사)자	인수자	비고

[별지 제9호 서식]

【취급기관 일반현황】

연번	기관명	주소	전화 번호	기관장 (직책)	정책임자 (직책)	부책임자 (직책)	인가 일자	홈페이지	비고

【특수자료 보유현황】

구 분	전년도 보유건수	증가 건수	계
총 계			
정기간행물			
단 행 본			
시청각자료			
기 타			

* 일간지, 주간지는 월별로 합철 1건으로 계상

【특수자료 활용실적】

구 분	열 람	대 출	복사(양도)
계	명 회	명 회	개 기관 건
정기간행물	명 회	명 회	개 기관 건
단 행 본	명 회	명 회	개 기관 건
시청각자료	명 회	명 회	개 기관 건
기 타	명 회	명 회	개 기관 건

❸ 국가기밀자료 國會 지원지침

국무조정실 총괄 06000-346(2004. 11. 24.)

□ 국회의장 또는 위원장 명의 요구원칙 준수 유도

○ 국회의 자료제출 요구는 국회법 제128조에 따라 국회의장 또는 위원장 명의로 요청하도록 협조 요청

○ 국회의원들이 단독명의 또는 개별적으로 안건심의 및 국정감사·조사 관련서류 제출을 요구할 경우 정식 절차에 의거 요청토록 유도

□ 국회 제공자료 사전 보안성 검토 철저 및 제출창구 일원화

○ 비밀 또는 대외보안이 요구되는 자료를 국회에 제공할 경우 자체 보안심사위원회(위원장 차관급)를 개최하여 지원자료의 범위, 비밀분류의 적절성, 경고문 삽입 및 자료회수 방안 등 사전 검토 철저 단, 부득이한 경우 기획관리실장 통제하에 자료제공 가능

○ 국회 자료제공 창구를 기획관리실로 일원화하여 각 부서의 임의·개별적인 자료지원 차단

□ 비밀자료 제공·설명시 주의의무 고지 등 보안조치 강화

○ 국회에 대한 비밀자료 서면 제공은 가급적 지양하고, 담당공무원이 의원에게 직접 구두 설명하되 비밀문건 열람 필요시 현장에서 열람후 회수 의무화
다만, 단순한 상황이나 경미한 사항은 해당 비밀 취급이 인가된 사무보조자(의원보좌관 등)에게 구두 설명 가능

○ 국회의원에게 비밀내용 설명시 동석한 사무보조자(의원보좌관 등)에 대해서는 해당등급의 비밀취급인가 여부를 반드시 확인하고, 설명·열람 내용을 메모·녹음 등의 방법으로 가록 유지를 못하도록 조치

○ 비밀자료를 지원 또는 설명시 해당자료의 비밀등급과 외부에 누설하여서는 안된다는 사실을 사전 고지하고, 이를 위반할 경우에는 형법 제127조(공무상비밀누설죄), 군사기밀보호법 및 국회법 등 관계법규에 의해 처벌될 수 있음을 사전 경고

○ 국회에 비밀자료를 제출한 경우에는 비밀관리 기록 유지·보관 철저·복사금지 등 비밀보호를 위한 보안규정을 철저 준소토록 하고, 보안이 취약한 장소로 반출하지 않도록 고지

※ 보안업무규정(대통령령) 및 國會보안업무규정(국회 규칙) 참조

□ 국가안위에 중대한 영향을 미치는 기밀자료 제출 거부

○ 군사·외교·대북관계에 관한 국가기밀 사항으로서 그 발표로 말미암아 국가 안위에 중대한 영향을 미치는 사항에 대해서는 기관장이 이를 소명하고 서류제출을 거부하는 등 보안관리 철저

※「국회에서의 증언·감정 등에 관한 법률」 제4조 제1항 참조

○ 자료제출 거부 여부는 자체 보안심사위원회에서 심의·결정

□ 의원의 기밀내용 질의시 비공개 회의 및 비공개·비보도 요청

○ 국회 본회의·상임위 등에서 국가기밀사항을 공개 질의할 경우 즉시 질의내용이 국가안보와 관련된 사안임을 고지하고 발언을 중단시킨후 비공개 회의를 요청하여 국가기밀 사항이 외부에 공개되는 일이 없도록 조치

○ 국회의원이 이미 질의한 기밀내용은 회의록 배부·반포시 게재금지 요청 및 언론사에 비보도 요청

※「국회법」 제117조, 제118조 제1항 참조

□ 국가기밀 언론 공개시 법적 대응조치 강구

○ 국회의원 또는 사무보조자(의원보좌관 등)가 비밀을 공개할 경우 형법, 군기법 및 국회법 등 관계법률에 따라 엄중 대처

※ 의원은 국회법 및 국정감사·조사법에 따라 윤리위원회 의결로 징계 가능

○ 국가기밀을 공개한 의원은 물론 全 언론사에 대해서도 지체없이 非보도를 요청하고, 국회의장에게 관련자 징계조치 등 재발방지 대책 촉구

○ 관계 공무원에 대해서는 「보안업무규정」에 따라 비밀자료 유출경위 등을 철저히 조사하여 엄중 문책

❹ 비밀기록물 관리지침

국가기록원의 【2009년도 기록물관리지침】 발췌

1 관련근거

○ 공공기록물 관리에 관한 법률·시행령 제7장 비밀기록물의 관리

○ 보안업무규정·보안업무규정 시행규칙

2 비밀기록물 관리대상

○ "비밀"이라 함은 그 내용이 누설되는 경우 국가안전보장에 유해로운 결과를 초래할 우려가 있는 국가 기밀로서 비밀로 분류된 것을 말함(「보안업무규정」 제2조)

○ 비밀기록물은 공공기록물 관리에 관한 법률에 의해 관리하여야 하는 "기록물" 중 비밀로 분류된 것을 말함

- Ⅰ급비밀 : 누설되는 경우 대한민국과 외교관계가 단절되고 전쟁을 유발하며, 국가의 방위계획·정보활동 및 국가방위상 필요 불가결한 과학과 기술의 개발을 위태롭게 하는 등의 우려가 있는 비밀
- Ⅱ급비밀 : 누설되는 경우 국가안전보장에 막대한 지장을 초래할 우려가 있는 비밀
- Ⅲ급비밀 : 누설되는 경우 국가안전보장에 손해를 끼칠 우려가 있는 비밀(「보안업무규정」 제4조)

○ 비밀기록물 관리의 적용대상은 비밀기록물 원본에 한함

※ 비밀을 책자형태로 간행하였을 경우에는 이를 간행물이 아닌 비밀기록물로 취급하며, 비밀 관리절차에 따라 관리

3 비밀기록물의 관리원칙

○ 비밀기록물 관리체계 구축

- 기록물관리기관의 장은 비밀기록물 관리에 필요한 별도의 전용 서고 및 시설·장비 등을 설치·운영

○ 비밀기록물 전담관리요원 지정

■ 비밀취급인가를 받은 비밀기록물 전담관리요원을 지정

■ 이 경우 비밀취급 인가권자는 비밀의 누설 또는 유출 방지를 위하여 비밀기록물관리 전담요원에 대한 신원조사, 보안교육 등 필요한 보안조치를 국가정보원장에게 요청

○ 보안대책 수립·시행

■ 기록물관리기관의 장은 비밀기록물 및 비밀기록물 관리에 관한 정보를 취급하는 과정에서 비밀이 누설되지 않도록 국가정보원장이 정하는 보안대책을 수립·시행하여야 하며, 국가정보원장은 이를 확인

■ 비밀기록물 관리업무를 담당하였거나 비밀기록물에 접근·열람하였던 자는 그 과정에서 알게 된 비밀을 누설하여서는 안 됨

4 비밀기록물의 생산

○ 공공기관은 비밀기록물을 생산하는 때에는 당해 기록물의 원본에 비밀보호기간 및 보존기간을 함께 책정하여 보존기간이 만료될 때까지 관리

○ 비밀기록물의 비밀보호기간 부여

■ 분류된 비밀에는 보호기간을 명시하기 위하여 예고문을 기재(「보안업무규정」 제12조)

■ ① 모든 비밀에는 "~로 재분류(일자 또는 경우)"와 같이 예고문을 기재 ② 예고문의 재분류 일자 또는 경우는 도래가 명확한 것이어야 하며, "처리 후", "필요시" 또는 "참고 후"와 같이 불확실한 것을 기재하여서는 안 됨(「보안업무규정시행규칙」 제9조)

○ 비밀기록물 원본의 보존기간 부여

■ 비밀기록물 원본의 보존기간은 기록물철 또는 건단위로 책정하며, 기록관리기준표의 해당 단위과제에 책정된 보존기간을 적용

※ 비밀관련 기록관리기준표 관리 : 기록물관리기관의 장은 기록관리기준표의 단위과제에 비밀관련 내용에 포함되어 있는 경우에는 그 내용이 노출되지 않도록 비밀로 지정하여 별도 관리

■ 비밀기록물의 보존기간은 비밀보호기간 이상의 기간으로 책정하여야 하며, 비밀기록물의 보호기간이 변경된 경우에는 변경된 보호기간 이상으로 보존기간을 재책정

▣ 보호기간 및 보존기간 표시방법 예시 ▣

원 본	보호기간, ~로 재분류(일자 또는 경우)	보존기간 :
사 본	~로 재분류(일자 또는 경우)	

5 비밀기록물의 생산현황 통보

○ 비밀기록물 생산·해제 및 재분류현황 통보

- 공공기관의 장은 매년 3월 31일까지 관할 기록관 또는 특수기록관의 장에게 통보
- 기록관 또는 특수기록관의 장은 매년 5월 31일까지 관할 영구기록물관리기관의 장에게 통보
- 전년도 비밀기록물 원본의 생산·해제 및 재분류 현황을 통보

※ 대외비를 제외한 Ⅰ급, Ⅱ급, Ⅲ급 비밀의 등급별·보존기간별·보호기간별 생산·해제 및 재분류 현황을 통보

○ 비밀기록물 생산목록 통보

- 공공기관이 장은 비밀기록 생산현황에 포함된 비밀기록물 원본의 목록을 작성·관리하여야 함
- 비밀기록물 원본의 목록은 생산 후 3년이 경과한 다음연도 3월 31일까지 관할 기록관 또는 특수기록관의 장에게 통보
  - 비밀기록물 원본 목록의 제목 중 비밀정보가 포함되어 있는 경우에는 해당 정보를 삭제하고 제출 가능
- 기록관 또는 특수기록관의 장은 비밀기록물 원본의 목록 중 보존기간 30년 이상의 기록물에 대해서는 매년 5월 31일까지 영구기록물관리기관의 장에게 통보
- 중앙기록물관리기관의 장은 지방기록물관리기관의 장에게 국가위임사무와 관련된 비밀기록물로서 보존기간이 30년 이상인 비밀기록물의 생산·해제 및 재분류 현황을 요청할 수 있음

○ 영구기록물관리기관의 비밀 생산현황 정보 관리

- 영구기록물관리기관의 장은 통보받은 생산·해제 및 재분류현황에 관한 정보 중 비밀기록물의 목록은 별도의 비밀기록물 전용 전산장비에 저장·관리하여야 하며, 이 경우 해당 기록물 보호기간이 종료될 때까지 해당 목록을 비밀로 관리

6 비밀기록물의 이관

○ 처리과에서 기록관 또는 특수기록관으로 이관

■ 공공기관이 생산한 비밀기록물 원본은 다음 사유 발생시 기록관 또는 특수기록관으로 이관
① 일반문서로 재분류한 경우
② 예고문에 의하여 비밀보호기간에 만료된 경우
③ 생산 후 30년이 경과한 경우

○ 기록관 또는 특수기록관에서 영구기록물관리기관으로 이관

■ 기록관 또는 특수기록관의 장은 처리과에서 인수한 기록물 중 보존기간이 30년 이상인 비밀기록물은 인수한 다음 연도 중에 관할 영구기록물관리기관으로 이관
※ 단, 2007년 4월 5일 이전에 생산된 비밀기록물 중 보존기간이 20년으로 책정된 경우에는 보존기간 30년으로 관리하여 이관대상에 포함됨

■ 다만, 인수한 기록물이 보존기간의 기산일로부터 10년이 지나지 아니한 경우에는 남은 기간을 기록관 또는 특수기록관에서 보존 후 이관

○ 비밀기록물 이관방법

■ 전자비밀기록물은 국가정보원장이 정하는 바에 따라 보안을 유지할 수 있는 전송망을 통하여 이관하거나, 매체에 수록하여 봉인된 봉투에 담아 이관

■ 비전자적인 형태로 생산된 비밀기록물은 봉인된 봉투에 건 또는 권별로 담아 이관

■ 일반문서로 재분류된 기록물의 이관은 일반문서의 이관절차를 따름

◈ 비밀기록물 이관 및 인수인계시 주의사항 ◈

○ 비밀기록물의 각 건별 쪽수를 정확히 표시하여 이관

■ 각 문건별 중앙 하단에 당해 문건의 전체 쪽수와 각 쪽이 일련번호를 붙임표(-)로 이어 표시(예시 : 3-1, 3-2, 3-3)

■ 쪽수는 위로부터 아래의 순으로 부여하며, 양면에 내용이 있는 경우는 양면 모두 순서대로 쪽수 부여

◈ 비밀관리기록부 정리 ◈

○ 이관 사유가 발생하여 비밀기록물을 이관할 때에는 비밀관리기록부의 수령자 란에 "공공기록물 관리에 관한 법률에 의거 기록관 또는 특수기록관으로 이관" 기입

7 해제된 비밀기록물의 정리

○ 비밀해제 기록물의 편철

■ 비밀기록물이 일반문서로 재분류된 경우에는 기록관리기준표의 해당 단위과제에서 생산된 기록물철에 편철하여 관리

■ 다만, 관련된 기록물철이 없거나 개별 기록물 단위로 별도 관리가 필요한 경우에는 그 기록물을 기록물철로 보아 관리할 수 있음

○ 비밀해제 기록물의 공개여부 구분

■ 비밀기록물이 일반문서로 재분류된 경우에는 「공공기관의 정보공개에 관한 법률」 제9조 1항 및 「공공기록물 관리에 관한 법률」 제35조에 따라 해당 기록물의 공개여부를 구분하여 관리하여야 함

8 영구기록물관리기관의 비밀기록물 재분류

○ 영구기록물관리기관의 장은 그 기관에 관리하는 비밀기록물중 아래 조건에 해당하는 경우에는 재분류할 수 있음

① 보존기간의 기산일로부터 30년이 경과한 비밀기록물(예고문의 비밀보호기간이 남아있는 경우에는 생산기관의 동의를 얻어야 함)

② 당해 기록물의 생산기관이 폐지되고 그 기능을 승계한 기관이 분명하지 않은 비밀기록물의 비밀 보호기간이 종료된 경우

Ⅳ 정보보안 관련 규정

1 국가사이버안전관리규정

제정 2005. 1. 31 대통령훈령 제 141 호

제1조(목적) 이 훈령은 국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적으로 한다.

제2조(정의) 이 훈령에서 사용하는 용어의 정의는 다음과 같다.

1. "정보통신망"이라 함은 「전기통신기본법」 제2조제2호의 규정에 의한 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.
2. "사이버공격"이라 함은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 말한다.
3. "사이버안전"이라 함은 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 말한다.
4. "공공기관"이라 함은 다음 각목의 기관을 말한다.
   가. 「정부투자기관관리 기본법」 제2조의 규정에 의한 정부투자기관
   나. 「정부산하기관관리 기본법」 제2조의 규정에 의한 정부산하기관
   다. 「정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항 및 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항의 규정에 의한 연구기관
   라. 그 밖에 다른 법령의 규정에 의하여 설립된 공공기관 중 제6조의 규정에 의한 국가사이버안전전략회의에서 정보통신망의 안전성 확보가 필요하다고 지정한 기관

제3조(적용범위) 이 훈령은 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망에 대하여 이를 적용한다. 다만, 「정보통신기반보호법」 제8조의 규정에 의하여 지정된 주요정보통신기반시설에 대하여는 적용하지 아니한다.

제4조(사이버안전 확보의 책무) ①중앙행정기관의 장은 소관 정보통신망에 대하여 안전성을 확보할 책임이 있으며 이를 위하여 사이버안전업무를 전담하는 전문인력을 확보하는 등

필요한 조치를 강구하여야 한다.
②관계 중앙행정기관의 장은 소관 공공기관 및 지방자치단체의 장으로 하여금 제1항의 규정에 의한 전문인력의 확보 등 필요한 조치를 강구하도록 하여야 한다.

제5조(국가사이버안전정책 및 관리) 국가사이버안전과 관련된 정책 및 관리에 대하여는 국가정보원장이 관계 중앙행정기관의 장과 협의하여 이를 총괄·조정한다.

제6조(국가사이버안전전략회의) ①국가사이버안전에 관한 중요사항을 심의하기 위하여 국가정보원장 소속하에 국가사이버안전전략회의(이하 "전략회의"라 한다)를 둔다.
②전략회의의 의장은 국가정보원장이 된다.
③전략회의의 위원은 외교통상부차관·법무부차관·국방부차관·행정자치부차관·정보통신부차관·국가안전보장회의사무처의 사무차장 및 전략회의 의장이 지명하는 관계 중앙행정기관의 차관급 공무원으로 한다.
④전략회의는 다음 각호의 사항을 심의한다.
1. 국가사이버안전체계의 수립 및 개선에 관한 사항
2. 국가사이버안전 관련 정책 및 기관간 역할조정에 관한 사항
3. 국가사이버안전 관련 대통령 지시사항에 대한 조치방안
4. 그 밖에 전략회의 의장이 부의하는 사항
⑤전략회의의 구성·운영 등에 관하여 필요한 사항은 전략회의의 의장이 따로 정한다.

제7조(국가사이버안전대책회의) ①전략회의의 효율적인 운영을 위하여 전략회의에 국가사이버안전대책회의(이하 "대책회의"라 한다)를 둔다.
②대책회의의 의장은 국가정보원의 사이버안전업무를 담당하는 차장이 되며, 위원은 전략회의의 위원이 속하는 기관의 실·국장급 공무원으로 한다.
③대책회의는 다음 각호의 사항을 심의한다.
1. 국가사이버안전 관리 및 대책방안
2. 전략회의의 결정사항에 대한 시행방안
3. 전략회의로부터 위임받거나 전략회의의 의장으로부터 지시받은 사항
4. 그 밖에 대책회의의 의장이 부의하는 사항
④대책회의의 구성·운영 등에 관하여 필요한 사항은 대책회의의 의장이 따로 정한다.

제8조(국가사이버안전센터) ①사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 위하여 국가정보원장 소속하에 국가사이버안전센터(이하 "사이버안전센터"라 한다)를 둔다.

②사이버안전센터는 다음 각호의 업무를 수행한다.
1. 국가사이버안전정책의 수립
2. 전략회의 및 대책회의의 운영에 대한 지원
3. 사이버위협 관련 정보의 수집·분석·전파
4. 국가정보통신망의 안전성 확인
5. 국가사이버안전매뉴얼의 작성·배포
6. 사이버공격으로 인하여 발생한 사고의 조사 및 복구 지원
7. 외국과의 사이버위협 관련 정보의 협력
③국가정보원장은 사이버안전센터의 업무 수행과 관련하여 필요하다고 인정하는 경우에는 관계 중앙행정기관의 장에게 소속 공무원 및 전문요원의 파견을 요청할 수 있다.

제9조(사이버안전대책의 수립·시행 등) ①중앙행정기관의 장은 소관 정보통신망을 보호하기 위하여 사이버안전대책을 수립·시행하고, 이를 지도·감독하여야 한다.
②관계 중앙행정기관의 장은 공공기관의 장 및 지방자치단체의 장으로 하여금 제1항의 규정에 의한 사이버안전대책을 수립·시행하도록 할 수 있다.
③국가정보원장은 제1항 내지 제2항의 규정에 의한 사이버안전대책의 수립에 필요한 국가사이버안전매뉴얼을 작성 배포할 수 있다. 다만, 국가사이버안전매뉴얼을 작성하는 경우에는 미리 관계 중앙행정기관의 장과 협의하여야 한다.
④국가정보원장은 제1항 내지 제2항의 규정에 의한 사이버안전대책의 이행여부 등 정보통신망에 대한 안전성을 확인할 수 있으며 필요하다고 인정하는 경우에는 해당 중앙행정기관의 장에게 시정 등 필요한 조치를 권고할 수 있다. 다만, 지방자치단체 및 공공기관의 정보통신망에 대한 안전성 확인은 관계 중앙행정기관의 장과 협의하여 수행한다.

제10조(사이버공격과 관련한 정보의 협력) ①중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 국가정보통신망에 대한 사이버공격의 계획 또는 공격사실, 사이버안전에 위협을 초래할 수 있는 정보를 입수한 경우에는 지체없이 그 사실을 국가정보원장에게 통보하여야 한다. 다만, 수사사항에 대하여는 수사기관의 장이 국가기밀의 유출·훼손 등 국가안보의 위협을 초래한다고 판단되는 경우에 입수한 정보를 국가정보원장에게 통보하여야 한다.
②국가정보원장은 제1항의 규정에 의하여 관련 정보를 제공받은 경우에는 대응에 필요한 조치를 강구하고 그 결과를 정보를 제공한 해당기관의 장에게 통지한다.

제11조(경보 발령) ①국가정보원장은 사이버공격에 대한 체계적인 대응 및 대비를 위하여 사이버공격의 파급영향, 피해규모 등을 고려하여 관심·주의·경계·심각 등 수준별 경보를

발령할 수 있다. 다만, 민간분야에 대하여는 정보통신부장관이 경보를 발령하며, 국가정보원장과 정보통신부장관은 국가차원에서의 효율적인 경보 업무를 수행하기 위하여 경보 관련 정보를 발령 전에 상호 교환하여야 한다.
②제1항의 규정에 의하여 경보를 발령하였을 때에는 관계 중앙행정기관의 장은 공공기관의 장 및 지방자치단체의 장에게 이를 신속히 전파하고 적절한 조치를 취하여야 한다.
③국가정보원장은 사이버공격이 국가안보에 중대한 위해를 초래할 것으로 판단되는 경우에는 국가안전보장회의사무처장과 협의하여 심각 수준의 경보를 발령할 수 있다.
④국가정보원장은 제1항의 규정에 의한 경보 발령에 필요한 정보를 관계 중앙행정기관의 장에게 요청할 수 있다. 이 경우 관계 중앙행정기관의 장은 특별한 사유가 없는 한 이에 협조하여야 한다.

제12조(사고통보 및 복구) ①중앙행정기관의 장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취하고 지체없이 그 사실을 국가정보원장에게 통보하여야 한다.
②공공기관 및 지방자치단체의 장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취한 후 그 사실을 관계 중앙행정기관의 장에게 통보하고, 관계 중앙행정기관의 장은 이를 지체없이 국가정보원장에게 통보하여야 한다.
③국가정보원장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견하거나 제1항 및 제2항의 규정에 의한 통보를 받은 때에는 관계 중앙행정기관의 장에게 사고복구 및 피해의 확산방지에 필요한 조치를 요청할 수 있으며, 요청받은 관계 중앙행정기관의 장은 특별한 사유가 없는 한 이에 협조하여야 한다.

제13조(사고조사 및 처리) ①국가정보원장은 사이버공격으로 인하여 발생한 사고에 대하여 그 원인 분석을 위한 조사를 실시할 수 있다. 다만, 경미한 사고라고 판단되는 경우에는 해당 기관의 장이 자체적으로 조사하게 할 수 있으며, 이 경우 해당 기관의 장은 사고개요 및 조치내용 등 관련 사항을 국가정보원장에게 통보하여야 한다.
②국가정보원장은 제1항의 규정에 의하여 조사한 결과 범죄혐의가 있다고 판단되는 경우에는 해당 기관의 장과 협의하여 수사기관의 장에게 그 내용을 통보할 수 있다.
③국가정보원장은 사이버공격으로 인하여 그 피해가 심각하다고 판단되는 경우에는 관계 중앙행정기관의 장과 협의하여 범정부적 합동조사 및 복구지원팀을 구성·운영할 수 있다.
④국가정보원장은 제3항의 규정에 의한 합동조사 및 복구를 위하여 관계 중앙행정기관의 장에게 필요한 인력 및 관련 자료의 지원을 요청할 수 있다.

제14조(전문기관간 협력) ①사이버안전업무를 전담하는 전문기구를 운영하는 기관은 국가사이버안전업무를 효율적으로 수행하기 위하여 다음 각호의 사항을 상호 긴밀히 협력하여야 한다.

1. 사이버위협 관련 정보의 탐지 및 정보공유체계의 구축·운영
2. 사이버안전 관련 정보의 분석·전파
3. 사이버안전 위해 요소에 대한 조치방안
4. 공격기법 분석 및 공격차단 등 대응방안
5. 그 밖에 경보의 수준별 세부 대응조치 등 필요한 사항

②사이버안전센터장은 제1항의 규정에 의한 전문기구를 운영하는 기관간 협력을 원활하게 하기 위하여 관계전문가 회의를 소집할 수 있다.

제15조(연구개발) ①국가정보원장은 국가사이버안전에 필요한 기술개발과 기술수준의 향상을 위하여 필요한 시책을 추진할 수 있다.

②중앙행정기관의 장은 공공분야의 사이버안전 관련 기술의 확보를 위하여 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항의 규정에 의하여 설립된 한국전자통신연구원의 국가보안기술 연구·개발을 전담하는 부설연구소로 하여금 관련 연구개발을 수행하게 할 수 있다.

③제2항의 규정에 의한 사이버안전에 필요한 기술의 연구개발에 관한 세부사항은 국가정보원장이 따로 정한다.

제16조(인력양성 및 교육홍보) ①관계 중앙행정기관의 장은 사이버안전의 기반 조성에 필요한 기술인력을 양성하고 국민의 인식제고를 위하여 다음 각호의 시책을 강구하여야 한다.

1. 사이버안전 관련 전문기술인력의 확보 및 양성
2. 사이버안전 교육프로그램의 개발 및 투자
3. 그 밖에 전문인력 양성, 교육 및 홍보 등에 관하여 필요한 사항

②국가정보원장은 관계 중앙행정기관의 장이 사이버안전과 관련한 전문인력의 양성, 교육 및 홍보를 위하여 필요한 지원을 요청하는 경우 이에 대하여 지원할 수 있다.

제17조(예산) 중앙행정기관의 장은 소관분야와 관련된 사이버안전대책의 수립·시행에 필요한 재정상의 조치를 강구하여야 한다.

제18조(안전성 확인 등에 대한 특례) ①제9조, 제11조 내지 제13조의 규정에 불구하고 국방분야의 사이버안전과 관련한 다음 각호에 대하여는 국방부장관이 그 업무를 수행한다.

1. 제9조제4항의 규정에 의한 안전성 확인
2. 제11조제1항의 규정에 의한 경보 발령
3. 제12조제1항의 규정에 의한 사고통보
4. 제13조제1항의 규정에 의한 사고조사

②국방부장관은 제1항의 규정에 의한 업무를 수행함에 있어 국가안보에 필요하다고 판단되는 경우에는 관련 내용을 국가정보원장에게 통보하여야 한다.

부 칙

이 훈령은 발령한 날부터 시행한다.

② 전자문서 보안조치 수행지침

2002. 9 국가정보원

제1조(목적) 이 지침은 「전자정부구현을위한행정업무등의전자화촉진에관한법률시행령」(이하 "영"이라 한다) 제34조제5항의 규정에 의하여 전자문서를 보관, 유통함에 있어 위조·변조·훼손 또는 유출 방지를 위하여 국가정보원장(이하 "국정원장"이라 한다)이 안전성을 확인한 보안조치를 하는데 필요한 사항을 규정함을 목적으로 한다.

제2조(적용범위) 이 지침은 영 제2조제2호의 규정에 의한 행정기관(국회, 법원, 헌법재판소 및 중앙선거관리위원회의 행정사무를 처리하는 기관을 제외한다)에 적용한다.

제3조(용어 정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. "전자정부"라 함은 정보기술을 활용하여 행정기관의 사무를 전자화 함으로써 행정기관 상호간 또는 국민에 대한 행정업무를 효율적으로 수행하는 정부를 말한다.
2. "행정기관"이라 함은 중앙행정기관(대통령 소속기관 및 국무총리 소속기관을 포함한다. 이하 같다) 및 그 소속기관, 지방자치단체를 말한다.
3. "전자문서"라 함은 컴퓨터 등 정보처리능력을 가진 체계에 의하여 전자적인 형태로 작성되어 송·수신 또는 저장되는 정보를 말한다.
4. "암호화"라 함은 국정원장이 승인한 암호체계 내에서 전자문서를 안전하게 유통하고 보관할 수 있도록 하는 행위를 말한다.
5. "암호모듈"이라 함은 전자문서의 암호화작업을 수행하기 위한 암호키, 키관리 검증서, 암호논리 등이 내장된 보안장치를 말한다.
6. "암호키"라 함은 전자문서를 암호화와 복호화를 수행하는데 사용되는 전자적 정보를 말한다.
7. "암호화 개인키"라 함은 암호화된 암호키를 복호하기 위하여 사용되는 전자적 정보를 말한다.
8. "암호화공개키"라 함은 암호키를 암호화하기 위하여 사용되는 전자적 정보를 말한다.
9. "키관리 검증서"라 함은 사용자가 소유하고 있는 암호화 개인키와 암호와 공개키가 합치한다는 사실을 확인, 증명하는 전자적 정보를 말한다.
10. "키관리 검증기관"이라 함은 검증서 발급 및 검증관련 기록 등 검증업무를 수행하는 자를 말한다.
11. "암호모듈관리관"이라 함은 안전한 장소에서 암호모듈 발급에 필요한 체계를 이용하여 암호모듈 발급업무를 수행하는 자를 말한다.

제4조(보안조치의 범위) 행정기관의 장은 전자문서의 보관 및 유통에 있어 변조·훼손 또는 유출 방지를 위하여 다음 각 호의 보안조치를 수립·시행하여야 한다.

1. 물리적 보안조치
2. 관리적 보안조치
3. 정보시스템·네트워크 보안조치
   가. 정보시스템·네트워크 구축 및 관리등과 관련한 보안조치
   나. 정보보호제품 도입 및 설치에 관한 보안조치
   다. 컴퓨터바이러스에 대한 보안조치
   라. 접근통제에 대한 보안조치
   마. 정보시스템 취약성에 대한 보안조치
   바. 기타 정보시스템·네트워므 보안에 필요한 조치
4. 전자문서 암호화
   가. 암호모듈 사용 및 관리에 필요한 보안조치
   나. 암호모듈 및 암호키 분실·유출 방지 등에 필요한 보안조치
   다. 기타 암호모듈의 획득·발급 등에 필요한 조치
5. 기타 정보통신환경의 변화에 따라 국정원장이 전자문서의 안전성 확보를 위하여 필요하다고 인정하는 사항

제5조(보안조치 안전성 확인) ①행정기관의 장은 전자정부 구현에 따른 정보시스템의 구축, 다른 전산망과의 연결 또는 전자문서 암호체계를 구현하거나 법 제45조의 규정에 의하여 전자정부 구현을 위한 중장기사업 계획을 수립하고자 할 경우에는 제4조제1항의 규정에 따른 보안대책을 강구하고, 국정원장의 안전성에 대한 확인을 문서(전자문서를 포함한다. 이하 같다)로 요청하여야 한다. 다만, 행정기관이 중앙행정기관이 아닌 경우에는 중앙행정기관을 경유하여야 한다.

②국정원장은 제1항의 규정에 따라 안전성 확인요청을 받은 경우에 그 결과를 관계중앙행정기관의 장에게 문서로 통보하며, 보안조치가 미흡하다고 판단되는 경우에는 보완을 요청할 수 있다.

③국정원장은 각 행정기관의 장이 수립한 보안조치와 그 시행상에 있어서의 미비점을 발굴 보완하거나 제1항의 규정에 의한 보안조치의 안전성에 대하여 원격이나 방문을 통하여 확인할 수 있다.

제6조(보안조치의 안전성 기술지원) 국정원장은 보안조치에 대한 안전성 확인을 위해 필요하다고 인정하는 경우 정부출연연구기관 등의 설립운영 및 육성에 관한 법률 제8조의 규정

에 의하여 설립된 한국전자통신연구원의 국가보안기술 연구 개발을 전담하는 부설연구소(이하 "국가보안기술연구소"라 한다)등을 기술지원 기관으로 지정하여 전자문서의 안전성에 필요한 기술적 지원을 수행하게 할 수 있다.

제7조(정보보호제품 획득에 대한 보안성 검토) ①행정기관의 장은 제4조의 보안 조치와 관련된 정보보호제품을 도입하여 활용하고자 하는 경우에는 국정원장에게 해당 제품에대한 보안기능 및 운영환경 적합성 등에 대하여 보안성검토를 요청하여야 한다.
②국정원장은 전자정부의 정보시스템에 대한 보안조치를 효율적으로 구현하기 위하여 정보보호제품에 요구되는 보안기능 및 보증에 대한 규격 등을 고지할 수 있다.

제8조(전자문서의 암호화) 행정기관의 장은 전자문서의 안전성을 확보하기 위하여 비밀인 전자문서와 영 제34조제1항 내지 제2항의 규정에 의하여 보호되어야 할 행정정보 및 전자공문서를 보관 또는 유통하는 경우에는 국정원장이 승인한 암호알고리즘으로 암호화하여야 한다.

제9조(암호모듈 사용) 행정기관의 장이 전자문서를 암호화하기 위하여 암호모듈을 사용하고자 할 경우에는 국정원장의 승인을 받아야 하며, 제8조의 규정에 의한 암호알고리즘은 승인받은 암호모듈 내에서 유지되어야

제10조(암호모듈 발급) ①행정기관의 사용자는 제16조에 의한 해당 암호모듈관리관에게 암호모듈 신청서를 작성 제출하고, 해당 암호모듈관리관은 사용자의 신원을 확인한 후 사용자의 정보 및 키관리 검증업무에 필요한 사항을 암호모듈에 기록하여 사용자에게 발급한다.
②행정기관의 장은 암호모듈을 발급한 경우 행정기관 사용자의 암호모듈신청서(별지 제1호 서식) 사본과 암호모듈발급관리대장(별지 제2호 서식)사본을 국정원장에게 제출하여야 한다.

제11조(암호모듈 관리) ①행정기관의 장은 해당기관에서 사용하는 암호모듈이 분실 또는 유출되거나 훼손된 경우에는 그 사실을 국정원장에게 즉시 통보하여야 한다.
②제1항의 규정에 의하여 통보를 받은 국정원장은 암호모듈에 대한 안전성과 신뢰성을 확보할 수 있는 조치를 강구하여야 한다.

제12조(전자문서 암호화 업무수행) ①전자문서의 암호화 등과 관련하여 국가정보원은 다음 각 호의 업무를 수행한다.
1. 암호키 생성·저장·분배·파기 등의 키관리 제반업무

2. 암호알고리즘 및 암호프로그램에 대한 암호모듈 주입 업무
3. 암호키관리센터에 대한 업무 조정 및 통제
4. 키관리 검증기관 지정 업무
5. 키관리 검증기관 실질심사
6. 키관리 검증기관 준수 요건 및 기준 수립
7. 기타 전자문서의 암호화 및 키관리와 관련된 기술개발계획 수립 등 필요한 사항

제13조(키관리 검증기관의 지정) 국정원장은 키관리 검증업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 키관리 검증기관으로 지정할 수 있다.

제14조(키관리 검증기관의 신청 및 실질심사) ①키관리 검증기관으로 지정받고자 하는 자는 국정원장에게 키관리 검증기관의 지정을 신청하여야 한다.
②신청을 받은 국정원장은 키관리 검증기관으로 지정받고자 하는 자에 대한 실질심사를 실시하고, 적합하다고 판단되는 경우에는 신청자에게 키관리 검증기관으로 지정하여야 한다.
③제2항의 규정에 의한 키관리 검증기관의 지정 및 실질심사 등에 관한 필요한 사항은 국정원장이 정한다.

제15조(키관리 검증 관리업무) ①국정원장은 키관리 검증에 대한 안전성 및 신뢰성을 확보하기 위하여 키관리 검증기관의 암호화공개키에 대한검증업무를 수행한다.
②키관리 검증기관은 사용자 및 암호모듈관리관에 대한 키관리 검증업무를 수행하며, 검증업무를 개시하기 전에 국정원장으로부터 암호화공개키를 검증받아야 한다.

제16조(암호모듈관리관 운영) ①각 행정기관은 각 기관에서 사용하는 암호모듈의 발급을 해당기관의 암호모듈관리관을 통해 수행하여야 한다.
②각 행정기관은 암호모듈의 발급에 필요한 예산을 확보하여야 한다.
③해당 행정기관에서 불가피하게 암호모듈을 발급하지 못할 경우에는 국가정보원에 암호모듈 발급업무의 대행을 요청할 수 있다.
④각 행정기관의 암호모듈관리관은 해당 행정기관의 장이 임명하며, 암호모듈 관리관을 임명한 경우에는 국정원장에게 통보하여야 한다.

제17조(종합 보안대책 수립) ①국정원장은 법 제45조의 규정에 의한 전자정부 중장기사업계획에 반영하기 위함이거나 행정기관의 보안조치 추진에 대한투명성을 제고시키기 위하여 범정부차원의 종합 보안대책을 수립 지원할 수 있다.

②국정원장은 제1항의 규정에 의한 종합대책을 수립하기 위하여 행정기관의 보안조치 추진실적과 향후계획 등 관련 자료를 요청할 수 있다.이 경우에 행정 기관의 장은 특별한 사유가 없는 한 관련내용 요청에 협조하여야 한다.
③제1항의 종합 보안대책은 제18조제1항의 규정에 의한 전자정부보안대책협의회의 협의를 거쳐 정한다.
④행정기관 및 전자정부 주무기관의 장은 전자정부를 구현함에 있어 제1항의 규정에 의한 종합보안대책을 적극 반영하여야 한다.

제18조(전자문서 보안조치와 관련된 협의) ①국정원장은 다음 각 호의 사항에 대한 업무추진을 위하여 행정기관의 의견을 수렴하고, 협의조정을 위하여 필요하다고 인정할 경우에는 관계기관의 공무원들로 전자정부보안대책협의회를 구성·운영할 수 있다.
1. 종합 보안대책 수립에 관한 사항
2. 전자문서 보관 및 유통에 따른 보안조치에 관한 사항
3. 전자문서의 보안조치와 관련하여 행정기관의 역할에 관한 사항
4. 암호키 관리 및 보관에 관한 사항
5. 기카 전자문서의 보안에 대한 국정원장이 부의하는 사항
②국정원장은 전자정부보안대책협의회의 운영을 위해 효율적이라고 판단되거나 전자문서의 안전한 유통·보관을 위하여 필요한 사항에 대하여 하계 및 민간기관 전문가로부터 자문을 받을 수 있다.
③제1항의 규정에 의한 전자정부보안대책협의회의 구성 및 운영에 관하여 필요한 사항은 국정원장이 별도로 정한다.

제19조(기술개발 및 보급지원) ①행정기관의 장은 전자문서의 안전성을 확보하기 위하여 보안기술 또는 관련 장비의 개발 보급에 필요한 대책을 강구하여야 한다.
②국정원장은 제1항의 규정에 의하여 개발된 기술 또는 장비의 시험적용이 필요한 경우에는 해당기관을 지정, 적용하게 할 수 있다.

제20조(전자문서 연계에 따른 보안조치 협력) 행정기관의 장은 개인, 산업체, 민간단체 등이 정부의 전자정부 시스템에 연계하여 전자문서를 유통하거나 전자거래를 수행하고자 하는 경우에는 정부의 보안조치를 권고할 수 있다.

제21조(준용) 이 지침이 정하지 아니한 사항으로서 전자문서의 안전성에 관련된 사항은 보안업무규정 및 국가정보통신보안기본지침을 따른다.

❸ 전산자료 보호등급 세부 분류기준

1. 목적 및 적용대상

1-1. 목 적

이 기준은 국가정보보안기본지침 제32조(전산자료 보호등급 분류기준)에 따라 각급 기관별 전산자료의 가치 및 중요도에 따른 보안수준을 분류하여 전산자원을 체계적·효율적으로관리함에 있어 참고할 수 있도록 세부사항을 권고함에 있음

1-2. 적용 대상

이 기준은 비밀로 분류된 전산자료를 제외한 일반자료를 대상으로 함

2. 용어 정의

가. "기밀성"이라 함은 정당한 사용자가 허용된 정보만을 알수 있도록 하는 정보보호의 특성을 말함

나. "무결성"이라 함은 비인가자가 정보내용을 불법적으로 위·변조 또는 훼손할 수 없도록 하는 정보보호의 특성을 말함

다. "가용성"이라 함은 정당한 사용자가 정보를 접근하고자 할 경우 지체없이 접근하여 사용할 수 있도록 하는 정보보호의 특성을 말함

3. 분류 기준

3-1. 분 류

전산자료 보호가치 및 업무특성 등 각급기관의 전산환경에 적합한 전산자료의 보호등급을 분류함

3-2. 전산자료 특성

동 기준은 전산자료의 기밀성·무결성·가용성 등 정보보호 특성을 고려하여 설정함. 다만, 각급기관의 전산환경에 따라 동 기준에서 제시한 3가지 특성 이외에 다른 정보보호 특성을 고려할 수 있음

3-3. 보호등급 단계

전산자료의 보호수준은 기밀성·무결성·가용성 등 정보보호 특성이 손상될 경우에 예상 피해

정도에 따라 '가'급, '나'급, '다'급의 3단계로 구분할 수 있음

① 보호수준이 '가'급인 경우는 3가지 정보보호 특성 중 한 가지 특성이 손상되더라도 예상되는 피해정도가 클 경우를 말함

② 보호수준이 '나'급인 경우는 3가지 정보보호 특성 중 한 가지 특성이 손상되더라도 예상되는 피해정도가 중간일 경우를 말함

③ 보호수준이 '다'급인 경우는 3가지 정보보호 특성 중 한 가지 특성이 손상되더라도 예상되는 피해정도가 낮은 경우를 말함

3-4. 예상 피해정도의 구분

전산자료의 기밀성·무결성·가용성 등이 손상될 경우 피해정도는 다음과 같이 결정함

가. 피해정도가 큰 전산자료는 다음과 같은 경우임

① 개인 신상 및 재산권에 심각한 손상을 줄 수 있는 피해

② 기관의 신뢰성에 심각한 손상을 줄 수 있는 피해

③ 기관의 중요업무 수행에 장애를 줄 수 있는 피해

④ 복구에 많은 예산과 상당한 기간이 요구되는 피해

⑤ 다른 기관의 업무수행에 영향을 주는 피해

나. 피해정도가 중간인 전산자료는 다음과 같은 경우임

① 개인 신상 및 재산권에 경미한 손상을 줄 수 있는 피해

② 기관의 기본적 임무수행에 지장을 초래하는 피해

③ 기관의 신뢰성을 손상하는 피해

④ 내부 관리상 문제를 주는 피해

⑤ 다른 기관의 업무수행에 경미한 영향을 주는 피해

다. 피해정도가 낮은 전산자료는 다음과 같은 경우임

① 중요업무가 아닌 부수적 업무수행에 경미한 지장을 주는 피해

② 기관의 신뢰성에 경미한 손상을 주는 피해

③ 내부 관리상 문제가 발생하나 빠른 기간 내에 복구가 가능한 피해

라. 추가 고려사항

전산자료의 기밀성·무결성·가용성 등 정보보호 특성 이외에 해당자료로 수행되는 업무의 중요성, 전산자료 보유건수 및 대체성 등을 고려할 수 있음

① 해당 전산자료로 수행되는 업무가 각급기관에서 차지하는 비중이 클수록 전산자료는 높은 부호수준을 요구함
② 입력된 전산자료의 건수가 많을수록 전산자료의 보호수준은 높게 요구될 수 있음
③ 해당 전산자료의 손상에 대비한 백업 등 대체수단이 없을 경우 전산자료의 보호수준은 높게 요구될 수 있음

④ 정보시스템 저장매체 불용처리지침

(국가정보원 사안-655(2006. 3. 13)

제1조(목적) 본 지침은 「국가정보보안기본지침」 제39조 제3항의 규정에 의하여 정보시스템 저장매체에 수록된 자료의 삭제방법과 세부 처리절차를 규정함을 목적으로 한다.

제2조(용어 정의) ① "저장매체"란 자기저장장치 · 광 저장장치 · 반도체 저장장치 등 자료기록이 가능한 전자장치를 말한다.
② "정보시스템"이라 함은 정보의 수집 · 가공 · 저장 · 검색 · 송신 · 수신에 활용되는 전자기기와 소프트웨어의 조직화된 체계를 말하며, 저장매체를 내장한 복사기 · 팩스 등 사무용 기기를 포함한다.
③ "소자(消磁)"란 저장매체에 역자기장을 이용해 매체의 자화값을 "0"으로 만들어 저장자료의 복원이 불가능하게 만드는 것을 말한다.
④ "완전포맷"이라 함은 저장매체 전체의 자료저장 위치에 새로운 자료(0 또는 1)를 중복하여 저장하는 것을 말한다.

제3조(정보시스템 저장자료 보안조치책임) 정보시스템을 폐기 · 양여 · 교체 · 반납하거나 외부 수리(이하 '불용처리'라 한다)를 위하여 당해 기관 외부로 반출할 경우 저장매체에 저장된 자료의 보안조치책임은 당해 기관의 장이 진다.

제4조(정보시스템 저장자료 삭제) 정보시스템 저장매체에 저장된 자료를 삭제할 경우는 다음과 같다.
1. 정보시스템의 사용연한이 경과하여 폐기 또는 양여할 경우
2. 정보시스템 무상 보증기간중 저장매체 또는 저장매체를 포함한 정보시스템을 교체할 경우
3. 정보시스템의 임대기간이 만료되어 반납할 경우
4. 고장 수리를 위한 외부 반출 등 당해 기관이 정보시스템 저장매체를 보안통제할 수 없는 환경으로 이동이 필요한 경우
5. 기타 정보시스템 사용자 변경 등으로 저장자료 삭제가 필요하다고 판단되는 경우

제5조(저장자료 삭제책임) ① 개인에게 지급된 정보시스템의 저장자료는 사용자 본인 책임하에 삭제하여야 한다.

② 홈페이지 등 각 부서가 공통적으로 사용하는 정보시스템은 정보보안담당관 책임하에 저장자료를 삭제하여야 한다.

제6조(저장자료 삭제방법의 지정) ① 각급기관의 정보보안담당관은 별표를 준용하여 당해 기관의 실정에 맞게 정보시스템별 저장자료 삭제방법을 사전 지정하여야 한다.
② 당해 기관내에서 정보시스템의 사용자가 변경된 경우, 비밀처리에 사용한 정보시스템은 완전포맷 3회 이상, 그 외의 정보시스템은 완전포맷 1회 이상으로 저장자료를 삭제하여야 한다.
③ 본 지침에서 정한 별표와 다른 방법으로 저장자료를 삭제하고자 할 때에는 사전 국가정보원장과 협의하여야 한다.

제7조(저장자료 삭제확인) ① 각급기관의 정보보안담당관은 정보시스템을 불용 처리할 경우 사전 저장자료 삭제여부를 확인하여야 한다.
② 정보시스템에 저장된 자료의 삭제를 외부업체에 의뢰할 때에는 정보보안담당관이 입회하여 삭제 절차·방법 준수여부 등을 확인 감독하여야 한다.

제8조(정보시스템 도입시 보안조치) ① 각급기관의 장은 정보시스템의 도입시 고장수리 등을 위해 공급업체가 저장매체를 교환·반출해 갈 경우에 대비, 저장자료 삭제방법 등 저장매체 보안조치 방안을 계약서상에 포함하여야 한다.
② 정보시스템을 임차 사용할 때에는 임차기간 만료후 반납시 당해 시스템의 저장자료 삭제방법 등 저장매체 보안조치 방안을 임차계약서상에 포함하여야 한다.

제9조(정보시스템 외부반출시 보안조치) ① 불용처리 등을 위해 정보시스템을 외부로 반출할 경우 사전 정보보안담당관의 통제를 받아야 하며 정보보안담당관은 그 현황을 기록 유지하여야 한다.
② 각급기관의 장은 저장매체의 고장수리·저장자료 복구 등을 외부에 의뢰할 경우 저장매체에 저장된 자료의 유출 방지를 위해 수리 또는 복구 참여자에 대해 보안서약서 집행·교육 등 필요한 보안조치를 하여야 한다.
③ 각급기관의 장은 정보시스템을 불용 처리할 경우 당해 시스템의 사용기관·부서·사용자 등을 인식할 수 있는 표시를 모두 제거하여야 한다.

제10조(소자장비 등의 적합성 검증) 각급기관의 장은 정보시스템의 저장자료를 삭제하는 장비나 소프트웨어를 도입할 경우 사전 국가정보원에 제품성능에 대한 적합성 검증을 의뢰하여야 한다.

제11조(삭제방법의 지속 개선) 각급기관의 장은 국가정보원과 긴밀히 협의하여 정보시스템에 저장된 자료의 삭제방법·절차 등을 지속 개선하여야 한다.

부 칙

(시행일) 이 지침은 2006년 3월 15일부터 시행한다.

<별표>

정보시스템 저장매체·자료별 삭제방법

저장매체 \ 저장자료	공개자료	민감자료 (개인정보 등)	비밀자료 (대외비 포함)
플로피디스크	㉮	㉮	㉮
광디스크 (CD·DVD 등)	㉮	㉮	㉮
자기 테이프	㉮·㉯중 택일	㉮·㉯중 택일	㉮
반도체메모리 (EEPROM 등)	㉮·㉰중 택일	㉮·㉰중 택일	㉮·㉰중 택일
	완전포맷이 되지 않는 저장매체는 ㉮ 방법 사용		
하드디스크	㉱	㉮·㉯·㉰중 택일	㉮·㉯중 택일

㉮ : 완전파괴(소각·파쇄·용해)
* 비밀이 저장된 플로피디스켓·광디스크 파쇄시에는 파쇄조각의 크기가 0.25mm 이하가 되도록 조치

㉯ : 전용 消磁장비 이용 저장자료 삭제
* 소자장비는 반드시 저장매체의 磁氣力보다 큰 磁氣力 보유

㉰ : 완전포맷 3회 수행
* 저장매체 전체를 '난수'·'0'·'1'로 각각 중복 저장하는 방식으로 삭제

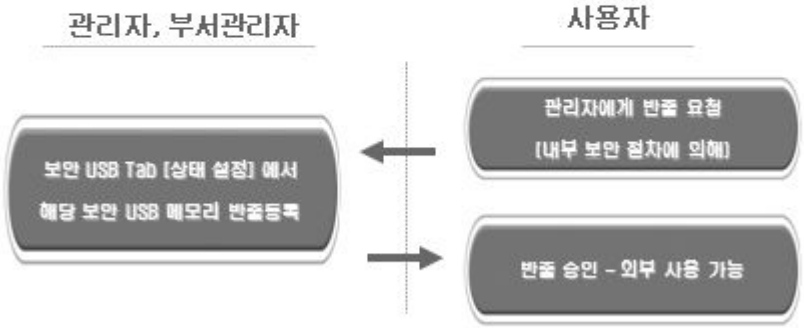
㉱ : 완전포맷 1회 수행
* 저장매체 전체를 '난수'로 중복 저장하는 방식으로 삭제

❺ 보조기억매체 사용상 주의사항

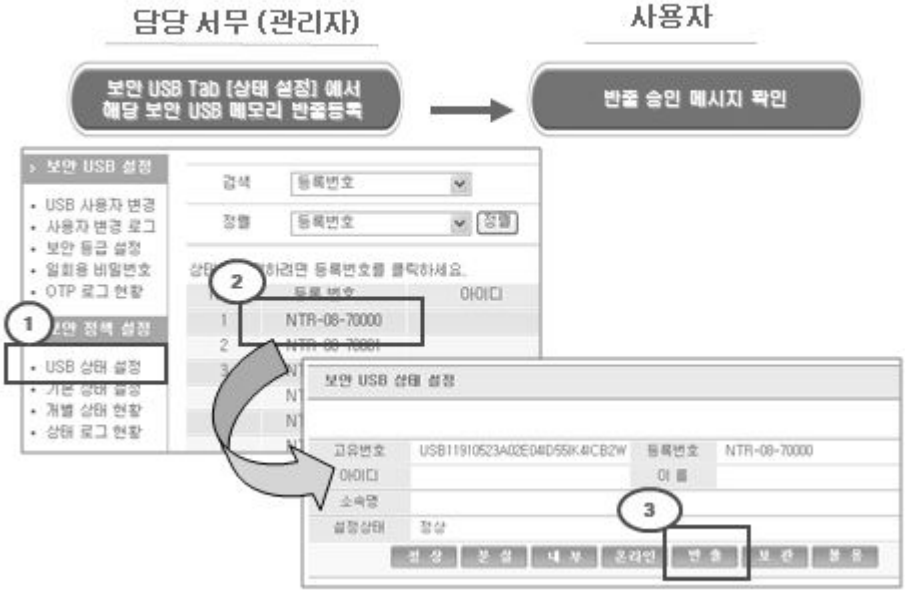
1. 보안USB 반출 승인하기

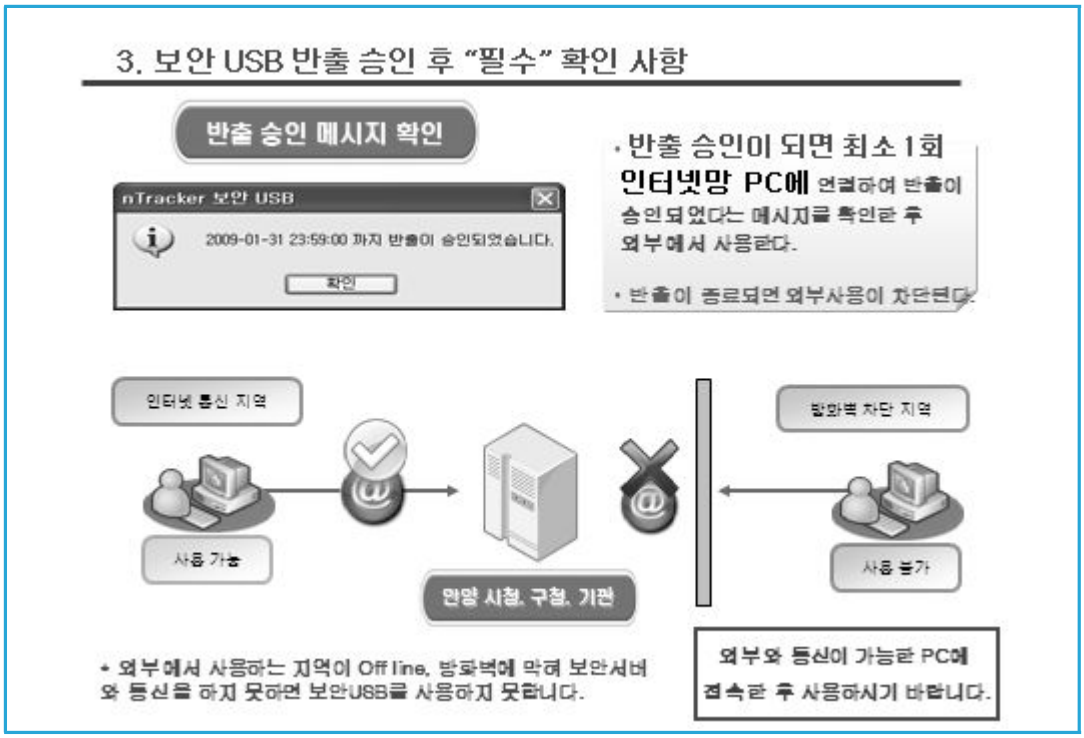
보안 USB 메모리 외부 사용시 반출을 승인한다.

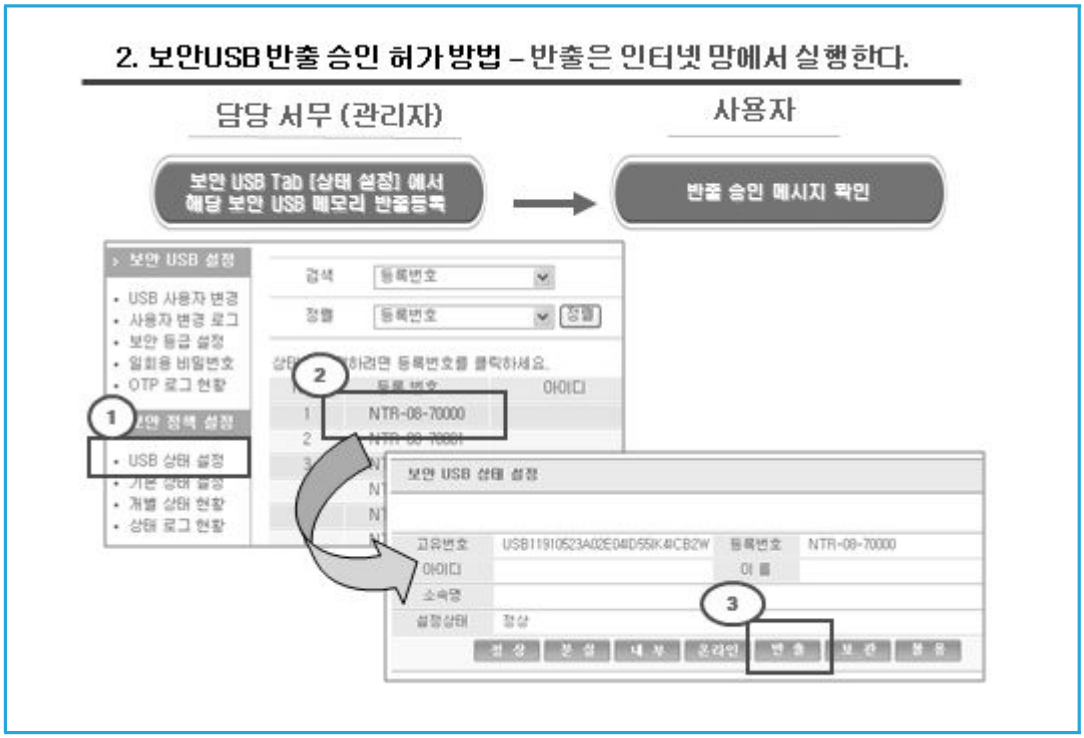
- 보안 USB 메모리는 업무망, 인터넷망에서만 사용할 수 있도록 보안 설정이 되어 있습니다.
  (보안 USB 메모리 적용기간을 두어 내 외부 구분 없이 사용 기간이 될 수 있음)
- 반출 승인은 내부 보안 절차에 따라 처리 한다.



2. 보안USB 반출 승인 허가방법 – 반출은 인터넷 망에서 실행한다.




3. 보안 USB 반출 승인 후 "필수" 확인 사항
반출 승인 메시지 확인
nTracker 보안 USB
2009-01-31 23:59:00 까지 반출이 승인되었습니다.
확인
• 반출 승인이 되면 최소 1회 인터넷망 PC에 연결하여 반출이 승인되었다는 메시지를 확인한 후 외부에서 사용한다.
• 반출이 종료되면 외부사용이 차단된다.
인터넷 통신 지역
방화벽 차단 지역
사용 가능
사용 불가
안양 시청, 구청, 기관
• 외부에서 사용하는 지역이 Off line, 방화벽에 막혀 보안서버와 통신을 하지 못하면 보안USB를 사용하지 못합니다.
외부와 통신이 가능한 PC에 접속한 후 사용하시기 바랍니다.

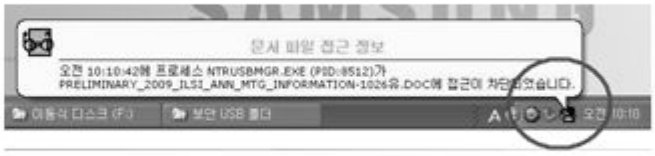

2. 보안USB 반출 승인 허가방법 – 반출은 인터넷 망에서 실행한다.
담당 서무 (관리자)
사용자
보안 USB Tab [상태 설정] 에서 해당 보안 USB 메모리 반출등록
반출 승인 메시지 확인
보안 USB 설정
USB 사용자 변경
사용자 변경 로그
보안 등급 설정
일회용 비밀번호
OTP 로그 현황
보안 정책 설정
USB 상태 설정
개별 상태 현황
상태 로그 현황
검색
등록번호
정렬
NTR-06-70000
아이디
보안 USB 상태 설정
고유번호
등록번호
NTR-08-70000
아이디
이 름
소속명
설정상태
정상
1
2
3

4. 파일 저장 작업시 주의 사항

- 파일이 오픈된 상태에서는 "보안USB"로 파일을 저장하면
- 정상적으로 저장이 되지 않습니다. – 암호화가 진행되지 못함.
- 반드시 오픈 된 화면을 종료한 후에 파일을 복사하시기 바랍니다.
- 문서를 수정 및 저장할 경우에는 자료의 유실을 방지하기 위해서는
- 반드시 휴지통 아이콘에서 "안전제거"를 해주시기 바랍니다.

5. 파일 복사 문제 – 해결 방법

문서 모니터링 S/W가
복사를 하지 못하게
방지하여 발생함



+ 해결 : 제어판 → 프로그램 추가/삭제에서 → "문서관리 모니터링" 프로그램을 제거한다.

프로그램을 제거한 후
다시 파일을 복사/복원 하면 정상적으로 복사가 됨.

제2편

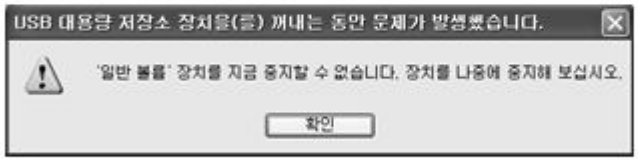
6. "안전 제거"가 되지 않을 때 조치

경고 문구 발생

"장치를 종지할 수 없습니다."

윈도우 탐색기 또는 다른 장치 또는 프로그램에서

이동식 디스크를 사용하고 있어 종료가 되지 못함.



* 해결 : 보안 USB를 강제로 포트에서 제거한다.

7. 보안 USB의 하드웨어 안전제거 방법

8. 기타 주의 사항

· 헤드폰 사용자 – PC를 어음하여 데이터를 전송할 수 없습니다.

- 삼성, LG, KTF등 통신사 프로그램이 PC에 설치되어 있는 경우
- 동영 멈춤 등 Lock(락)이 발생합니다.
- 예) AnycallPCManager를 삭제하여 PC에 락이 걸리지 않습니다.
- 삼성, LG, KTF 등 통신사 프로그램을 반드시 삭제 하시기 바랍니다.
- 충전용일 경우 사용이 가능합니다. (충전용 USB 케이블을 사용 바랍니다.)

· 외부 작업자가 농림수산식품부 내에서 작업을 할 경우

- 외부 작업자도 농림수산식품부 내에서는 일반 USB를 사용할 수 없습니다.
- 작업이 끝난 후 관련 담당자와 협의 하여 프로그램을 제거하시기 합니다.

· USB를 사용하여 공인인증서 로그인하기 – GPKI (행정용), NPKI (은행용)

- 공인인증서는 보안USB 또는 일반 USB로 복사를 받아 사용할 수 있습니다.
- 사용 전에 매체 등록이 되어 있어야 은행업무를 볼 수 있습니다. – 인터넷 뱅킹은 가능
- 인증서는 읽기만 가능합니다. 신규 저장 및 갱신은 집에 있는 PC를 사용하세요.

保安業務 便覽

발 행 처 | 농림수산식품부

발 행 인 | 운영지원과장 이 근 성

편집총괄 | 사 무 관 홍 상 표

편집정리 | 행 정 주 사 김 채 균

내용문의 | 농림수산식품부 운영지원과
☏ 02-500-1573

인 쇄 | 이문기업(주)
☏ 02-504-1600