

새만금개발청 정보보안 업무규정

제정 2014. 7. 29. 새만금개발청 훈령 제 28호
일부 개정 2016. 3. 30. 새만금개발청 훈령 제 70호
전부 개정 2020. 5. 27. 새만금개발청 훈령 제154호

제1장 총 칙

제1조(목적) 이 지침은 「국가 정보보안 기본지침」에 따라 새만금개발청의 정보보안업무에 필요한 사항을 정함을 목적으로 한다.

제2조(정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. “정보보안” 또는 “정보보호”라 함은 정보통신망 및 정보시스템을 통해 수집, 가공, 저장, 검색, 송·수신되는 정보의 유출, 위·변조, 훼손 등을 방지하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위로서 「국가사이버안전관리규정」 제2조제3호의 사이버안전전을 포함한다.
2. “정보보안담당관”이라 함은 새만금개발청의 정보보안업무를 총괄하기 위하여 새만금개발청장(이하 “청장”이라 한다)이 임명한 사람을 말한다.
3. “보안담당관”이라 함은 「보안업무규정」 제43조에 따른 보안담당관을 말한다.
4. “정보통신망”이라 함은 「국가정보화 기본법」 제3조제11호에 따른 정보통신망을 말한다.
5. “인터넷서비스망”(이하 “인터넷망”이라 한다)이라 함은 청장이 구축·운영하는 정보통신망 중에서 소속 공무원 등의 이용을 위한 인터넷과 연결된 정보통신망을 말한다.
6. “내부전산망”(이하 “내부망”이라 한다)이라 함은 청장이 구축·운영하는 정보통신망 중에서 인터넷과 분리된 업무 전용(專用) 정보통신망을 말한다.
7. “정보시스템”이라 함은 「전자정부법」 제2조 제13호에 따른 정보시스템을 말한다.
8. “휴대용 저장매체”라 함은 디스켓·CD·외장형 하드디스크·USB메모리

등 정보를 저장할 수 있는 것으로 PC·서버 등의 정보시스템과 분리할 수 있는 기억장치를 말한다.

9. “업무자료”라 함은 다음 각 목의 어느 하나에 해당하는 것을 말한다.
 - 가. 「전자정부법」 제2조제6호에 따른 행정정보 및 같은 법 제2조제7호에 따른 전자문서
 - 나. 「공공기록물 관리에 관한 법률 시행령」 제2조제2호에 따른 전자기록물
 - 다. 기타 다른 법령에 의하여 공무원등이 직무상 작성·취득하였거나 보유·관리하는 자료로서 전자적으로 처리되어 부호·문자·음성·음향·영상 등으로 표현된 것
10. “비밀”이라 함은 업무자료 중에서 「보안업무규정」 제4조에 따라 분류된 비밀을 말한다.
11. “대외비”라 함은 업무자료 중에서 「보안업무규정 시행규칙」 제16조제3항에 따라 분류된 대외비를 말한다.
12. “비공개 업무자료”라 함은 비밀 및 대외비를 제외한 업무자료 중에서 다음 각 목의 어느 하나에 해당하는 자료 또는 정보를 말한다.
 - 가. 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따른 비공개 대상 정보
 - 나. 가목에 따른 비공개 대상 정보의 주요 내용이 기술된 문장 또는 문구다. 그 밖에 청장이 비공개 대상 정보라고 판단하는 자료
13. “공개 업무자료”라 함은 업무자료 중에서 비밀 및 대외비와 비공개 업무자료를 제외한 모든 자료 또는 정보를 말한다.
14. “정보통신실”이라 함은 서버·스위치·라우터·교환기 등 전산 및 통신 장비 등이 설치·운영되는 장소 또는 전산실·통신실·데이터센터 등을 말한다.
15. “정보보호시스템”이라 함은 「국가정보화 기본법」 제3조제6호에 따른 정보보호시스템을 말한다.
16. “보안적합성 검증”이라 함은 정보보호시스템·네트워크장비 등 보안기능이 있는 정보통신제품에 대하여 「전자정부법 시행령」 제69조제1항 및 제3항에 따라 안전성을 검증하는 활동을 말한다.
17. “공무원등”이라 함은 국가공무원법 또는 그 밖에 법률, 규정 등으로 새만금개발청에 근무 중인 사람을 말한다.

18. “개별사용자”라 함은 청장으로부터 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 공무원등과 새만금개발청의 장과 계약에 의하여 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 사람을 말한다.
19. “전자파 보안”이라 함은 정보통신시설 및 기기 등을 대상으로 전자파에 의한 정보유출을 방지하고 파괴·오작동 유발 등의 위협으로부터 정보를 보호하는 일체의 행위를 말한다.
20. “대도청 측정(TSCM)”이라 함은 유·무선 도청탐지장비 등을 사용하여 은닉된 도청장치를 색출하거나 누설전자파(정보통신기기로부터 자유공간 또는 전도성 경로를 통해 비(非)의도적으로 누출되는 정보를 포함한 전자파) 등 각종 도청 위해(危害)요소를 제거하는 제반활동을 말한다.
21. “고출력 전자파(EMP)”라 함은 지상 30km 이상에서 핵 폭발에 의해 생성되는 고고도(高高度) 핵 전자파와 의도적으로 정보기기 등을 손상시키거나 오동작을 유발할 수 있는 고출력 비핵 전자파를 말한다.
22. “정보보안 관리실태 평가”라 함은 「전자정부법」 제56조 등에 따라 새만금개발청의 국가정보보안 정책에 대한 이행여부를 확인하기 위하여 실시하는 평가를 말한다.
23. “암호자재”라 함은 비밀을 소통·보호하기 위한 목적으로 암호기술을 적용하여 만들어진 장치나 수단을 말한다.
24. “암호알고리즘”이라 함은 정보의 유출, 위·변조, 훼손 등을 방지하기 위하여 기밀성·무결성·인증·부인방지 등의 기능을 제공하는 수학적 논리를 말한다.
25. “상용 암호모듈”이라 함은 암호알고리즘을 소프트웨어, 하드웨어, 펌웨어 또는 이를 조합한 형태로 구현한 것으로서 중요자료를 보호하기 위하여 민간이 상용(商用)으로 판매하는 것을 말한다.
26. “검증필 암호모듈”이라 함은 전자정부법 시행령 제69조 와 암호모듈 시험 및 검증지침 에 따라 국가정보원장이 안전성을 확인한 상용 암호모듈을 말한다.
27. “암호자재 제작업체”라 함은 암호자재의 저작권을 획득한 업체를 말한다.
28. “사이버공격”이라 함은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단을 사용하여 정보통신망을 불법침입·교란·마

- 비·파괴하거나 정보를 위조·변조·훼손·절취하는 행위를 말한다.
29. “안보위해(危害) 공격”이라 함은 사이버공격 중에서 다음 각 목의 어느 하나에 해당하는 행위를 말한다.
 - 가. 군사분계선 이북(以北)지역에 기반을 두고 있는 반(反)국가단체의 구성원 또는 그 지령을 받은 자에 의한 사이버공격
 - 나. 「방첩업무규정」 제2조제2호에 따른 외국의 정보활동
 - 다. 「산업기술의 유출방지 및 보호에 관한 법률」 제2조에 따른 국가핵심 기술 또는 국가연구개발사업으로 개발한 산업기술을 부정한 방법으로 취득하는 행위
 - 라. 「방위산업기술 보호법」 제2조제1호에 따른 방위산업기술을 부정한 방법으로 취득하는 행위
 - 마. 「국민보호와 공공안전을 위한 테러방지법」 제2조제1호에 따른 테러 행위
 - 바. 국제범죄조직에 의한 사이버공격
 - 사. 「형법」 중 내란(內亂)의 죄, 외환(外患)의 죄, 「군형법」 중 반란의 죄, 암호 부정사용의 죄, 「군사기밀 보호법」에 규정된 죄, 「국가보안법」에 규정된 죄에 해당되는 행위
 - 아. 국가기밀에 속하는 문서·자재·시설 및 지역에 관한 정보를 유출하거나 그 운영을 방해하는 행위
 - 자. 「전자정부법」 제56조제3항에 따른 보안조치 대상 정보통신망에서 전자문서를 위조·변조·훼손·절취하여 국가의 독립, 영토의 보전, 헌법과 법률의 기능, 헌법에 의하여 설치된 국가기관의 유지에 위해를 초래하는 행위
 - 차. 「정보통신기반 보호법」 제3조에 따라 공공분야 실무위원회가 담당하는 주요정보통신기반시설 또는 같은 법 제7조제2항 각 호에 따른 주요 정보통신기반시설에 대한 같은 법 제12조에 따른 침해행위
30. “보안관제”라 함은 사이버공격 정보를 실시간으로 탐지 및 분석, 대응하는 일련의 활동을 말한다.
31. “보안관제센터”라 함은 일정한 수준의 시설 및 장비와 이를 운영하기 위한 전문 또는 전담인력을 갖추고 보안관제업무를 수행하는 조직을 말한다.
32. “국가보안관제체계”라 함은 「국가사이버안전관리규정」 제10조의2제2

항에 따라 국가정보원장이 새만금개발청의 보안관제센터와 사이버공격에 관한 정보를 수집·배포하기 위하여 구축·운영하는 실시간 탐지·대응체계를 말한다.

33. “부문보안관제센터”라 함은 「국가사이버안전관리규정」 제10조의2제2항에 따라 설치·운영되는 보안관제센터 중에서 다음 각 목에 해당하는 기구를 말한다.

가. 중앙행정기관의 장이 해당기관의 정보통신망을 대상으로 운영하는 보안관제센터

나. 「책임운영기관의 설치·운영에 관한 법률」 제4조제1항에 따라 설치된 국가정보자원관리원(이하 “정보자원관리원”이라 한다)의 장이 국가기관·지방자치단체의 공동 활용을 위하여 운영하는 정보통신망(이하 “국가정보통신망”이라 한다) 및 정보자원관리원에 입주한 기관의 정보시스템을 대상으로 운영하는 보안관제센터

다. 행정안전부장관이 지방자치단체의 정보통신망을 대상으로 운영하는 보안관제센터

라. 교육부장관이 시·도 교육청의 정보통신망을 대상으로 운영하는 보안관제센터

마. 한국인터넷진흥원이 운영하는 침해사고대응센터

제3조(적용범위) 이 지침은 다른 법령에 규정된 것을 제외하고는 새만금개발청의 각 과 단위 부서(이하 “각 부서”라 한다) 및 그 밖에 업무상 새만금개발청의 조정·감독을 받는 단체에 대하여 적용한다.

제4조(책무) ① 청장은 국가안보 및 국익과 관련된 정보(업무자료를 포함한다. 이하 같다)와 정보통신망을 보호하기 위하여 보안대책을 수립·시행하여야 하며 정보보안에 대한 책임을 진다.

② 청장은 소속 공무원 등에 대한 근무성적 또는 성과 평가를 실시할 경우 정보보안내규 준수여부 등을 반영할 수 있다.

제5조(정보보안담당관 운영) ① 청장은 정보보안업무를 효율적이고 체계적으로 수행하기 위하여 정보보안 전문지식을 보유한 적정인력을 확보하여 정보보안 전담조직을 구성·운영하여야 한다.

② 청장은 다음 각 호에 해당하는 업무를 전담할 정보보안담당관을 임명하여야 한다. 이 경우 「정보통신기반 보호법 시행령」 제9조제1항에 따라 지정한 정보보호책임자를 정보보안담당관으로 임명할 수 있다.

1. 정보보안 정책·계획의 수립·시행 및 정보보안내규 제·개정
2. 정보보안 전담조직 관리, 전문인력 및 관련예산 확보
3. 정보화사업 보안성 검토 및 보안적합성 검증 총괄
4. 정보통신실, 정보통신망 현황자료 등에 관한 보안관리 총괄
5. 소관 주요정보통신기반시설 보호
6. 사이버공격 대응훈련 및 정보보안 관리실태 평가 총괄
7. 보안관제, 사고대응 및 정보협력 업무 총괄
8. 정보보안교육 총괄 및 ‘사이버보안진단의 날’ 계획 수립·시행
9. 정보보안감사 및 정보보안업무 감독
10. 부서 분임정보보안담당관 업무 감독
11. 그 밖에 정보보안과 관련한 사항

③ 청장은 정보보안담당관이 직무를 원활히 수행할 수 있도록 조직, 인력 및 예산을 운영하여야 한다.

④ 청장은 정보보안담당관이 직무를 효율적으로 수행할 수 있도록 각 부서의 공무원등 중에서 부서의 정보보안업무를 수행할 수 있는 적정인력을 분임정보보안담당관으로 임명하여야 한다. 별도로 임명하지 아니할 경우 각 부서의 장을 분임정보보안담당관으로 임명한 것으로 본다.

⑤ 정보보안담당관은 제2항 각 호에 해당하는 업무를 수행함에 있어 필요한 경우 해당 업무의 일부를 부서 분임정보보안담당관에게 위임할 수 있다.

제6조(연도 추진계획 수립) ① 청장은 매년 「연도 정보보안업무 추진계획」(「국가사이버안전관리규정」 제9조에 따른 사이버안전대책을 포함한다. 이하 같다)을 수립·시행하여야 한다.

② 청장은 정보보안 정책 및 계획을 수립·시행함에 있어 다른 기관과 협의·조정할 필요가 있을 경우 국가정보원장에게 조정을 요청할 수 있다.

제7조(정보보안감사 등) ① 청장은 정보보안업무 및 활동을 조사·점검하기 위하여 연1회 이상 정보보안감사를 실시하여야 하며, 이를 위하여 필요한 경우 정보보안담당관을 감사 또는 감찰업무를 수행하는 부서에 배속하여 정보보안감사

를 수행하도록 할 수 있다.

② 청장은 제1항에 따른 정보보안감사를 실시할 경우 국가정보원장이 배포한 정보보안점검 체크리스트 등을 활용할 수 있다.

③ 청장은 정보보안감사 담당자를 다음 각 호의 법규를 준용하여 우대하여야 한다.

1. 공공감사에 관한 법률 제18조에 따른 근무성적평정, 임용 등에서 우대
2. 중앙행정기관 등의 자체감사 역량 강화에 관한 규정 (국무총리훈령) 제7조에 따른 전문역량 강화 및 제9조에 따른 근무성적평정·전보·수당 등에서 우대
3. 자체감사활동의 지원 및 대행·위탁감사에 관한 규칙 (감사원규칙) 제4조제4호에 따른 근무여건 개선 및 사기제고
- ④ 청장은 정보보안감사 이외 정보보안업무에 필요한 경우 정보보안 점검방문을 실시할 수 있으며, 점검방문의 대상, 방식은 제2항부터 제4항까지를 준용한다.

제8조(정보보안교육) ① 청장은 정보보안에 대한 경각심을 제고하기 위하여 정보보안 교육계획을 수립하여 연1회 이상 모든 소속 공무원등을 대상으로 교육(온라인 교육을 포함한다)을 실시하여야 한다.

② 제1항에 따라 모든 공무원등은 특별한 사유가 없는 한 연1회 이상 정보보안 교육을 이수하여야 한다.

③ 청장은 제1항에 따라 정보보안교육을 실시할 경우 기관의 실정에 맞는 교육 자료를 작성 활용하여야 하며 필요한 경우 국가정보원장에게 자료 또는 강사 지원 등 협조를 요청할 수 있다.

④ 청장은 정보보안담당관, 분임정보보안담당관 및 정보보안담당자의 업무 전문성을 제고하고 소속 공무원등의 정보보안 지식을 함양하기 위하여 전문기관의 교육 이수나 학술회의 참가 등을 장려하여야 한다.

제9조(사이버보안진단의 날) ① 청장은 기관의 실정에 맞게 매월 세 번째 수요일을 ‘사이버보안진단의 날’로 지정·시행하여야 한다. 다만, 부득이한 사유로 해당 일에 시행하지 못할 경우 같은 달 다른 날에 시행하여야 한다.

② 부서 분임정보보안담당관은 정보보안담당관 총괄 하에 ‘사이버보안진단의 날’에 소속 부서의 정보통신망과 정보시스템의 보안취약 여부 확인 등 보안진단을 실시하여야 한다.

제2장 정보화사업 보안

제1절 사업 계획

제10조(보안책임) ① 새만금개발청에서 정보통신망 또는 정보시스템을 개발·구축·운영·유지보수하는 사업(이하 “정보화사업”이라 한다)을 담당하는 정보화사업담당관은 해당 정보화사업에 대한 보안관리를 수행하여야 한다.

② 정보화사업을 추진하는 부서의 장은 정보화사업에 대한 보안관리 책임을 지고 관리·감독하여야 한다.

③ 정보보안담당관 및 보안담당관은 각종 정보화사업과 관련한 보안대책의 적절성을 평가하고 정보화사업 수행 전반에 대하여 보안대책의 이행여부를 점검하여 필요한 경우 정보화사업을 추진하는 부서의 장에게 시정을 요구할 수 있다.

제11조(보안대책 수립) ① 청장은 정보통신망 또는 정보시스템을 구축·운영하기 위한 정보화사업 계획을 수립할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 보안관리체계(조직, 인원 등) 구축 등 관리적 보안대책
2. 설치·운영장소 보안관리 등 물리적 보안대책
3. 정보통신망 또는 정보시스템의 구성요소별 기술적 보안대책
4. 국가정보원장이 개발하거나 안전성을 확인한 암호자재, 상용 암호모듈 및 정보보호시스템 도입·운영계획
5. 긴급사태 대비 및 재난복구 계획
6. 용역업체 작업장소에 대한 보안대책
7. 기존 운용중인 정보통신망 및 정보시스템에 대한 용역업체 접근 통제대책
8. 누출금지정보 보안관리 방안

제12조(제안요청서 기재사항) ① 청장은 용역업체에 정보화사업을 발주하기 위하여 제안요청서를 작성할 경우 다음 각 호의 사항을 포함하여야 한다.

1. 용역업체 작업장소에 대한 보안요구사항

2. 기존 운용중인 정보통신망 및 정보시스템에 대한 용역업체 접근 통제대책
 3. 누출금지정보 목록
 4. 용역업체가 누출금지정보를 제외한 소프트웨어 산출물을 제3자에게 제공하고자 할 경우 발주자의 승인절차
- ② 제1항제3호에 따른 누출금지정보 목록을 작성할 경우 다음 각 호의 사항을 포함하여야 한다.
1. 기관 소유 정보시스템 내·외부 IP주소 현황
 2. 정보시스템 구성 현황 및 정보통신망 구성도
 3. 개별사용자의 계정·비밀번호 등 정보시스템 접근권한 정보
 4. 정보통신망 또는 정보시스템 취약점 분석·평가 결과물
 5. 정보화사업 용역 결과물 및 관련 프로그램 소스코드(외부에 유출될 경우 국가안보 및 국익에 피해가 우려되는 중요 용역사업에 해당)
 6. 암호자재 및 정보보호시스템 도입·운용 현황
 7. 정보보호시스템 및 네트워크장비 설정 정보
 8. 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따라 비공개 대상 정보로 분류된 기관의 내부문서
 9. 「개인정보보호법」 제2조제1호에 따른 개인정보
 10. 「보안업무규정」 제4조에 따른 비밀 및 동 규정 시행규칙 제16조제3항에 따른 대외비
 11. 그 밖에 청장이 공개가 불가하다고 판단한 자료

제2절 보안성 검토

- 제13조(검토 시기 및 절차)** ① 청장은 정보화사업을 수행하고자 할 경우 정보화사업과 관련한 보안대책의 적절성을 평가하기 위하여 사업 계획 단계(사업 공고 전)에서 보안성 검토 절차를 이행하여야 한다.
- ② 청장은 제1항에 따른 보안성 검토를 위하여 제14조제1항 및 제2항에 따라 보안성 검토 기관의 장에게 검토를 의뢰하거나 자체적으로 실시하여야 한다. 각 부서의 장이 제14조제1항 각 호에 해당하는 정보화사업에 대하여 국가정보원장에게 보안성 검토를 의뢰하고자 할 경우 정보보안담당관을 거쳐 의뢰하여야 한다.

제14조(검토 기관) ① 청장은 추진하는 다음 각 호에 해당하는 정보화사업에 대하여 국가정보원장에게 보안성 검토를 의뢰하여야 한다. 다만, 정보화사업의 규모·중요도 등을 고려하여 정보보안담당관이 자체적으로 보안성 검토 수행하도록 위임할 수 있다.

1. 비밀·대외비를 유통·관리하기 위한 정보통신망 또는 정보시스템 구축
2. 국가정보원장이 개발하거나 안전성을 확인한 암호자재를 적용하는 정보통신망 또는 정보시스템 구축
3. 외교·국방 등 국가안보상 중요한 정보통신망 또는 정보시스템 구축
4. 100만명 이상의 개인에 대한 「개인정보보호법」상 민감정보 또는 고유식별정보를 처리하는 정보시스템 구축
5. 주요정보통신기반시설로 지정이 필요한 정보통신기반시설 구축
6. 제23조제1항에 따른 제어시스템 도입
7. 재난관리·국민안전·치안유지·비상사태 대비 등 국가위기 관리와 관련한 정보통신망 또는 정보시스템 구축
8. 국가정보통신망 등 여러 기관이 공동으로 활용하기 위한 정보통신망 또는 정보시스템 구축
9. 행정정보, 국가지리, 환경정보 등 국가 차원의 주요 데이터베이스 구축
10. 정상회의, 국제회의 등 국제행사를 위한 정보통신망 또는 정보시스템 구축
11. 내부망 또는 폐쇄망을 인터넷 또는 다른 정보통신망과 연동하는 사업
12. 내부망과 기관 인터넷망을 분리하는 사업
13. 통합데이터센터·보안관제센터 구축
14. 소속 공무원등이 업무상 목적으로 이용하도록 하기 위한 무선랜, 이동통신망(HSDPA, WCDMA, LTE, 5G 등) 등 구축
15. 원격근무시스템 구축
16. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제20조에 따라 클라우드컴퓨팅서비스제공자의 클라우드컴퓨팅서비스(이하 “민간 클라우드컴퓨팅서비스”라 한다)를 이용하는 사업
17. 남북 회담 및 협력사업 등을 위한 북한지역 내 정보통신망 또는 정보시스템 구축
18. 외국에 개설하는 사무소 운영을 위한 정보통신망 또는 정보시스템 구축
19. 첨단 정보통신기술을 활용하는 정보화사업으로서 국가정보원장이 해당

기술에 대하여 안전성 확인이 필요하다고 지정하는 사업

② 청장은 다음 각 호에 해당하는 정보화사업에 대하여 보안성 검토를 실시한다.

1. 제1항 단서에 따라 국가정보원장으로부터 보안성 검토를 위임받은 사업
2. 홈페이지 및 웹메일 등 웹기반 정보시스템 구축
3. 인터넷전화시스템 구축
4. 다른 기관의 정보통신망 또는 정보시스템과 연동하여 정보의 소통 또는 서비스를 제공하는 정보시스템 구축
5. 새만금개발청 정보통신망 또는 정보시스템과 분리된 외부인 전용(專用) 무선랜, 인터넷망 및 교육장 정보통신망 등 구축
6. 인터넷과 분리된 소속 공무원등의 인사·복지관리 등의 목적을 위한 정보시스템 구축
7. 주요정보통신기반시설 취약점 분석·평가, 정보보안컨설팅 등 용역사업
8. 기존 분리된 내부망·기관 인터넷망간 자료전송시스템 구축 등 후속사업
9. 대규모 백업·재해복구센터 구축
10. 새만금개발청 정보통신망 또는 정보시스템과 분리된 영상회의시스템 구축
11. 인터넷과 분리된 CCTV 등 영상정보처리기기 구축
12. 백업시스템 구축
13. 대민(對民) 콜센터시스템 구축
14. 기타 청장이 필요하다고 판단하는 정보통신망 또는 정보시스템 구축

제15조(검토 생략) ① 청장은 다음 각 호에 해당하는 정보화사업에 대하여는 보안성 검토 절차의 이행을 생략할 수 있다. 이 경우 청장은 관련 매뉴얼·가이드라인 등을 준수하는 등 자체 보안대책을 수립·시행하여야 한다.

1. 제14조제1항 및 제2항 각 호의 정보화사업에 해당하지 아니하는 단순 장비·물품 도입
 2. 제14조에 따른 보안성 검토를 거쳐 완료한 정보화사업에 대하여 정보통신망 구성을 변경하지 아니하는 범위 내에서 다음 각 목의 사항을 포함한 후속운영·유지보수·컨설팅(단일 회선의 이중화는 본 호를 적용함에 있어 정보통신망 구성의 변경이 아닌 것으로 본다)
- 가. 서버·스토리지·네트워크장비 등 장비 노후화로 인한 단순 장비 교체
나. 전화기·무전기·CCTV 등 통신·영상기기의 노후화로 인한 단순 장비 교체

3. 다년도에 걸쳐 계속되는 사업으로써 사업 착수 당시 보안성검토를 완료한 후 사업 내용의 변동 없이 계속 추진하는 운영·유지사업

4. PC·프린터 및 상용 소프트웨어 등 단순 제품 교체

② 청장은 제1항제2호부터 제4호까지에 해당하는 정보화사업을 수행할 경우 기존 보안성 검토결과를 준수하여야 한다.

제16조(제출 문서) 정보화사업담당관은 제14조제2항에 따라 보안성 검토를 의뢰할 경우 다음 각 호의 사항이 포함된 문서를 제출하여야 한다.

1. 사업계획서(사업목적 및 추진계획을 포함한다)
2. 제안요청서
3. 정보통신망 구성도(필요시 IP주소체계를 추가한다)
4. 자체 보안대책

제17조(검토결과 조치) 청장은 제14조에 따라 보안성 검토결과를 통보받은 경우 검토결과를 반영하여 보안대책을 보완하여야 한다.

제18조(현황 제출) 정보보안담당관은 전년도에 실시한 정보화사업에 대한 보안성 검토결과 현황을 매년 1.25.까지 국가정보원장에게 제출하여야 한다.

제3절 사업 수행

제19조(정보통신제품 도입요건) 청장은 정보 및 정보통신망 등을 보호하기 위하여 정보보호시스템·네트워크장비 등 보안기능이 있는 정보통신제품을 도입·운용하고자 할 경우 [별표 1]에 따른 정보보호시스템 유형별 도입요건을 준수하여야 한다.

제20조(암호가 주기능인 제품 도입요건) 청장은 정보통신망을 이용하여 유통·보관되는 중요자료를 보호하기 위하여 암호가 주기능인 제품을 도입·운용하고자 할 경우 [별표 2]에 따른 암호가 주기능인 제품 도입요건을 준수하여야 한다.

제21조(상용 암호모듈 도입시 고려사항) 청장은 국가정보원장이 안전성을 확인한 상용 암호모듈을 도입하여 정보시스템 등에 적용하고자 할 경우 실제 적용 이전에 해당 상용 암호모듈의 정상 동작여부, 정보시스템 적용 단계에서 구동과정상 오류 발생여부 등을 점검하여야 한다.

제22조(영상정보처리기기 도입시 고려사항) 청장은 제78조제1항에 따른 영상정보처리기기를 도입·운용하고자 할 경우 한국정보통신기술협회(TTA)의 공공기관용 보안 성능품질 인증 등 일정한 보안성능이 확인된 제품을 우선적으로 도입할 수 있다.

제23조(제어시스템 도입시 고려사항) ① 청장은 설비 등을 중앙에서 감시·제어하기 위한 정보시스템(이하 “제어시스템”이라 한다)을 도입·운용하고자 할 경우 사업 계획 단계(사업 공고 전)에서 국가정보원장이 배포한 「국가·공공기관 제어시스템 보안가이드라인」에 따른 보안대책을 수립·시행하여야 한다.

② 청장이 도입하는 제어시스템의 실제 가동 이전에 국가정보원장에게 해당 제어시스템의 안전성 확인을 요청할 수 있다.

③ 청장은 제어시스템을 도입·운용할 경우 최신 백신 소프트웨어 설치, 응용프로그램 보안패치 및 침해사고 대응방안 등 보안대책을 수립·시행하고 정기적으로 취약점을 점검하여야 한다. 다만, 제어시스템에 백신 소프트웨어 등 보안 소프트웨어를 설치함으로써 제어시스템의 정상 운영에 차질을 초래할 경우 국가정보원장과 협의하여 설치하지 아니할 수 있다.

④ 청장은 국가안보상 중요한 제어시스템을 운용할 경우 인터넷 및 일반사무용 내부망과 분리·구축하여야 한다.

⑤ 청장은 제4항에도 불구하고 제어시스템을 기관 인터넷망과 연동할 필요가 있을 경우 연동 구간에 일방향 전송장비 설치 등 안전한 망연동 수단을 설치·운용하여야 한다.

제24조(계약 특수조건) ① 청장은 「국가를 당사자로 하는 계약에 관한 법률 시행령」 제76조제1항제3호다목에 따른 정보통신망 또는 정보시스템 구축 및 유지보수 등의 계약 이행과정에서 정보통신망 또는 정보시스템에 허가 없이 접속하거나 무단으로 정보를 수집할 수 있는 비인가 프로그램을 설치하거나 그러한 행위에 악용될 수 있는 정보통신망 또는 정보시스템의 약점을 고의로 생성 또

는 방지하는 행위 등을 금지하는 내용의 계약 특수조건을 계약서에 명시하여야 하며 계약기간(하자 보증기간을 포함한다) 내에 발생한 보안 약점 등에 대해서는 계약업체로 하여금 개선 조치하도록 하여야 한다.

② 청장은 필요한 경우 계약업체로부터 제1항과 관련한 행위가 없다는 대표자 명의의 확인서를 요구할 수 있다.

제25조(용역업체 보안) ① 청장은 용역업체에 정보화사업을 발주할 경우 다음 각 호의 보안사항을 준수하도록 계약서에 명시하여야 한다.

1. 제13조제1항 각 호에 따른 제안요청서에 포함된 사항
2. 소프트웨어 개발보안에 필요한 사항
3. 사업 참여인원의 보안관련 준수사항과 위반할 경우 손해배상 책임에 관한 사항
4. 사업 수행과 관련한 보안교육, 보안점검 및 사업기간 중 참여인원 임의 교체 금지
5. 정보통신망 구성도·IP주소 현황 등 업체에 제공하는 자료는 자료 인계 인수 대장을 비치하여 보안조치 후 인계·인수하고 무단 복사 및 외부반출 금지
6. 업체의 노트북·휴대용 저장매체 등 관련 장비는 반출·입시마다 악성코드 감염여부, 누출금지정보 무단 반출여부 등 점검
7. 사업 종료시 업체의 노트북·휴대용 저장매체 등 관련 장비는 저장자료 복구가 불가하도록 완전 삭제
8. 사업 종료 시 누출금지정보 전량 회수
9. 그 밖에 청장이 보안관리가 필요하다고 판단하는 사항 또는 국가정보원장이 보안조치를 권고하는 사항

② 청장은 비밀 및 중요 용역사업을 수행할 경우 용역업체 참여인원이 다음 각 호에 해당되는 사실을 알게 된 경우 교체를 요구하여야 한다.

1. 「국가공무원법」 제33조제3호부터 제6의3호까지에 해당하는 사람
2. 「국가를 당사자로 하는 계약에 관한 법률」 제27조제1항 각 호의 행위를 한 사람

③ 청장은 제1항에 따라 계약서에 명시된 보안 준수사항의 이행여부를 정기적으로 점검하고 미비점을 발견한 경우 용역업체로 하여금 시정 조치하도록 하여야 한다.

④ 그 밖에 용역업체 보안과 관련한 사항은 국가정보원장이 배포한 「국가·공

공기관 용역업체 보안관리 가이드라인」을 준수하여야 한다.

제26조(소프트웨어 개발보안) 청장은 정보시스템을 개발할 경우 「전자정부법」 제45조 및 「행정기관 및 공공기관 정보시스템 구축·운영지침」(행정안전부 고시)제50조부터 제53조까지에 따라 보안약점이 발생하지 아니하도록 개발(이하 “소프트웨어 개발보안”이라 한다)하고 정보시스템 감리 등을 통해 보안약점을 진단하여야 한다.

제27조(원격지 개발보안) ① 청장은 용역업체가 발주기관 이외 장소(이하 “원격지”라 한다)에서 개발 작업(유지보수는 제외한다)을 수행하고자 요청할 경우 제12조제1항제1호에 따른 용역업체 작업장소에 대한 보안요구사항 등을 포함한 관리적·기술적 보안대책을 수립·시행하여야 한다. 이 경우 정보화사업담당관은 보안대책을 수립한 후 정보보안담당관의 승인을 받아야 한다.

② 청장은 용역업체의 원격지 개발과 관련한 보안대책 이행여부를 정기 또는 수시로 점검(불시 점검을 포함한다)하여야 한다. 이 경우 정보화사업담당관이 점검한 후 그 결과를 정보보안담당관에게 통보하여야 한다.

③ 청장은 제2항에 따라 용역업체의 원격지 개발과 관련한 보안대책 이행여부를 점검한 결과 미흡하다고 판단될 경우 원격지 개발 허가를 취소하여야 한다.

④ 청장은 용역업체가 발주기관 내 장소에서 개발 작업을 수행하더라도 개발용 서버가 민간 클라우드컴퓨팅서비스를 이용하는 등으로 원격지에 위치할 경우 원격지 개발로 간주하고 제1항에 따른 보안대책을 수립·시행하여야 한다.

제28조(소프트웨어 산출물 제공) ① 청장은 용역업체가 「용역계약일반조건」(기획재정부 계약예규) 제56조에 따른 지식재산권을 행사하기 위하여 소프트웨어 산출물의 반출을 요청할 경우 제안요청서 또는 계약서에 명시된 누출금지정보에 해당하지 아니하면 제공하여야 한다.

② 청장은 제1항에 따라 소프트웨어 산출물을 용역업체에 제공할 경우 업체의 노트북·휴대용 저장매체 등 관련 장비에 저장되어 있는 누출금지정보를 완전 삭제하여야 하며 업체로부터 누출금지정보가 완전 삭제되었다는 대표자 명의의 확인서를 받아야 한다.

③ 청장은 용역업체가 소프트웨어 산출물을 제3자에게 제공하고자 할 경우 제공하기 이전에 승인을 받도록 하여야 한다.

④ 그 밖에 소프트웨어 산출물 제공과 관련한 사항은 「소프트웨어사업 관리감독에 관한 일반기준(과학기술정보통신부 고시)」을 준수하여야 한다.

제29조(누출금지정보 유출시 조치) ① 청장은 용역업체가 제안요청서 또는 계약서에 명시된 누출금지정보를 유출한 사실을 알게 된 경우 업체를 대상으로 계약 위반에 따른 조치를 취하여야 한다. 이 경우 용역업체의 누출금지정보 유출 사실을 알게 된 정보화사업담당관 또는 사업과 관계된 공무원 등은 즉시 정보보안담당관을 거쳐 소속 기관의 장에게 보고하여야 한다.

② 제1항에 따라 용역업체의 누출금지정보 유출 사실을 알게 되거나 보고를 받은 부서의 장은 그 사실을 관계 청장 및 국가정보원장에게 통보하여야 하고 「국가를 당사자로 하는 계약에 관한 법률 시행령」 제76조에 따라 입찰 참가자격 제한 등 관련조치를 취하여야 한다.

제4절 보안적합성 검증

제30조(검증대상 제품) ① 청장은 다음 각 호에 해당하는 제품을 도입하고자 하거나 도입한 경우 실제 적용·운용 이전에 안전성을 확인하기 위하여 보안적합성 검증을 받아야 한다.

1. 상용(商用) 정보보호시스템 등 정보보호를 목적으로 도입·운용하는 정보통신제품
2. 청장이 자체 개발하거나 업체 등에 의뢰하여 개발한 정보보호시스템
3. 저장매체 소자장비 또는 완전삭제 소프트웨어
4. L3 이상 스위치, 라우터 등 네트워크장비

② 청장은 제1항에도 불구하고 다음 각 호에 해당하는 제품의 경우 보안적합성 검증 절차를 생략할 수 있다. 다만, 제1호부터 제4호까지에 해당 하는 경우에는 국가정보원장이 해당 인증기관 및 시험기관의 결과를 수용한 제품에 한한다.

1. 「국가정보화 기본법」 제38조제1항 및 같은 법 시행령 제35조에 따라 과학기술정보통신부장관이 정한 정보보호시스템 공통평가기준을 준수한 인증(이하 “CC인증”이라 한다) 제도에 따라 국내용 CC인증 또는 국제용 CC인증을 받은 정보통신제품
2. 「소프트웨어산업 진흥법」 제13조에 따른 품질인증(이하 “GS인증”이라 한

다)을 받은 정보통신제품

3. 「정보보호산업의 진흥에 관한 법률」 제17조에 따른 성능평가를 받은 정보통신제품
 4. 「국가표준기본법」 제23조 및 공인기관 인정제도 운영요령(국가기술표준원 고시) 제3조에 따른 한국인정기구(KOLAS)(이하 “한국인정기구”라 한다)에 의해 국제표준(ISO/IEC 17025)에 따라 인정받은 시험기관에서 시험한 정보통신제품
 5. 국가정보원장이 공지한 검증필 제품목록에 등재된 정보통신제품
 6. 국가정보원장이 개발하고 안전성을 확인하여 기술 이전한 정보통신제품
- ③ 청장은 제2항에도 불구하고 취약점이 발견되거나 보안위협이 제기되는 제품의 경우 보안적합성 검증을 받아야 한다.

제31조(검증 기관) 청장은 도입하고자 하거나 도입한 제30조제1항 각 호에 해당하는 제품에 대하여 국가정보원장에게 검증을 의뢰하여야 한다.

제32조(검증 신청) ① 청장은 제30조에 따라 보안적합성 검증을 받고자 할 경우 제31조에 따른 검증 기관에 다음 각 호에 해당하는 문서·제품 등을 제출하고 검증을 신청하여야 한다.

1. 공통사항
 - 가. [서식 제1호]에 따른 보안적합성 검증 신청서
 - 나. 제안요청서 사본(해당하는 경우)
 - 다. 보안기능 운용설명서 등 제품설명서
 - 라. CC인증서 사본(해당하는 경우)
 - 마. 보안기능 점검결과
 - 바. 검증대상 제품
2. 네트워크장비
 - 가. 제1호의 공통사항 일체
 - 나. 장비 펌웨어 이미지 및 해시값
 - 다. [서식 제2호]에 따른 네트워크장비 변경내용 분석서(펌웨어 업데이트 경우에 해당)
3. 자체 개발하거나 업체 등에 의뢰하여 개발한 제품
 - 가. 제1호의 공통사항 일체

나. 기본 및 상세 설계서(검증 기관이 요청할 경우)

다. 개발완료 보고서

- ② 제1항에 따라 청장은 검증 기관의 장이 필요하다고 판단하여 추가 자료를 요청할 경우 이를 제출하여야 한다.

제33조(검증결과 통보 및 조치) 청장은 제품의 보안기능 보완 등 개선조치가 필요하다고 통보받은 경우 해당 조치를 실시하고, 그 결과를 검증기관의 장에게 통보하여야 한다.

제34조(취약점 조치) 청장은 보안적합성 검증이 완료된 제품에서 새로운 취약점이 발견된 경우 이를 제거 또는 보완하고 그 결과를 검증기관의 장에게 통보하여야 한다.

제35조(형상변경 및 용도변경시 조치) 청장은 보안적합성 검증이 완료된 제품의 보안기능 등 형상 변경이 필요하거나 도입 목적 이외 용도로 운용이 필요한 경우 검증 기관의 장과 협의하여 추가 검증 등 필요한 조치를 취하여야 한다.

제36조(도입현황 제출) 청장은 매 반기마다 해당 반기 내에 도입한 제30조에 따른 모든 제품에 대하여 [서식 제3호]에 따른 정보통신제품 도입현황 등을 검증 기관의 장에게 제출하여야 한다.

제3장 정보통신망 및 정보시스템 보안

제1절 정보통신망 보안

제37조(내부망·인터넷망 분리) ① 청장은 내부망과 기관 인터넷망을 분리·운영하여야 한다.

- ② 청장은 내부망과 기관 인터넷망을 분리·운영하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 침입차단·탐지시스템 설치 등 비(非)인가자 침입 차단 대책
2. 네트워크 접근관리시스템 설치 등 비(非)인가 장비의 내부망 접속 차단 대책

3. 내부망 정보시스템의 인터넷 접속 차단대책
 4. 내부망과 기관 인터넷망간 안전한 자료전송 대책
 5. 기타 국가정보원장이 배포한 국가·공공기관 업무전산망 분리 및 자료 전송 보안가이드라인 에서 제시하는 보안대책
- ③ 청장은 정보시스템에 부여되는 IP주소를 체계적으로 관리하여야 하며 비(非)인가자로부터 내부망을 보호하기 위하여 네트워크주소변환기(NAT)를 이용하여 사설 IP주소체계를 구축·운영하여야 한다. 또한 IP주소별로 정보시스템 접속을 통제하여 비(非)인가 기기에 의한 내부망 접속을 차단하여야 한다.
- ④ 청장은 분리된 내부망과 기관 인터넷망간 자료전송을 위한 접점이 불가피한 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.
1. 침입차단·탐지시스템 설치·운용
 2. 내부망과 기관 인터넷망간 접점 최소화
 3. 내부망과 기관 인터넷망간 일방향 전송장비 등을 이용한 자료전송체계를 구축·운영하고 원본파일은 3개월 이상, 전송기록은 6개월 이상 유지
 4. 정기적으로 전송실패 기록을 확인하고 악성코드 유입여부 등 점검
 5. 내부망 자료를 기관 인터넷망으로 전송할 경우 부서 분임정보보안담당관 또는 결재권자의 사전 또는 사후 승인절차 마련
- ⑤ 청장은 제1항에도 불구하고 예산 부족 등 사유로 부득이한 경우 국가정보원장과 협의하여 내부망과 기관 인터넷망을 분리하지 아니할 수 있다. 이 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.
1. 정보시스템 및 개별사용자 PC 영역 등에 대한 접근 통제대책
 2. 인터넷 PC의 악성코드 감염 최소화를 위한 인터넷 사용 통제대책
 3. 인터넷 PC의 악성코드 감염에 따른 내부망으로의 피해확산 차단대책
 4. 사이버공격 탐지·대응 등 안전한 업무환경을 위한 보호대책
- ⑥ 청장은 내부망과 기관 인터넷망의 IP주소 현황을 정기적으로 확인하고 갱신하여야 한다.

제38조(클라우드컴퓨팅 보안) ① 청장은 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제12조에 따라 클라우드컴퓨팅을 자체 구축·운영하고자 할 경우 국가정보원장이 배포한 「국가·공공기관 클라우드 컴퓨팅 보안가이드라인」에 명시된 기관 자체 클라우드컴퓨팅 구축 보안기준에 따라 보안대책을 수립·시행하여야 한다.

- ② 청장은 민간 클라우드컴퓨팅서비스를 이용하고자 할 경우 다음 각 호에 해당하는 사항을 준수하여야 한다.
1. 국내에 위치한 정보시스템에 데이터가 저장되는 서비스로서 일반 이용자용 서비스 영역과 물리적으로 분리되어 제공되는 서비스 영역(이하 “공공 전용(專用) 클라우드”라 한다)에 한하여 활용
 2. 과학기술정보통신부장관이 고시한 「클라우드컴퓨팅서비스 정보보호에 관한 기준」에 부합하는 서비스 선정
 3. 국가정보원장이 배포한 「국가·공공기관 클라우드 컴퓨팅 보안 가이드라인」에서 제시하는 민간 클라우드컴퓨팅서비스 이용 보안기준 및 행정안전부 장관이 배포한 「행정·공공기관 민간 클라우드 이용 가이드라인」에 따른 절차 이행
- ③ 새만금개발청의 내부망과 연동된 공공 전용(專用) 클라우드는 이 지침을 적용함에 있어 새만금개발청의 내부망으로 본다.
- ④ 새만금개발청의 기관 인터넷망과 연동된 공공 전용(專用) 클라우드는 이 지침을 적용함에 있어 새만금개발청의 기관 인터넷망으로 본다.
- ⑤ 제2항에 따라 민간 클라우드컴퓨팅서비스를 이용하는 부서의 장은 클라우드 컴퓨팅서비스제공자에 의하여 누출금지정보가 유출된 경우 제29조에 따른 조치를 취하여야 한다.

- 제39조(정보보호시스템·네트워크장비 보안)** ① 청장은 침입차단·탐지시스템 등 정보보호시스템과 스위치·라우터 등 네트워크장비를 설치·운영하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.
1. 물리적으로 안전한 장소에 설치하여 비(非)인가자의 무단접근 통제
 2. 기관 외부 정보통신망에서 정보보호시스템·네트워크장비에 대한 원격 접속 금지. 다만, 기관 내부에서의 원격 접속은 보안대책 수립 후 허용
 3. 최초 설치할 경우 디폴트(default) 계정은 삭제하거나 변경 사용하고 장비 관리를 위한 관리자 계정을 별도로 생성·운영
 4. 불필요한 서비스 포트와 개별사용자 계정은 차단 및 삭제
 5. 펌웨어 무결성과 컴퓨터 운영체제·소프트웨어의 취약점 및 버전 업데이트 여부를 정기적으로 점검하고 최신 버전으로 유지
- ② 장비 관리자는 정보보호시스템·네트워크장비의 로그기록을 1년 이상 유지하여야 하고 비(非)인가자의 접속여부를 정기적으로 점검하여 그 결과를 정보보

안담당관에게 통보하여야 한다.

- ③ 장비 관리자는 침입차단·탐지시스템의 침입차단·탐지규칙(rule)의 생성 근거를 유지하고 정기적으로 필요성 여부를 점검·갱신하여야 한다.

제40조(무선랜 보안) ① 청장은 내부망을 제외한 정보통신망에서 다음 각 호의 경우와 같이 청사 내에 무선랜(WiFi)을 구축·운영할 수 있다.

1. 기관 인터넷망에 중계기(AP)를 설치하여 제70조제1항에 따라 청장이 지급한 단말기의 접속만을 허용하는 업무용 무선랜
 2. 상용 인터넷망에 중계기(AP)를 설치하여 제75조제1항에 따라 반입한 공무원
 3. 상용 인터넷망에 중계기(AP)를 설치한 외부인 전용(專用) 무선랜
- ② 청장은 제1항에 따라 무선랜을 구축·운영하고자 할 경우 국가정보원장이 배포한 「국가·공공기관의 무선랜 구축 보안가이드라인」을 준수하여 보안대책을 수립·시행하여야 한다.
- ③ 제2항에 따른 보안대책을 수립할 경우 제1항제1호 및 제2호에 따른 무선랜에 대하여는 다음 각 호의 사항을 포함하여야 한다.
1. 네트워크 이름(SSID) 브로드캐스팅(broadcasting) 금지
 2. 추측이 어렵고 복잡한 네트워크 이름(SSID) 사용
 3. WPA2 이상(256비트 이상)의 암호체계를 사용하여 소통자료 암호화
 4. 비(非)인가 단말기의 무선랜 접속 차단 및 무선랜 이용 단말기를 식별하기 위한 IP주소 할당기록 등 유지
 5. IEEE 802.1X, AAA(Authentication Authorization Accounting) 등의 기술에 따라 상호 인증을 수행하는 무선랜 인증제품 사용
 6. 무선침입방지시스템 설치 등 침입 차단대책
 7. 기관의 내부망 정보시스템 또는 인접해 있는 다른 기관의 정보시스템이 해당 무선랜에 접속되지 아니하도록 하는 기술적 보안대책
 8. 그 밖에 무선랜 단말기·중계기(AP) 등 구성요소별 분실·탈취·훼손·오용 등에 대비한 관리적·물리적 보안대책
- ④ 부서 분임정보보안담당관은 제2항 및 제3항에 따른 보안대책의 적절성을 수시로 점검·보완하여야 한다.

제41조(이동통신망 보안) ① 청장은 이동통신망(HSDPA·WCDMA·LTE·5G 등)을 이용하여 시스템을 구축하거나 중요자료를 소통하고자 할 경우 암호화 및

비인가 단말기의 이동통신망 접속 차단 등 기술적 보안대책을 수립·시행하여야 한다.

- ② 청장은 제1항에 따라 이동통신망을 이용한 시스템을 구축·운영 할 경우 기관의 다른 정보통신망과 혼용되지 않도록 하여야 한다.

제42조(영상회의시스템 보안) ① 청장은 영상회의시스템을 구축·운영하고자 할 경우 통신망(국가정보통신망·전용(專用)선·인터넷 등) 암호화 등 보안대책을 수립·시행하여야 한다.

- ② 기타 영상회의시스템 보안과 관련한 사항은 국가정보원장이 배포한 「안전한 정보통신 환경 구현을 위한 네트워크 구축 가이드라인」을 준수하여야 한다.

제43조(인터넷전화 보안) ① 청장은 인터넷전화시스템을 구축·운영하거나 민간 인터넷전화 사업자망을 이용하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 한국정보통신기술협회(TTA) verified ver.4 이상 보안규격으로 인증받은 행정기관용 인터넷전화시스템 설치·운영
 2. 인터넷전화기에 대한 장치 및 사용자 인증
 3. 제어신호 및 통화내용 등 데이터 암호화
 4. 인터넷전화망과 다른 정보통신망과의 분리
 5. 인터넷전화 전용(專用) 침입차단시스템 등 정보보호시스템 설치·운영
 6. 백업체제 구축
- ② 청장은 민간 인터넷전화 사업자망을 이용할 경우 해당 사업자로 하여금 서비스 제공 구간에 대한 보안대책을 수립하도록 하여야 한다.
- ③ 기타 인터넷전화 보안과 관련한 사항은 국가정보원장이 배포한 「국가·공공기관 인터넷전화 보안 가이드라인」을 준수하여야 한다.

제44조(인터넷 사용제한) ① 청장은 국가비상사태 및 대형 재해·재난의 발생, 사이버공격 등으로부터 정보통신망과 정보시스템의 정상적인 운영을 보장하기 위하여 소속 공무원등에 대한 인터넷 사용을 일부 제한할 수 있다.

- ② 청장은 기관 인터넷망의 효율적인 운영 관리 및 악성코드 유입 차단을 위하여 게임·음란·도박 등 업무와 관련이 없는 인터넷 이용을 차단하여야 한다.

제45조(외교통신 보안) ① 청장은 재외공관과 비밀 등 중요자료를 소통하고자 할 경우 국가정보원장이 개발하거나 안전성을 확인한 암호자재를 사용하는 외교정보통신망을 사용하여야 한다.

② 청장은 재외공관에 직원을 파견하고자 할 경우 해당 직원에 대하여 파견 이전에 정보시스템 보안관리 방법 등 정보보안교육을 실시하여야 하며 파견 후에는 정보보안업무에 대한 인계인수를 철저히 하여야 한다.

③ 청장은 주요인사의 외국방문 행사와 관련한 자료 및 장비 등을 수발하고자 할 경우 외교정보통신망 또는 외교행낭 등 안전한 수단을 이용하여야 하며 일반 국제전화·팩스·인터넷 등 보안성이 없는 정보통신수단을 이용하여서는 아니 된다.

④ 기타 외교통신 보안과 관련한 세부사항은 국가정보원장이 제시하는 보안대책을 준수하여야 한다.

제2절 정보시스템 보안

제46조(정보시스템 보안책임) ① 청장은 정보시스템(PC·서버·네트워크장비·정보통신기기 등을 포함한다)을 도입·운용할 경우 해당 정보시스템에 대하여 관리자 및 관리책임자를 지정·운영하여야 한다.

② 정보시스템 관리자 및 관리책임자는 서버·네트워크장비 등 부서가 공동으로 사용하는 정보시스템의 운용·관리에 대한 보안책임을 진다.

③ 정보시스템 관리책임자는 정보시스템을 실제 운용하는 부서의 장이 되며 관리책임자는 [서식 제4호]에 따른 정보시스템 관리대장을 수기 또는 전자적으로 작성·관리하여야 한다.

④ 정보시스템 관리책임자는 해당 부서의 [서식 제4호]에 따른 정보시스템관리대장에 정보시스템의 최종 변경 현황을 유지하여야 하며 사본 1부를 정보보안담당관에게 제출하여야 한다.

⑤ 정보보안담당관은 정보시스템 운용과 관련하여 보안취약점을 발견하거나 보안대책 수립이 필요하다고 판단하는 경우 개별사용자, 정보시스템 관리자 및 관리책임자에게 개선 조치를 요구할 수 있으며 조치가 완료될 때까지 정보시스템의 운용을 일시 제한할 수 있다.

제47조(정보시스템 유지보수) ① 청장은 정보시스템의 유지보수와 관련한 절차, 주기, 문서화 등과 관련한 사항을 자체 내규(또는 지침 등)에 포함 하여야 한다. 정보시스템의 유지보수 절차 및 문서화를 수립할 경우 고려사항은 다음 각 호와 같다.

1. 유지보수 인원에 대한 보안서약서[서식 제7호] 집행, 보안교육 등을 포함한 유지보수 인가 절차를 마련하고 인가된 인원만 유지보수에 참여
2. 결함이 의심되거나 발생한 결함, 예방 및 유지보수에 대한 기록 유지
3. 유지보수를 위하여 정보시스템을 원래 설치장소에서 다른 장소로 이동할 경우 통제수단 마련
4. 유지보수 일시 및 담당자 인적사항, 출입통제 조치사항, 작업수행 내용 등 기록 유지

② 정보시스템 관리자는 용역업체 등이 유지보수와 관련한 장비·도구 등을 반출·입할 경우 악성코드 감염여부 및 자료 무단 반출여부 확인 등 보안조치를 실시하고 그 결과를 정보보안담당관에게 제출하여야 한다.

③ 정보시스템 관리자는 직접 또는 용역업체를 활용하여 정보시스템을 유지 보수할 경우 내부망 및 기관 인터넷망과 분리된 별도의 유지보수 전용(專用) 정보통신망 및 전용(專用) 단말기를 사용하여야 하며 기관 외부 정보통신망에서 원격으로 유지 보수하여서는 아니 된다. 다만, 불가피한 경우 보안대책 수립 후 정보보안담당관의 승인을 받아 수행하거나 용역업체에게 일정기간 동안 매번 접속 포트(port)를 열어주는 방식으로 접속을 허용할 수 있으며 접속사실이 기록된 로그기록은 1년 이상 보관하여야 한다.

④ 정보시스템 관리자는 정보시스템의 기능 개선·오류 수정 등을 위하여 용역업체를 통한 프로그램 개발이 필요할 경우 용역업체 인원을 해당 기관에 상주시켜 개발 작업을 수행하여야 한다. 프로그램 개발이 완료된 경우에는 정상 동작여부 등 안전성을 확인한 후 적용하여야 한다.

⑤ 청장은 소관 정보시스템에 대하여 중요도·가용성 등에 따라 등급을 분류하고 해당 등급에 맞게 정보 보존 및 관리, 장애관리, 보안관리 등을 수행하여야 한다.

제48조(정보시스템 위탁운영 보안) ① 청장은 소관 정보시스템에 대하여 외부업체 위탁 운영을 최소화하여야 한다. 다만, 위탁 운영을 할 경우에는 관리적·물리적·기술적 보안대책을 수립·시행하여야 한다.

- ② 정보시스템의 위탁 운영은 다른 기관 또는 외부업체 인원이 해당 기관에 상주(常駐)하여 수행하는 것을 원칙으로 한다. 다만, 해당 기관에 위탁 수행 인원의 상주(常駐)가 불가한 경우에는 보안대책 수립 후 그러하지 아니할 수 있다.
- ③ 기타 정보시스템 위탁운영 보안과 관련한 사항은 제25조(용역업체 보안)를 준용한다.

제49조(서버 보안) ① 청장은 서버를 도입·운영하고자 할 경우 사이버공격으로 인한 자료 절취 및 위·변조 등에 대비하여 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 서버 내 저장자료에 대하여 업무별·자료별 중요도에 따라 개별사용자의 접근권한 차등 부여
2. 개별사용자별 자료 접근범위를 서버에 등록하여 인가여부를 식별하도록 하고 인가된 범위 이외 자료 접근통제
3. 서버 운용에 필요한 서비스 포트 이외 불필요한 서비스 포트 제거 및 관리자용 서비스와 개별사용자용 서비스 분리·운용
4. 관리자용 서비스 접속시 특정 IP주소가 부여된 관리자용 단말기 지정·운용
5. 서버 설정 정보 및 저장자료에 대한 정기적 백업 실시
6. 데이터베이스에 대하여는 개별사용자의 직접 접속 차단, 개인정보 등 중요 정보 암호화 등 데이터베이스별 보안조치 실시

② 서버 관리자는 제1항에 따른 보안대책의 적절성을 수시 확인하여야 하며 연 1회 이상 서버 설정 정보와 저장자료의 절취 및 위·변조 가능성 등 보안 취약점을 점검·보완하여야 한다.

제50조(공개서버 보안) ① 청장은 외부인에게 공개할 목적으로 웹서버 등 공개서버를 구축·운영하고자 할 경우 내부망과 분리된 영역(DMZ)에 설치하여야 한다.

② 청장은 비(非)인가자의 공개서버 저장자료 절취 및 위·변조, 분산서비스거부(DDoS) 공격 등에 대비하여 침입차단·탐지시스템 및 DDoS 대응장비 설치 등 보안대책을 수립·시행하여야 한다.

③ 공개서버 관리자는 비(非)인가자의 공개서버 내 비공개 정보에 대한 무단접근을 방지하기 위하여 서버에 접근할 수 있는 개별사용자를 제한하고 불필요한 계정은 삭제하여야 한다.

④ 공개서버 관리자는 공개서버 서비스에 필요한 프로그램을 개발·시험하기 위하여 사용한 도구(컴파일러 등) 및 서비스와 관계가 없는 산출물은 개발 완료 후 삭제하여야 한다.

⑤ 기타 공개서버 보안과 관련한 사항은 제49조(서버 보안)를 준용한다.

제51조(로그기록 유지) ① 청장은 정보시스템의 효율적인 통제·관리 및 사고발생시 추적 등을 위하여 로그기록을 유지·관리하여야 한다.

② 제1항에 따른 로그기록에는 다음 각 호의 사항이 포함되어야 한다.

1. 접속자, 정보시스템·응용프로그램 등 접속대상
2. 로그인·오프, 자료의 열람·출력 등 작업 종류 및 시간
3. 접속 성공·실패 등 작업 결과
4. 전자우편 사용 등 외부발송 정보 등

③ 정보시스템 관리자는 로그기록을 생성하는 정보시스템의 경우 시간 동기화 프로토콜(NTP) 적용 등을 통해 정확한 기록을 유지하여야 한다.

④ 정보시스템 관리자는 로그기록을 정기적으로 점검하고 점검 결과 비(非)인가자의 접속 시도, 자료의 위·변조 및 삭제 등 의심스러운 정황이나 위반한 사실을 발견한 경우 즉시 정보보안담당관에게 통보하여야 한다.

⑤ 정보시스템 관리자는 로그기록을 1년 이상 보관하여야 하며 로그기록의 위·변조 및 외부유출 방지대책을 수립·시행하여야 한다.

제52조(업무용 통신단말기 보안) ① 청장은 업무용 통신단말기를 이용하여 업무자료 등 중요정보를 소통·관리하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 통신단말기에 대한 장치 및 개별사용자 인증
2. 제어신호 및 통화내용 등 데이터 암호화
3. 분실·탈취·훼손 등에 대비한 관리적·물리적·기술적 보안대책

② 청장은 제1항에 따른 보안대책을 수립하기 위하여 국가정보원장에게 취약점 점검 및 기술 지원을 요청할 수 있다.

③ 청장은 제1항제1호에 따른 통신단말기 개별사용자를 대상으로 인증 및 암호화에 필요한 디지털정보를 발급할 수 없을 경우 국가정보원장이 배포한 「정보통신기기 암호기술 적용지침」을 준수하여야 한다.

④ 청장은 기관의 주요 보직자가 안전한 통화를 위하여 사용하는 공용(公用)휴

대폰(이하 “보안폰“이라 한다)이 분실·훼손되지 않도록 현황을 관리하여야 한다. 이 경우 정보보안담당관은 데이터 암호화 등을 위하여 필요한 소프트웨어의 설치·유지보수 등을 지원할 수 있다.

제53조(모바일 업무 보안) ① 청장은 휴대폰·태블릿 PC 등을 이용한 모바일 업무환경(내부 행정업무, 현장 행정업무 및 대민서비스 업무 등)을 구축·운용하고자 할 경우 보안대책을 수립·시행하여야 한다.

② 기타 모바일 업무 보안과 관련한 사항은 국가정보원장이 배포한 「국가·공공기관 모바일 활용업무에 대한 보안가이드라인」을 준수하여야 한다.

제54조(사물인터넷 보안) ① 청장은 사물인터넷을 이용한 시스템을 구축·운용하고자 할 경우 사물인터넷 기기 및 중요 데이터 등을 보호하기 위하여 보안대책을 수립·시행하여야 한다.

② 청장은 사물인터넷을 이용한 시스템을 구축·운용하고자 할 경우 내부망과 분리하여야 한다. 다만, 내부망과 연동이 필요한 경우에는 망간 자료전송제품 설치 등 보안대책을 수립하여야 한다.

③ 청장은 사물인터넷 서비스를 위한 소프트웨어를 개발할 경우 제26조(소프트웨어 개발보안)를 준수하여야 한다.

④ 기타 사물인터넷 보안과 관련한 사항은 국가정보원장이 배포한 「국가·공공기관 사물인터넷(IoT) 보안가이드라인」을 준수하여야 한다.

제55조(원격근무 보안) ① 청장은 소속 공무원등의 재택·파견·이동근무 등 원격근무를 지원하기 위한 정보시스템을 구축·운용하고자 할 경우 관리적·물리적·기술적 보안대책을 수립·시행하여야 한다.

② 청장은 제1항에 따른 원격근무를 지원하기 위하여 원격근무 가능 업무 및 공개·비공개 업무 선정기준을 수립하여야 하고 비밀·대외비를 취급하는 업무는 원격근무 대상에서 제외하여야 한다. 다만, 불가피한 경우에는 보안대책 수립 후 국가정보원장과 사전 협의하여야 한다.

③ 청장은 원격근무자로부터 원격근무 보안서약서[서식 제8호]를 징구하고 원격근무자의 보직변경·퇴직 등 변동사항이 발생할 경우 정보시스템의 접근권한 조정 등 관련절차를 수립·시행하여야 한다.

④ 원격근무자는 사이버공격으로 인한 업무자료 유출을 방지하기 위하여 원격

근무용 단말기에 보안소프트웨어 등을 설치·운영하고 단말기 수시 점검 및 업무자료 저장금지 등 보안조치를 실시하여야 한다.

⑤ 원격근무자는 원격근무용 단말기 고장 등으로 단말기를 정비 또는 반납하고자 할 경우 자료유출 방지 등 보안대책 수립 후 정보보안담당관과 협의하여 관련조치를 취하여야 한다.

⑥ 청장은 비공개 업무와 관련한 원격근무의 경우에는 국가정보원장이 안전성을 확인한 상용 암호모듈을 사용하여 소통자료를 암호화하고 행정전자서명체계를 이용하여 인증하며 일회용 비밀번호·생체인증 등 보안기술을 적용하여야 한다.

⑦ 청장은 원격근무와 관련한 보안대책 이행여부를 정기적으로 점검·보완하여야 한다.

제56조(국제회의 보안) ① 청장은 국제협상 등 중요 국제회의를 위하여 PC·노트북 등 정보시스템을 국외 현지에서 설치·운용하고자 할 경우 관련 정보·자료가 유출되지 아니하도록 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 설치장소에 대한 물리적 접근통제
2. 정보시스템 접근 통제 및 분실 방지 등 보안관리
3. 정보시스템 저장자료 암호화 등 자료 접근통제
4. 전화기·팩스 등 통신장비에 대한 도청방지

② 국제회의 참가자는 회의 상대방이 제공한 PC·노트북·휴대용 저장매체 등 정보시스템을 사용하여서는 아니 된다.

제57조(저장매체 불용처리) ① 청장은 정보시스템 또는 저장매체(하드디스크·반도체 기반 저장장치(SSD) 등)를 외부수리·교체·반납·양여·폐기·불용 처리하고자 할 경우 정보시스템 및 저장매체에 저장된 자료가 외부에 유출되지 않도록 자료 삭제 등 보안조치를 실시하여야 한다. 이 경우 정보시스템 관리자 및 개별사용자는 분임정보보안담당관과 협의하여야 한다.

② 제1항에 따라 자료를 삭제할 경우 해당 기관의 실정에 맞게 저장매체별·자료별 차별화된 삭제 방법을 적용할 수 있다.

③ 비밀·대외비를 저장하거나 암호화 키를 저장한 저장매체는 소각·파쇄·용해 등의 방법으로 완전 파괴하여야 한다.

④ 기타 정보시스템 및 저장매체의 불용처리와 관련한 사항은 국가정보원장이 배포한 「정보시스템 저장매체 불용처리지침」을 준수하여야 한다.

제3절 자료 보안

제58조(비밀의 전자적 처리) ① 청장은 「보안업무규정」에 따라 비밀의 생산, 분류, 보관, 열람, 출력, 송·수신, 이관, 파기 등을 전자적으로 처리할 수 있다.

② 청장은 비밀을 전자적으로 처리하는 전(全) 과정에서 기밀성, 무결성, 인증, 부인방지 등 보안성을 확보하여야 하며 이를 위하여 국가정보원장이 개발하거나 안전성을 확인한 암호자재를 사용하여야 한다.

③ 제1항에 따라 비밀을 전자적으로 처리할 경우 내부망과 기관 인터넷망이 물리적으로 분리된 기관은 내부망 PC에서 비밀을 전자적으로 처리할 수 있으며 그 밖의 기관은 내부망 및 기관 인터넷망과도 분리된 별도의 비밀 작업용 PC에서 처리하여야 한다.

④ 종이문서로 출력된 비밀의 관리에 관하여는 「보안업무규정」을 준수하여야 한다.

제59조(비밀관리시스템 운용) ① 청장은 비밀을 전자적으로 안전하게 처리하기 위하여 국가정보원장이 개발·보급한 비밀관리시스템을 도입·운용할 수 있다.

② 비밀관리시스템을 구축한 기관의 장은 비밀의 생산·보관·유통 등 전반에 대하여 비밀관리시스템을 활용하여 비밀을 안전하게 관리하여야 한다.

③ 청장은 비밀관리시스템을 자체적으로 개발·운용하고자 할 경우 제60에 따른 비밀의 전자적 처리 규격을 준수하여 개발하여야 한다.

제60조(비밀의 전자적 처리 규격) 청장은 비밀관리시스템의 개발에 필요한 다음 각 호의 사항을 포함한 비밀의 전자적 처리 규격은 국가정보원장이 정한 것을 따른다.

1. 비밀의 생산, 분류, 보관, 열람, 출력, 송·수신, 이관, 파기 등 전(全) 과정에서 요구되는 보안기능
2. 비밀의 관리를 위한 기능
3. 비밀을 표시하기 위한 양식 및 외형 정의

4. 비밀을 전자적으로 처리하면서 발생하는 각종 로그 기록·관리 기능
5. 비밀을 관리하기 위한 각종 대장 및 카드 정의
6. 개별사용자 및 시스템 관리 기능
7. 그 밖에 비밀을 전자적으로 처리하는데 필요한 보안·관리 기능

제61조(대외비의 전자적 처리) ① 청장은 대외비를 전자적으로 처리 하고자 할 경우 보호기간이 만료되지 않은 대외비는 국가정보원장이 안전성을 확인한 상용 암호모듈을 사용하여 위조·변조·훼손 및 유출 등을 방지하기 위한 보안대책을 강구하여야 하며, 보호기간이 만료된 대외비는 제62조에 따른 비공개 업무자료의 처리 기준을 준용하여야 한다.

② 청장은 업무와 관계되지 아니한 사람이 대외비를 열람, 복제·복사, 배부할 수 없도록 보안대책을 수립·시행하여야 한다.

제62조(비공개 업무자료 처리) ① 공무원등은 비공개 업무자료를 다음 각 호의 어느 하나에 해당하는 방법으로만 처리하여야 한다.

1. 소속 또는 근무중인 기관의 내부망 PC 및 서버에 작성 및 저장·보관
2. 소속 또는 근무중인 기관의 장이 지급한 휴대용 저장매체에 작성 및 저장·보관
3. 소속 또는 근무중인 기관의 장이 자체적으로 구축·운용하는 전자우편시스템(이하 “기관 전자우편”이라 한다), 공무원등이 공동으로 사용할 목적으로 문화체육관광부장관이 구축·운용하는 전자우편시스템(이하 “공직자통합메일”이라 한다) 및 공무원등이 다른 공무원등과 자료를 공유하거나 소통하기 위하여 사용하는 전용(專用) 소프트웨어(이하 “공공 전용(專用) 메신저”라 한다)를 이용한 수·발신
4. 그 밖에 다른 법규에 따라 허용되는 처리방법

② 공무원등은 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 경우 소속 또는 근무중인 기관의 장이 지급한 인터넷 PC 또는 출장용 노트북을 이용하여 비공개 업무자료를 처리할 수 있다.

1. 기관 전자우편, 공직자통합메일 또는 공공 전용(專用) 메신저의 발신 기능을 이용하여 제2조제12호나목의 문장 또는 문구 작성
2. 기관 전자우편, 공직자통합메일 또는 공공 전용(專用) 메신저로 수·발신하는 과정에서의 일시적 저장

3. 제37조제5항에 따른 기관 인터넷망 PC에 작성·저장

③ 공무원등은 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 경우 개인이 소유한 PC·휴대용 저장매체·휴대폰 등을 이용하여 비공개 업무자료를 처리할 수 있다.

1. 기관 전자우편, 공직자통합메일 또는 공공 전용(專用) 메신저의 발신 기능을 이용하여 제2조제12호다목의 문장 또는 문구 작성
 2. 기관 전자우편, 공직자통합메일 또는 공공 전용(專用) 메신저로 수·발신하는 과정에서의 일시적 저장
 3. 국가정보원장이 안전성을 확인한 원격근무시스템에 접속하여 작성
 4. 국민의 생명·신체, 국가안보 및 공공의 안전 등을 위하여 긴급히 작성, 저장, 수·발신이 필요하다고 소속 또는 근무중인 기관의 장이 인정하는 경우
- ④ 공무원등은 제3항제4호에 해당하는 경우를 제외하고는 「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」 제2조제1항제2호에 따른 정보통신서비스(전자우편·메신저 등을 포함한다) 또는 국외에서 제공하는 이와 유사한 서비스(이하 “상용 정보통신서비스”라 한다)를 이용하여 비공개 업무자료를 처리 하여서는 아니 된다.
- ⑤ 공무원등은 제2항부터 제4항까지에 따라 작성·저장한 비공개 업무자료는 활용 후 즉시 삭제하여야 한다.

제63조(행정전자서명 인증서 등 관리) ① 공무원등은 비공개 업무자료를 처리하기 위하여 「전자정부법」 제29조에 따른 행정전자서명의 인증서(이하 “행정전자서명 인증서”라 한다)를 인터넷 PC 또는 개인이 소유한 PC·휴대용 저장매체·휴대폰 등에 저장·보관할 수 있다.

② 공무원등은 행정전자서명 인증서 및 인증서의 비밀번호, 기관 전자우편 또는 공직자통합메일의 비밀번호 등을 상용 정보통신서비스를 이용하여 수·발신하거나 저장·보관하여서는 아니 된다.

제64조(비공개 업무자료 유출방지) ① 청장은 제62조에 따른 비공개 업무자료 처리 절차 준수여부를 관리·통제할 수 있는 보안체계를 구축·운영 하여야 한다.

② 청장은 소속 공무원등이 공공 전용(專用) 메신저 이용을 활성화 할 수 있도록 노력하여야 한다.

제65조(공개 업무자료 처리) 공무원등은 관계 법규에 위배되지 않는 범위 내에서 인터넷 PC나 개인이 소유한 PC·휴대용 저장매체·휴대폰, 상용 정보통신서비스 등을 이용하여 공개 업무자료를 처리할 수 있다.

제66조(홈페이지 등 게시자료 보안) ① 청장은 비공개 업무자료가 홈페이지 또는 외부 웹사이트(이하 “홈페이지 등”이라 한다.)에 무단 게시되지 않도록 게시자료의 범위, 자료의 게시방법 등을 규정한 자체 홈페이지 정보공개 보안지침을 수립·시행하여야 한다.

② 부서 분임정보보안담당관은 해당 부서에서 홈페이지 등에 업무자료를 게시하고자 할 경우 자료 내용을 사전 검토하여 비공개 업무자료가 게시되지 아니하도록 하여야 한다.

③ 부서 분임정보보안담당관은 소속 부서에서 운용하는 홈페이지에서 비공개 업무자료가 무단 게시되었는지 여부를 정기적으로 점검하여야 한다.

④ 청장은 홈페이지 등에 비공개 업무자료가 무단 게시된 사실을 알게 된 경우 즉시 삭제 또는 차단 등 보안조치를 취하여야 한다.

제67조(정보통신망 현황자료 관리) ① 청장은 정보통신망과 관련한 다음 각 호에 해당하는 자료를 「보안업무규정 시행규칙」 제17조에 의거 국가 정보원장이 배포한 비밀세부분류지침에 따라 비밀로 분류·관리하여야 한다.

1. 국방 연구개발 및 정보통신 관련자료
2. 암호자재 운용현황
3. 국가보안시설(보호장비를 포함한다)의 운영·관리에 필요한 정보통신망 구성 현황(IP주소 할당현황을 포함한다) 및 그에 대한 취약점 분석·평가 결과물(「정보통신기반 보호법」 제9조에 따른 취약점 분석·평가결과를 포함한다)
4. 그 밖에 제2항 각 호에 해당하는 자료 중에서 국가정보원장이 비밀로 분류할 것을 요청한 자료

② 청장은 제1항 각 호에 해당하는 자료를 제외한 다음 각 호에 해당하는 자료를 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따른 비공개 대상 정보로 지정·관리하여야 한다.

1. 정보통신망 구성현황(IP주소 할당현황을 포함한다)
2. 정보시스템 운용현황

3. 취약점 분석·평가 결과물(「정보통신기반 보호법」 제9조에 따른 취약점 분석·평가결과를 포함한다)
 4. 주요 정보화사업 추진현황
- ③ 청장은 제1항 및 제2항에도 불구하고 다른 기관과 협력하여 정보통신망 및 정보시스템 운용 또는 정보보안업무를 수행할 필요가 있는 경우 제1항 및 제2항 각 호에 해당하는 자료를 다른 기관의 장에게 제공할 수 있다.

제68조(빅데이터 보안) ① 청장은 빅데이터와 관련한 시스템을 구축·운용하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 데이터의 수집 출처 확인 및 데이터 오·남용 방지
2. 데이터 수집을 위한 정보통신망 보안체계 수립
3. 수집된 데이터의 저장 및 보호체계 수립
4. 중요 데이터 암호화
5. 사용자별(데이터 제공자·수집자·분석요청자 및 분석결과 제공자 등) 권한 부여 체계 수립
6. 데이터 파기절차 수립

② 그 밖에 빅데이터 보안과 관련한 사항은 행정안전부장관이 고시한「개인정보의 안전성 확보조치 기준」 및 국가정보원장이 배포한「국가·공공기관 빅데이터 보안 가이드라인」을 준수하여야 한다.

제4절 사용자 보안

제69조(개별사용자 보안) ① 청장은 소관 정보통신망 또는 정보시스템의 사용과 관련하여 다음 각 호의 사항을 포함한 개별사용자 보안에 관한 절차 및 방법을 마련하여야 한다.

1. 직위·임무별 정보통신망 접근권한 부여 심사
2. 비밀 등 중요자료 취급시 비밀취급 인가, 보안서약서 징구 등 보안조치
3. 보직변경, 퇴직 등 변동사항 발생시 정보시스템 접근권한 조정

② 개별사용자는 본인이 PC 등 정보시스템을 사용하거나 정보통신망에 접속하는 행위와 관련하여 스스로 보안책임을 진다.

제70조(단말기 보안) ① 개별사용자는 소속된 기관에서 지급받은 PC·노트북·휴대폰·스마트패드 등 단말기(이하 “단말기”라 한다) 사용과 관련한 일체의 보안관리 책임을 진다.

② 개별사용자는 단말기에 대하여 다음 각 호에 해당하는 보안대책을 준수하여야 한다.

1. CMOS·로그온·자료 암호화 비밀번호의 정기적 변경 사용
2. 단말기 작업을 10분 이상 중단시 비밀번호 등을 적용한 화면보호 조치
3. 최신 백신 소프트웨어 설치
4. 운영체제 및 응용프로그램에 대한 최신 보안패치 유지
5. 출처, 유통경로 및 제작자가 불분명한 응용프로그램의 사용 금지
6. 인터넷을 통해 자료(파일) 획득시 신뢰할 수 있는 인터넷사이트를 활용하고 자료(파일) 다운로드시 최신 백신 소프트웨어로 검사 후 활용
7. 인터넷 파일공유·메신저·대화방 프로그램 등 업무상 불필요한 프로그램의 설치 금지 및 공유 폴더 삭제
8. 웹 브라우저를 통해 서명되지 않은 액티브-X 등이 다운로드·실행되지 않도록 보안 설정
9. 내부망과 기관 인터넷망이 분리된 기관의 인터넷 PC에서는 특별한 사유가 없는 한 문서프로그램을 읽기 전용(專用)으로 운용
10. 그 밖에 국가정보원장이 안전성을 확인하여 배포한 프로그램의 운용 및 보안권고문 이행

③ 부서 분임정보보안담당관은 정보보안담당관 총괄 하에 개별사용자의 제2항 각 호에 해당하는 보안대책의 준수여부를 정기적으로 점검하고 개선 조치하여야 한다.

제71조(계정 관리) ① 청장은 개별사용자에게 소관 정보통신망 또는 공용(公用) 정보시스템의 접속에 필요한 사용자 계정(아이디)을 부여하고자 할 경우 다음 각 호에 해당하는 사항을 준수하여야 한다.

1. 개별사용자별 또는 그룹별 접근권한 부여
2. 외부인에게 계정을 부여하지 아니하되 업무상 불가피한 경우 기관의 장 책임 하에 보안조치 후 필요한 업무에 한하여 일정기간 동안 접속 허용
3. 특별한 사유가 없는 한 용역업체 인원에게 관리자 계정 부여 금지
4. 비밀번호 등 식별 및 인증 수단이 없는 사용자 계정은 사용 금지

- ② 정보시스템 관리자는 개별사용자가 시스템 접속(로그온)에 5회 이상 실패할 경우 접속이 중단되도록 시스템을 설정하고 비(非)인가자의 침입 여부를 점검하여야 한다.
- ③ 정보시스템 관리자는 개별사용자의 보직변경, 퇴직, 계약종료 등 변동사항이 발생할 경우 신속히 사용자 계정을 삭제하거나 부여된 접근권한을 회수하여야 한다.
- ④ 정보시스템 관리자는 사용자 계정 부여 및 관리의 적절성을 연2회 이상 점검하고 그 결과를 정보보안담당관에게 통보하여야 한다
- ⑤ 정보시스템 관리자는 제1항 및 제3항에 의한 접근권한 부여, 변경, 회수 또는 삭제 등에 대한 내역을 기록하고 3년 이상 보관하여야 한다.

제72조(비밀번호 관리) ① 개별사용자 및 정보시스템 관리자는 각종 비밀번호를 다음 각 호에 해당하는 사항을 반영하고 숫자·문자·특수문자 등을 혼합하여 안전하게 설정하고 정기적으로 변경·사용하여야 한다.

- 1. 사용자 계정(아이디)과 동일하지 않은 것
 - 2. 개인 신상 및 부서 명칭 등과 관계가 없는 것
 - 3. 일반 사전에 등록된 단어의 사용을 피할 것
 - 4. 동일한 단어 또는 숫자를 반복하여 사용하지 말 것
 - 5. 사용된 비밀번호는 재사용하지 말 것
 - 6. 동일한 비밀번호를 여러 사람이 공유하여 사용하지 말 것
 - 7. 응용프로그램 등을 이용한 자동 비밀번호 입력기능을 사용하지 말 것
- ② 정보시스템 관리자는 서버 등 정보시스템에 보관되는 비밀번호가 복호화 되지 아니하도록 일방향 암호화하여 저장하여야 한다.
- ③ 청장은 공용(公用) 정보시스템에서 개별사용자를 식별 또는 인증하기 위하여 비밀번호에 갈음하거나 병행하여 지문인식 등 생체인증 기술 및 일회용 비밀번호 생성기(OTP) 등을 안전성 확인 후 사용할 수 있다. 이 경우 생체인증 정보는 안전하게 보관하여야 한다.

제73조(전자우편 보안) ① 청장은 전자우편을 컴퓨터바이러스·트로이목마 등 악성코드로부터 보호하기 위하여 백신 소프트웨어 설치, 해킹메일 차단시스템 구축 등 보안대책을 수립·시행하여야 한다.

- ② 청장은 기관 전자우편을 구축·운용할 경우 다른 전자우편과 자료를 안전하

- 게 소통하기 위하여 전자우편시스템에 암호화 기술을 적용하여야 한다.
- ③ 청장은 기관 전자우편을 구축·운용할 경우 수신된 전자우편의 발신지 IP주소 및 국가명이 표시되고 해킹메일로 의심될 경우 해킹메일 원본을 전송하여 신고할 수 있는 기능을 갖추어야 한다.
- ④ 개별사용자는 수신된 전자우편에 포함된 첨부파일이 자동 실행되지 아니하도록 기능을 설정하고 첨부파일을 다운로드할 경우 최신 백신 소프트웨어로 악성코드 은닉여부를 검사하여야 한다.
- ⑤ 개별사용자는 출처가 불분명하거나 의심되는 제목의 전자우편은 열람하지 말고 해킹메일로 의심될 경우 즉시 정보보안담당관에게 신고하여야 한다. 정보보안담당관은 해킹메일로 판단될 경우 국가정보원장과 청장에게 통보하여야 한다.
- ⑥ 청장은 전자우편 발신자 조작 등을 통한 기관 사칭 전자우편의 유포를 차단하기 위하여 보안대책을 수립·시행하여야 한다.

제74조(휴대용 저장매체 보안) ① 청장은 휴대용 저장매체를 사용하여 업무자료를 보관하고자 할 경우 자료의 위·변조, 저장매체의 훼손·분실 등에 대비한 보안대책을 수립·시행하여야 한다.

- ② 청장은 휴대용 저장매체 관리시스템을 운용하고자 할 경우 국가보원장이 안전성을 확인한 제품을 도입하여야 한다.
- ③ 정보보안담당관은 개별사용자가 휴대용 저장매체를 PC·서버 등에 연결할 경우 자동 실행되지 아니하고 최신 백신 소프트웨어로 악성코드 감염여부를 자동 검사하는 등의 보안 정책을 수립·시행하도록 관리하여야 한다.
- ④ 정보보안담당관 또는 분임정보보안담당관은 휴대용 저장매체를 비밀용·일반용으로 구분·관리하고 수량 및 보관 상태를 정기적으로 점검하며 외부 반출·입을 통제하여야 한다.
- ⑤ 정보보안담당관 또는 분임정보보안담당관은 비밀이 저장된 휴대용 저장매체에 대하여 매체별로 비밀등급 및 관리번호를 부여하고 비밀관리기록부에 등재·관리하여야 한다. 이 경우 매체 전면에 비밀등급 및 관리번호가 표시되도록 하여야 한다.
- ⑥ 정보보안담당관 또는 분임정보보안담당관은 비밀용 휴대용 저장매체를 다른 등급의 비밀용 또는 일반용으로 변경 사용하고자 할 경우 저장자료가 복구 불가하도록 완전 삭제 소프트웨어 등을 이용하여 삭제하여야 한다. 다만, 완전삭

제가 불가할 경우 변경 사용하여서는 아니 된다.

⑦ 정보보안담당관은 휴대용 저장매체를 폐기·불용 처리하고자 할 경우 저장 자료가 복구 불가하도록 완전삭제 소프트웨어 등을 이용하여 삭제하여야 한다. 다만, 완전삭제가 불가할 경우 파쇄하여야 한다.

⑧ 부서분임정보보안담당관은 정보보안담당관 총괄 하에 소속 부서에 대하여 개별사용자의 휴대용 저장매체 무단 반출, 미(未)등록 휴대용 저장매체 사용여 부 등 보안관리 실태를 정기적으로 점검하여야 한다.

⑨ 그 밖에 휴대용 저장매체 보안과 관련한 사항은 「USB메모리 등 휴대용 저장매체 보안관리지침」(부록 2)를 준수하여야 한다.

제75조(비인가 기기 통제) ① 공무원등은 개인 소유의 정보통신기기(휴대폰 등 이동통신단말기)를 제외한다. 이하 본 조에서 같다)를 소속된 기관으로 무단 반 입·사용하여서는 아니 된다. 다만, 부득이한 경우 소속 부서의 분임정보보안담 당관을 거쳐 정보보안담당관의 승인을 받은 후 사용할 수 있다.

② 공무원등은 개인 소유의 이동통신단말기 또는 이동통신망 접속장치(USB형 등)를 소속된 기관의 내부망 및 기관 인터넷망(제40제1항제1호에 따른 무선랜 을 포함한다)에 연결하여서는 아니 되며, 내부망 및 기관 인터넷망 정보시스템 을 상용 인터넷망에 연결하는 수단으로 사용하여서는 아니 된다. 부서분임정보 보안담당관은 이에 대하여 수시로 점검하여야 한다.

③ 정보보안담당관은 개인 소유의 정보통신기기가 업무자료를 외부로 유출하는 데 악용될 수 있거나 소속된 기관의 정보통신망 운영에 위해(危害)가 된다고 판단될 경우 반출·입 통제 등 보안대책을 수립·시행하여야 한다.

제76조(위규자 처리) 청장은 위규사항이 확인된 위규자 등에 대하여 「국가공무원법」 제33조 제1항 제2호의2에 따른 징계 관련 예규 제12장과 「새만금개발청법」 제34조 제1항 제2호의2에 따른 처분기준을 참고하여 필요한 조치를 취해야 한다.

제4장 융합 보안

제1절 정보통신시설 및 기기 보호

제77조(정보통신시설 보호) ① 청장은 다음 각 호의 중요 정보통신시설 및 장소를 「보안업무규정」 제34조에 따른 보호구역으로 설정 관리하여야 한다.

1. 전산실
2. 보안관리가 필요하다고 인정되는 정보시스템 설치 장소

② 청장은 제1항에서 지정된 보호구역에 대한 보안대책을 강구할 경우 다음 각 호 사항을 참고하여야 한다.

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

제78조(영상정보처리기기 보안) ① 청장은 업무상 목적으로 불특정사람 또는 사물을 촬영한 영상을 유·무선 정보통신망으로 전송·저장·분석하는 CCTV·IP 카메라·이동형 영상촬영장비·중계서버·관제서버·관리용PC 등의 기기·장비(이하 “영상정보처리기기”이라 한다)를 설치·운용하고자 할 경우 운영자의 계정·비밀번호 설정 등 인증대책을 수립하고 특정 IP주소에서만 접속 허용 등 비(非)인가자 접근 통제대책을 수립·시행하여야 한다.

② 청장은 영상정보처리기기를 통합·운용하는 시설(이하 “영상관제상황실”이라 한다)을 운영하고자 할 경우 영상관제상황실을 「보안업무규정」 제32조에 따른 보호구역으로 지정·관리하고 출입통제 장치를 운용하여야 한다.

③ 영상정보처리기기 관리자는 영상정보처리기기를 인터넷과 분리·운용하여야 한다. 다만, 부득이하게 인터넷과 연결·사용하여야 할 경우 전송내용을 암호화하여야 한다.

④ 영상정보처리기기 관리자는 제1항부터 제3항까지와 관련한 보안대책의 적절성을 수시 점검·보완하여야 한다.

⑤ 기타 영상정보처리기기 보안과 관련한 사항은 국가정보원장이 배포한

「CCTV 시스템 보안관리방안」 및 「안전한 정보통신 환경 구현을 위한 네트워크 구축 가이드라인」을 준수하여야 한다.

제79조(RFID 보안) ① 청장은 RFID시스템(대상이 되는 사물 등에 RFID 태그를 부착하고 전파를 사용하여 해당 사물 등의 식별정보 및 주변 환경정보를 인식하여 각 사물 등의 정보를 수집·저장·가공 및 활용하는 시스템을 말한다)을 구축하여 중요정보를 소통하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. RFID시스템(태그 및 리더기를 포함한다) 분실·탈취 대비 및 백업 대책
 2. 태그정보 최소화 대책
 3. 장치 및 운용자 인증, 중요정보 암호화 대책
- ② RFID시스템 관리자는 제1항과 관련한 보안대책의 적절성을 수시 점검·보완하여야 한다.
- ③ 기타 RFID 보안과 관련한 사항은 국가정보원장이 배포한 「RFID 보안관리 실무매뉴얼」을 준수하여야 한다.

제80조(디지털복합기 보안) ① 청장은 디지털복합기(디지털복사기 등도 포함한다. 이하 “복합기”라 한다)를 설치·운용하고자 할 경우 복합기 내 저장매체가 있거나 장치가 가능한 경우 자료유출을 방지하기 위하여 자료 완전삭제 또는 디스크 암호화 기능이 탑재된 복합기를 도입하여야 한다.

- ② 복합기 관리자는 제1항에 따라 복합기를 설치·운용할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.
1. 암호화 저장 기능이 있는 경우 해당 기능 사용
 2. 정기적으로 저장된 작업 내용(출력·스캔 등) 완전 삭제
 3. 공유 저장소 사용 제한 및 접근 제어
 4. 고정 IP주소 설정 및 불필요한 서비스 제거
- ③ 복합기 관리자는 다음 각 호의 어느 하나에 해당하는 경우 복합기의 저장매체에 저장된 자료를 완전 삭제하여야 한다.
1. 복합기 사용연한이 경과하여 폐기·양여할 경우
 2. 복합기 무상 보증기간 중 저장매체 또는 복합기 전체를 교체할 경우
 3. 고장 수리를 위한 외부 반출 등의 사유로 해당 기관이 복합기의 저장매체를 통제 관리할 수 없는 장소로 이동할 경우

4. 그 밖에 저장자료의 삭제가 필요하다고 판단되는 경우

- ④ 복합기 관리자는 소모품 교체 등 복합기 유지보수를 할 경우 부서분임정보 보안담당관의 입회·감독 하에 실시하고 저장매체의 무단 교체 등을 예방하여야 한다.
- ⑤ 복합기 관리자는 복합기를 통해 내부망과 기관 인터넷망간 접점이 발생하지 않도록 보안대책을 수립·시행하여야 한다.
- ⑥ 정보보안담당관은 소속된 기관의 저장매체가 장착되어 있는 복합기 운용과 관련한 보안대책의 적절성을 수시 점검·보완하여야 한다.
- ⑦ 기타 복합기 보안과 관련한 사항은 국가정보원장이 배포한 「정보시스템 저장매체 불용처리지침」을 준수하여야 한다.

제81조(재난 방지대책) ① 청장은 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애 발생에 대비하여 정보시스템의 이중화, 백업관리 및 복구 등 종합적인 재난 방지대책을 수립·시행하여야 한다.

- ② 청장은 재난 방지대책을 정기적으로 시험·검토하고 업무 연속성에 대한 영향평가를 실시하여야 한다.
- ③ 청장은 정보통신망의 장애 발생에 대비하여 정보시스템 백업시설을 확보하고 정기적으로 백업을 실시하여야 한다.
- ④ 청장은 제3항에 따른 백업시설을 구축·운영하고자 할 경우 정보통신실·통합데이터센터와 물리적으로 일정거리 이상 떨어진 안전한 장소에 설치하여야 하며 전력공급원 이중화 등 정보시스템의 가용성을 최대화 할 수 있도록 하여야 한다.

제2절 전자파 보안

제82조(대도청 측정) ① 청장은 다음 각 호의 어느 하나에 해당하는 시설·장소에 대하여 각종 수단에 의한 도청으로부터 정보유출을 방지하기 위한 보안대책(TSCM)을 수립·시행하여야 한다.

1. 기관 청사(신축, 이전 또는 증축, 개축, 대규모 수선 등)
2. 기관장실, 회의실 등 중요업무 장소
3. 중요회의·회담·협상·행사 장소

4. 기타 대도청 측정이 필요하다고 판단되는 시설·장소·장비
- ② 청장은 제1항에 따른 시설·장소에 대하여 자체 또는 「통신비밀보호법」 제10조의3에 따른 불법감청설비탐지업자 활용 등을 통해 대도청 측정을 실시하여야 한다. 다만, 국가기관의 장이 관리하는 시설·장소에 대하여는 국가정보원장에게 대도청 측정을 요청할 수 있다.
- ③ 청장은 제2항에 따라 자체 또는 불법감청설비탐지업자 등을 활용하여 측정한 결과 취약요인이 발견된 경우 그 결과를 국가정보원장에게 통보하고 기술지원 및 추가 측정을 요청할 수 있다.
- ④ 청장은 제2항에 따라 측정을 실시한 결과 취약요인이 발견된 경우 개선대책을 수립·시행하여야 한다.
- ⑤ 청장은 대도청 측정 결과를 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따른 비공개 대상 정보로 지정·관리하여야 한다.
- ⑥ 기타 대도청 측정과 관련한 사항은 국가정보원장이 배포한 「도청 탐지·방어활동 가이드라인」을 준수하여야 한다.

제83조(무선통신망 보안) ① 청장은 무선통신망(제40조에 따른 무선랜(WiFi)을 제외한다. 이하 본 조에서 같다)을 구축·운영하거나 이동통신망을 이용하여 관련 시스템을 구축·운영하는 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 접경 지역의 경우 무선통신망의 유선화 추진 또는 전파 차단시설 정책 시행
2. 비밀 등 중요자료를 소통하고자 할 경우 국가정보원장이 개발하거나 안전성을 확인한 암호자재 사용
3. 무선국 현황 관리 및 정기적인 전파 감시·측정

② 제1항에 따른 기관의 장은 연간 전파측정 계획을 수립하여 연1회 전파측정을 실시하여야 한다.

③ 제1항에 따른 기관의 장은 국가정보원장에게 제2항에 따른 연간 전파측정 계획서를 매년 1.25까지 제출하고 전파측정 실시 후 20일 이내에 [서식 제5호]에 따른 전파측정 결과보고서를 제출하여야 한다.

제5장 훈련 및 평가

제1절 훈련 및 진단

제84조(사이버공격 대응훈련) ① 청장은 새만금개발청의 정보통신망을 대상으로 매년 정기 또는 수시로 사이버공격 대응훈련을 실시하여야 한다.

② 청장은 국가차원의 사이버위기 발생에 대비하여 새만금개발청의 정보통신망을 대상으로 사이버위기 대응 모의훈련을 실시할 수 있다. 이 경우, 청장은 특별한 사유가 없는 한 사전에 훈련 일정 등을 해당부서에 통보하여야 한다.

③ 청장은 제2항의 모의훈련 결과 시정이 필요하다고 판단하는 경우에는 해당 부서의 장에게 필요한 조치를 요청할 수 있다. 이 경우 해당 부서의 장은 특별한 사유가 없는 한 필요한 조치를 이행하여야 하며, 청장은 그 이행여부를 확인할 수 있다.

④ 제2항에 따른 대응훈련은 「비상대비자원 관리법」 제14조에 따른 비상대비훈련과 함께 실시할 수 있다.

제85조(정보통신망 보안진단) ① 청장은 새만금개발청의 정보통신망을 대상으로 취약점을 진단하는 제반활동(이하 “보안진단”이라 한다)을 매년 정기적으로 실시하거나 관련예산 확보 등을 위하여 노력하여야 한다.

② 청장은 정보통신망에 대한 보안취약점 점검 또는 종합진단이 필요하다고 판단하는 경우 국가정보원장에게 보안진단을 요청할 수 있다.

③ 청장은 제2항에 따라 보안진단을 실시한 결과 개선이 필요하다고 요청받은 경우 특별한 사유가 없는 한 개선 조치하여야 한다.

제2절 정보보안 관리실태 평가

제86조(자체 평가) ① 청장은 국가정보원장이 배포한 평가지표에 따라 자체 평가를 실시하여야 한다.

② 청장은 자체 평가의 적절성을 입증하기 위하여 필요하다고 판단하는 경우 평가지표별 증빙자료를 국가정보원장에게 제출할 수 있다.

제87조(평가결과) 청장은 국가정보원으로부터 통보받은 정보 보안 관리실태 평가 결과에 따른 미비점을 개선·보완하여 정보보안 수준을 제고하여야 한다.

제6장 사이버위협 탐지 및 대응

제1절 보안관제

제88조(보안관제센터 설치·운영) 청장은 「국가사이버 안전관리규정」 제10조의2제1항에 따라 부문보안관제센터 또는 단위보안관제센터를 설치·운영하여야 하며, 해당 보안관제센터를 국가보안관제체계와 연계 운영하여야 한다. 이 경우 연계 방법은 국가보안관제체계를 운영하는 국가정보원장과 사전 협의하여야 정한다.

제89조(초동 조치) 청장은 사이버공격으로 인한 피해 최소화 및 확산 방지를 위하여 다음 각 호의 사항을 포함한 조치를 취하여야 한다.

1. 사이버공격 경유지(사이버공격에 악용되거나 악용될 우려가 있는 웹사이트 주소, IP주소, 전자우편 주소를 말한다) 및 공격 IP주소 차단
2. 피해 시스템을 정보통신망으로부터 분리하거나 악성프로그램의 동작을 정지시키는 조치
3. 사고 조사를 위한 피해 시스템 및 로그 기록의 보존

제90조(조치결과 통보) 청장은 사이버공격에 관한 정보를 제공받은 경우 제공받은 날로부터 5일 이내에 대응조치결과를 해당 보안관제센터를 운영하는 기관의 장에게 통보하여야 한다.

제2절 사고 대응

제91조(사이버공격으로 인한 사고) ① 「국가사이버안전관리규정」 제13조제1항에 따라 사고조사를 실시할 경우 청장은 안보위해(危害) 공격을 제외한 사이버공격으로 인한 사고에 대하여 조사를 실시한다.

② 청장은 제1항에 따라 사이버공격으로 인한 사고의 원인 분석 및 재발 방지를 위하여 다음 각 호에 해당하는 사항을 조사하여야 한다. 사이버공격으로 인하여 「보안업무규정」 제38조 및 제45조에 따른 보안사고가 발생한 경우에도 같다.

1. 공격 주체 및 피해자를 식별하기 위한 IP주소 및 MAC주소, 전자우편 주소, 정보통신서비스 이용자 계정 정보, 피해자의 성명 및 연락처
2. 사이버공격에 사용된 악성프로그램 및 공격 과정에서 생성·변경 또는 복제된 디지털정보
3. 공격 주체가 절취한 디지털정보
4. 공격 주체의 행위가 기록된 내역 또는 로그기록

③ 청장은 제2항에 따른 자료 제출을 요청받은 경우 관계 법규에 저촉되지 않는 범위 내에서 해당 자료를 제출하여야 하며 조사 기관의 장은 제출 받은 자료를 사고원인 분석, 공격자 의도 파악, 피해영향 평가 등 사이버공격에 대한 예방 및 대응과 관련한 목적으로만 사용하여야 한다.

④ 청장은 사고 원인을 규명할 때까지 피해 시스템에 대한 증거를 보존하고 임의로 관련 자료를 삭제하거나 포맷하여서는 아니 된다.

⑤ 청장은 민간 클라우드컴퓨팅서비스의 공공 전용(專用) 클라우드에서 사고가 발생한 경우 조사 기관의 장과 합동으로 조사반을 구성하여 클라우드컴퓨팅서비스제공자에 대하여 계약의 범위 내에서 자료의 보존 및 제출 요구, 현장 조사 등 필요한 조치를 취하여야 한다.

제92조(정보통신보안 규정 위반 및 자료유출 사고) ① 청장은 국가정보원장으로부터 「보안업무규정 시행규칙」 [별표 2]에 따른 정보통신보안규정 위반사항에 대한 사실을 통보받은 경우 동규정 시행규칙 제66조제3항에 따라 즉시 필요한 조치를 취하고 위규자, 위규 내용 및 조치 결과를 국가정보원장에게 통보하여야 한다.

② 청장은 비밀·대외비 등 국가 기밀에 속하는 업무자료가 유출되거나 비공개 업무자료가 유출된 사고 중 대공·방첩·테러·국제범죄조직과 관련된 사안일 경우 즉시 국가정보원장에게 통보하여 합동 조사를 실시하여야 한다.

③ 공무원등의 과실로 인하여 개인 소유의 정보통신기기 및 이동통신단말기, 상용 정보통신서비스에서 제2항에 따른 유출사고가 발생한 경우 조사 기관의 장은 공무원등의 소속된 기관의 장을 통해 해당 공무원등에게 저장자료·이용 내역 등의 자료 제출을 요청할 수 있다.

- ④ 공무원등은 제3항에 따른 요청이 위법하다고 판단하는 경우 그 사유를 소명하고 자료 제출을 거부할 수 있다.
- ⑤ 청장은 제1항 및 제2항에 따른 조사를 통해 유출이 확인된 자료에 대하여 관계 기관의 장과 합동으로 국가안보 및 국익, 정부정책에 미치는 영향을 평가하여 필요한 조치를 취하여야 한다.

제93조(재발방지 조치) ① 청장은 제91조 및 제92조에 따른 조사 결과 관계기관의 재발방지를 위한 보안조치 사항이 있을 경우 해당 기관의 장에게 통보하여야 한다. ② 청장은 사고 조사 결과와 관계 법규에 따른 관련자 징계, 개선 대책 수립 · 시행 등 필요한 조치를 취하여야 한다.

제94조(특례) 본 장에서 국가사이버안전관리규정 제12조 및 제13조에 따라 규정된 사항을 적용함에 있어서는 국가사이버안전관리규정 제18조를 준수 한다.

제7장 정보 협력

제95조(정보협조 요청) 청장은 국가정보원장이 사이버공격에 관한 정보를 종합 · 분석하거나 관련 현황을 작성하기 위하여 자료 제출 및 관련 지원을 요청하는 경우 관계 법규에 저촉되지 않는 범위 내에서 해당 자료를 제출하거나 필요한 지원을 할 수 있다. 다만, 「형사소송법」, 「군사법원법」 또는 「통신비밀보호법」에 따른 절차는 해당 법률이 정하는 바에 따른다.

제96조(기관간 정보공유 협력) 청장은 사이버공격의 예방 및 신속한 대응을 위하여 다음 각 호에 해당하는 정보(이하 “사이버위협정보“라 한다)를 기관간 상호 공유하도록 노력하여야 한다.

1. 사이버공격의 방법 및 대응조치에 관한 정보
2. 사이버공격에 사용된 악성프로그램 및 이와 관련된 정보
3. 정보통신망, 정보통신기기, 정보보호시스템 및 소프트웨어의 보안취약점에 관한 정보
4. 그 밖에 사이버공격 예방 및 대응에 필요한 정보

제97조(정보공유시스템 이용) 청장은 사이버위협정보를 체계적이고 효율적으로 공유 · 활용하기 위하여 국가사이버위협 정보공유시스템(이하 “정보공유시스템“이라 한다) 이용을 요청할 수 있다. 이 경우 다음 각 호에 해당하는 사항을 준수하여야 한다.

1. 정보공유시스템 전용(專用) 통신망 구축 및 전용(專用) 단말기 운용
2. 정보공유시스템 접근 · 활용 및 관련 장비를 운영할 담당자 지정 · 운영
3. 담당자가 변경될 경우 국가정보원장에게 통보

제98조(정보공유시스템의 정보 관리) ① 청장은 정보공유시스템에 등록된 정보를 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따른 비공개 대상 정보 및 「국가정보자료규정」 제2조제1호에 따른 국가정보자료로서 취급 · 관리하여야 한다.

② 청장은 정보공유시스템에 정보를 등록하는 사이버위협정보의 보안성 · 민감성 등을 고려하여 열람권한 및 보안등급을 부여할 수 있다.

제8장 보 칙

제99조(준용) 이 규정에 명시되지 않은 사항은 다음 관련규정 및 지침에 따른다.

1. 「국가정보원법」
2. 「정보 및 보안업무 기획 · 조정 규정」
3. 「보안업무규정」 및 시행규칙
4. 「전자정부법」 및 같은 법 시행령
5. 「정보통신기반보호법」 및 같은 법 시행령
6. 「공공기록물 관리에 관한 법률」 및 같은 법 시행령
7. 「개인정보보호법」 및 같은 법 시행령
8. 「국가사이버안전관리규정」(대통령훈령)
9. 「국가위기관리기본지침」(대통령훈령, 대외비)
10. 「국가 정보보안기술 연구개발 지침」(대외비)
11. 「전자정부 암호이용기반시스템 운용 및 관리지침」
12. 「국가 사이버안전 매뉴얼」 및 「사이버분야 위기관리 표준매뉴얼」
13. 「국가 · 공공기관 암호사용 기준」(대외비)

14. 「비밀의 전자적 처리 규칙」
15. 「정보통신기기 암호기술 적용지침」
16. 「국가 정보보안 기본지침」
17. 새만금개발청 보안업무 시행세칙
18. 그 밖의 관계 법령

제100조(제검토기한) 청장은 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 예규에 대하여 2020년 1월 1일 기준으로 매3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부 칙

제1조(시행일) 이 훈령은 발령한 날부터 시행한다.

별 표

정보보호시스템 유형별 도입요건

제품 유형	도입 요건	비 고
침입차단시스템(FW) 침입방지시스템(IPS)(침입탐지 포함) 통합보안관리제품 웹응용프로그램 침입차단제품 서버 접근통제제품 DB 접근통제제품 네트워크 접근통제제품 인터넷전화 보안제품 무선침입방지시스템 무선랜 인증제품 가상화제품 네트워크 자료유출 방지제품 디지털복합기 스마트폰 보안관리제품	CC인증	EAL 2 이상 또는 관련 PP 준수
스마트카드		EAL 4 이상
가상사설망제품 소프트웨어기반 보안USB 호스트 자료유출 방지제품	CC인증 및 검증필 암호모듈	EAL 2 이상 또는 관련 PP 준수 검증필 암호모듈 반드시 적용
스팸메일차단시스템 패치관리시스템 망간 자료전송제품	CC인증 또는 국가용 보안요구사항 준수 GS인증	· CC인증시 : EAL 2 이상 또는 관련 PP 준수 · GS인증시 : ISO 25023 및 국가용 보안요구사항을 준수
DDoS 대응장비 안티바이러스제품 소스코드 보안약점 분석도구	CC인증 또는 국가용 보안요구사항 준수 성능평가	· CC인증시 : EAL 2 이상 또는 관련 PP 준수 · 성능평가시 : 국가용 보안요구 사항을 준수
행정기관용 인터넷전화	TTA verified ver.4 이상	
기타 정보보호제품	-	CC인증 및 검증필 암호모듈 탑재 권고

* 최신 도입요건은 국가정보원 홈페이지(보안적합성 검증)를 참조

암호가 주기능인 제품 도입요건

제품 유형	도입 요건	비 고
메일 암호화제품	검증필 암호모듈 탑재	
구간 암호화제품		
하드웨어 보안토큰		
디스크·파일 암호화제품		
기타 암호화제품		
SSO제품	검증필 암호모듈 탑재 및 CC인증	· CC인증시 : 관련 PP 준수
DB 암호화제품		
문서 암호화제품(DRM 등)		

* 최신 도입요건은 국가정보원 홈페이지(상용 암호모듈 검증)를 참조

보안적합성 검증 신청서

서 식

신청기관	기관명			부서		
				담당자		
				담당자 전화번호		
	도입목적					
	사업명					
	보안성 검토			계약날짜		
				도입날짜		
유지보수	보안적합성 검증결과 반영여부(☐ 반영·개선 ☐ 반영불가)					
공인인증 대상확인	☐ CC인증 ☐ GS인증 대체가능 ☐ 성능평가 대체가능 ☐ 검증필 암호모듈 ☐ 해당사항 없음					
신청제품	업체명				대표자	
	주소				전화번호	
	제품명	* 신청제품이 2種 이상인 경우 신청서 추가 작성		제품 유형	방화벽, L3 스위치 등	
				펌웨어 (SW 버전)		
		도입 수량		해시값	* 네트워크 장비의 경우 기재	
	공인인증 현황	CC인증번호			인증등급 또는 준용 PP	EAL 등급 또는 준용 PP
		GS인증번호			준용 규격	
		성능평가 번호			준용 규격	
	업체 실무 담당자	전화번호				
		휴대폰번호				
		이메일				
암호모듈	☐ 없음 ☐ 있음 (☐ 검증 ☐ 미검증)		암호검증 번호	* 검증 암호모듈의 경우		

* 해시 프로그램 및 최신 양식은 국가정보원 홈페이지에서 다운받을 수 있습니다.

네트워크장비 변경내용 분석서

1. 제품 개요

가. 작성자 정보

도입기관	
개발업체	
작성일	
작성자	

나. 검증제품

제품명	
버전	
펌웨어 파일명 (해시값)	OOO.img (97BA3B7A1B325E4E8A517CDDB01AFFD32F93D27E2F2EAC750FEB)
검증일	

다. 이전 변경승인 내용

제품명	버전	변경승인 일자	변경승인 내용

2. 변경 내역

가. 변경 전 · 후 시스템 구성

제품명	소프트웨어		하드웨어	
	변경전	변경후	변경전	변경후

나. 변경된 보안기능 및 변경 내용

변경된 기능	변경 내용
로그인	관리자 로그인시 비밀번호를 수행하도록 제품 변경 * 필요시 화면 캡처

다. 변경이 제품 설계에 미치는 영향

항목	영향 분석	
펌웨어 변경 유무	로그인 기능 변경을 위해 관리자 인증과 관련된 일부코드가 변경됨에 따라 펌웨어가 변경됨	
	변경전	변경후
	test1.1.img	test1.2.img
	97BA3B7A1B325E4E8A517CDDDB01AFFD3	DCE24E537D2EB6E28E5BADBD1CEC0898
	* 필요시 화면 캡처	
사용자 인터페이스(UI) 변경 유무	로그인 기능 변경을 위해 내부 코드가 변경되었으며 제품의 사용자 인터페이스(UI) 변경은 없음	
	* 필요시 화면 캡처	

라. 변경부분에 대한 자체 시험결과

변경된 기능	시험 내용	시험 결과
로그인	관리자 로그인시 비밀번호 수행여부 확인	정상동작 확인 * 필요시 화면 캡처

[서식 제3호]

정보통신제품 도입현황

기관명		관계 중앙행정기관	
담당자		담당자 전화번호	
사업명			
보안성	보안성 검토받은 문서 제목 및 번호 표시 예) 000 보안성 검토결과(000-000, 2019.1.1)		

[illegible]

[서식 제4호]

정보시스템 관리대장

[illegible]

보안서약서

본인은 ____년 ____월 ____일부로 _____ 관련 용역사업(업무)을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 _____ 관련 업무 중 알게 될 일체의 내용이 직무상 기밀 사항임을 인정한다.
2. 본인은 이 기밀을 누설함이 국가안전보장 및 국가이익에 위해가 될 수 있음을 인식하여 업무수행 중 지득한 제반 기밀사항을 누설하거나 공개하지 아니한다. 단, 부패행위 신고 및 공익신고 등의 경우 비밀 준수 의무를 위반하지 않은 것으로 본다.
3. 본인이 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다. 단, 부패 행위 신고 및 공익신고 등의 경우 비밀 준수 의무를 위반하지 않은 것으로 본다.
4. 본인은 하도급업체를 통한 사업수행 시 하도급업체로 인해 발생하는 위반사항에 대하여 모든 책임을 부담한다.

____년 ____월 ____일

서 약 자 소 속 :
 직 위 :
 성 명 : (서명)
 생 년 월 일 :

서약집행자 소 속 :
(담당공무원) 직 위 :
 성 명 : (서명)
 생 년 월 일 :

원격근무 보안서약서

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

1. 나는 부여받은 인증 관련 정보 및 매체를 타인에게 유출하지 아니한다.
2. 나는 원격근무 중 작성·저장·열람·출력한 문서는 업무 목적에만 활용하고 타인에게 유출하지 아니한다.
3. 나는 원격근무용 소프트웨어 및 전산장비를 업무목적에만 활용하며 바이러스 백신 프로그램 및 기타 보안 프로그램을 설치하여 최신 상태로 유지한다.
4. 나는 여타 보안사항들을 성실히 준수하며 위반시 관련규정에 따라 처벌도 감수한다. 단, 부패행위 신고 및 공익신고 등의 경우 비밀 준수 의무를 위반하지 않은 것으로 본다.

____년 ____월 ____일

서 약 자 소 속 :
 직 위 :
 성 명 : (서명)
 생 년 월 일 :

서약집행자 소 속 :
(담당공무원) 직 위 :
 성 명 : (서명)
 생 년 월 일 :

정보보안점검 체크리스트

1. 정보보안 기본활동

연번	세부 점검사항	비고
1	기관 자체 실정에 맞는 정보보안업무 내규를 수립하고 있는가?	
2	매년 정보보안업무 활동계획을 수립·시행하는가?	
3	정보보안업무 전담 조직 및 직원(정보보안담당관)이 지정되어 있는가?	
4	소속 직원 근무성적 평가시 정보보안내규 준수여부를 반영하고 있는가?	
5	소속·산하기관 대상 정보보안 감사 또는 점검을 실시하는가?	
6	소속·산하기관 대상 정보보안 교육을 실시하고 있는가?	
7	사이버보안진단의 날을 내실 있게 수행하는가?	
8	정보보안 침해사고·규정위반 및 정보통신망 장애발생을 대비한 보고체계·조치 절차가 마련되어 있는가?	
9	보직변경 등 인사이동시 정보시스템 접근권한을 신속하게 조정하는가?	
10	서버·PC 등 정보시스템 현황을 제대로 파악하는가?	
11	정보통신장비(노트북 등) 반출입 통제 및 현황 관리를 철저히 하는가?	
12	업무자료를 상용 정보통신서비스로 전송하고 있지 않는가?	
13	정보통신망 구축 및 유지보수를 수행하는 외부인력(보안관제인력 포함)에 대해 보안서약서 징구, 보안교육 등 충분한 보안조치를 하고 있는가?	
14	용역업체 직원의 내부 정보시스템 접근을 통제하고 있는가?	
15	홈페이지 등 외부 게시자료에 대한 정보공개 지침을 수립·반영하는가?	
16	중요 정보화사업에 대하여 보안성 검토절차를 이행하는가?	
17	정보보호시스템(상용 암호모듈 포함) 도입시 보안적합성 검증절차를 준수하는가?	
18	비밀을 전자적으로 처리할 경우 암호자재로 암호화하는 등 규정을 준수하는가?	

부록

1. 정보보안점검 체크리스트
2. USB메모리 등 휴대용 저장매체 보안관리지침
3. 정보시스템 저장매체 불용처리지침
4. 정보자산 도입 및 폐기 절차

2. PC 및 서버 보안관리

연번	세부 점검사항	비고
1	PC · 서버에 설치된 운영체제 및 응용프로그램을 최신 보안업데이트 하였는가?	
2	PC · 서버의 불필요한 서비스를 검토하여 중단하고 정기적으로 인터넷에서 접속 가능여부를 확인하는가?	
3	백신이 자동 업데이트되고 실시간 감시기능이 설정되어 있는가?	
4	인터넷 PC에 업무관련 자료(비밀 포함)가 방치되어 있는가?	
5	P2P, 웹하드, 상용메신저 등 업무와 무관한 비인가 프로그램이 설치되어 있는가?	
6	비인가자 접근방지를 위해 CMOS · 로그인 등 PC 비밀번호를 설정하였는가?	
7	서버내 저장자료는 중요도에 따라 접근권한이 설정되어 있는가?	
8	정보통신망 구성측면에서 PC 및 서버 등의 위치가 적정한가?	
9	비인가 휴대용 저장매체(USB, 외장형 하드디스크, 메모리카드 등) 사용기록이 존재하는가?	
10	전자우편은 발신지 IP의 국가명이 표시되고 해킹메일은 신고가 용이한가?	
11	비밀은 비밀용 USB를 별도 지정하여 사용하고 일반자료와 혼합 저장하지 않는가?	
12	정보보호시스템 · 서버 · 네트워크장비 등 로그기록을 1년 이상 유지 · 관리하는가?	
13	비인가 USB · 정보통신기기 연결시 차단토록 보안 설정되어 있는가?	
14	PC · 노트북 등 저장매체가 있는 기기 고장시 저장된 자료의 완전 삭제를 확인 하고 외부에 수리를 의뢰하는가?	
15	「정보시스템 저장매체 불용처리지침」에 의거, 저장매체를 불용하였는가?	
16	모바일 업무는 행정업무와 현장업무를 구분하고 별도의 단말기를 운영하는가?	
17	불필요한 원격접속 S/W는 비활성화 또는 제거하였는가?	
18	상주 용역업체 네트워크와 직원용 네트워크를 분리하였는가?	
19	네트워크 접근제어를 위한 보안정책을 적절하게 설정하였는가?	
20	네트워크 접근제어 정책에 대한 생성일 · 목적 · 요청자 등 이력을 관리하는가?	
21	주요 정보보호시스템의 보안정책 설정파일을 주기적으로 백업하고 있는가?	

3. 네트워크 보안관리

연번	세부 점검사항	비고
1	정보시스템 세부 구성도(IP 포함)를 최신으로 유지하는가?	
2	업무자료를 소통하기 위한 내부망은 인터넷과 분리 운영하는가?	
3	인터넷 · 업무망간 자료공유 방안이 적절한가?	
4	업무자료를 소통하기 위한 내부망 구축시 사설주소체계(NAT)를 적용하는가?	
5	국가정보원장이 안정성을 검증한 정보보호시스템을 운용하고 있는가?	
6	인가받지 않은 단말기가 네트워크에 연결하지 못하도록 조치하고 있는가?	
7	네트워크를 통한 파일공유를 제한하고 필요시 보안대책을 세우고 있는가?	
8	장비 신규도입 등 전산망 구성 변동시 관련사항을 기록하는가?	
9	비인가 무선인터넷 · 무선랜 등 허가받지 않은 인터넷 접속경로가 존재하는가?	
10	첨단 정보통신기기(IoT 등)에 의한 내부 업무자료 유출 가능성이 존재하는가?	
11	시스템 최초 설치시 등록된 초기 계정 · 패스워드를 변경하였는가?	
12	네트워크 장비 · 정보보호시스템 · 서버는 비인가자가 접속하지 못하도록 IP 통제 등 보안설정하고 불필요한 서비스포트를 제거하는가?	
13	네트워크 장비 · 정보보호시스템 · 서버 등의 관리자 네트워크를 인터넷 · 업무망과 별도로 분리하여 운용하고 있는가?	
14	무선네트워크 구축시 사전에 보안성 검토를 수행하고 보안대책을 준수하는가?	
15	정보시스템에 대한 보안취약점을 주기적으로 점검하는가?	
16	소프트웨어개발보안(시큐어코딩)을 적용하여 개발하였는가?	
17	원격지 개발시 개발장소를 점검하고 있는가?	
18	원격 유지보수를 금지하고 비인가 원격접속을 차단하는가?	
19	직원의 재택 · 파견 · 이동근무 등 원격근무시 보안관리 대책이 적절한가?	
20	음란 · 도박 등 유해사이트를 차단하고 사이트목록을 주기적으로 갱신하는가?	
21	해외에 위치한 사무소와 인원에 대해 보안대책을 지원하고 주기적으로 점검하는가?	
22	인터넷전화 제품은 TTA Verified Ver 4. 이상을 사용하는가?	
23	인터넷전화는 인터넷망에 설치된 경우 물리적으로 분리하고, 업무망에 설치된 경우 물리적 또는 논리적(VLAN)으로 분리하였는가?	
24	서버가 위치한 네트워크는 방화벽 등으로 사용자 네트워크와 분리하고 있는가?	

4. 정보통신시설 보안관리

연번	세부 점검사항	비고
1	인위적·자연적 원인에 의한 정보통신망 장애 대비 백업 등 재난방지 대책을 강구하였는가?	
2	통합전산센터, 정보통신실 등 중요 정보통신시설을 보호구역으로 관리하는가?	
3	사무실 책상서랍 등에 비밀문건이나 비인가 정보통신기기가 방치 여부를 주기적으로 확인하는가?	
4	외부인의 정보통신실 출입을 통제하고 기록을 유지하는가?	
5	무정전 전원공급장치 등 비상시 전력장애 대책을 강구하였는가?	
6	침입경보장치, CCTV 등 보안장비와 방화장비(하론소화기 등) 정상동작 여부를 정기적으로 점검하고 있는가?	
7	정보통신시설에 비상시 긴급 파기를 위한 장비(해머 등)를 비치하고 있는가?	
8	정보통신시설에 대한 접근권한을 업무목적에 따라 차등 적용하고 있는가?	
9	정보통신장비 수리·점검시 정보보안담당관 또는 분임정보보안담당관 입회하에 진행하는가?	
10	민간 클라우드 컴퓨팅서비스 사용시 보안인증을 받은 서비스를 이용하는가?	
11	계약서에 정보통신망 구성도, IP주소현황 등 누출금지정보를 명시하고 있는가?	
12	시각동기화를 통하여 정보시스템 시각을 정확히 유지하고 있는가?	
13	CCTV 등 단독망 형태의 시스템을 인터넷망과 혼용하지 않고 분리·운영하는가?	

5. 암호자재 및 암호알고리즘 관리

연번	세부 점검사항	비고
1	비밀을 소통·보호하기 위하여 국가정보원장이 개발하거나 안전성을 확인한 암호자재를 사용하는가?	
2	국가정보원장이 승인하지 아니한 암호자재 또는 외국에서 생산된 암호기능 탑재 시스템을 무단으로 사용하는가?	
3	암호자재를 취급하는 인원을 암호자재 취급자로 지정·관리하는가?	
4	암호자재 취급인가자 중 암호자재 배부 또는 반납하는 직원에 대해 인감등록을 실시하는가?	
5	각 암호자재에 대한 운용관리 정·부책임자 및 실무 담당자를 지정하였는가?	
6	암호자재 설치, 운영, 보관에 대한 보안대책이 수립되었으며 이행되고 있는가?	
7	암호자재를 복제·복사하거나 또는 국가정보원장이 승인 없이 암호자재를 해외 제공·반출한 사례는 없는가?	
8	암호자재 관련 문서를 비밀로 생산하여 관리하고 있는가?	
9	사용중인 암호자재의 사용목적 및 보호대상 변경 시, 국가정보원장에게 승인을 받았는가?	
10	노후 등으로 사용하지 않거나 또는 도입 후 6개월 이내에 설치하지 않는(미래용·예비용 암호자재 제외) 등 보관만 하고 있는 암호자재가 있는가?	
11	‘암호자재 관리기록부’, ‘암호자재 점검기록부’, ‘지편자재 사용기록부’ 등을 누락하지 않고 작성·유지하고 있는가?	
12	암호자재 책임자는 주1회 이상 암호자재를 점검하여 그 결과를 ‘암호자재 점검기록부’에 기록·유지하고, 보안담당관은 점검사항을 월 1회 확인하고 있는가?	
13	암호자재 배부·반납 등의 업무는 암호자재 취급자가 직접 수행하고, ‘암호자재 증명서’를 작성·보관하고 있는가?	
14	암호자재의 정·부 책임자 및 실무 담당자 교체시 인계인수를 실시하고 ‘암호자재 관리기록부’에 인계인수 사항을 기록하는가?	

6. 보안관제 등 해킹 대응활동

연번	세부 점검사항	비고
1	사이버공격에 대응하기 위해 자체 관제센터를 운영(직접 혹은 보안관제 전문업체 용역)하거나 다른 국가·공공기관에 위탁 하였는가?	
2	보안관제센터 운영을 총괄 관리하는 전담 공무원이 있는가?	
3	사이버공격 탐지·대응 및 자체 DDoS공격 대응매뉴얼 등이 구비되어 있는가?	
4	해킹사고 조사결과, 보안 위규자에 대한 처벌이 자체 규정·지침 등에 명시되어 있고 실제로 이루어지고 있는가?	
5	국가사이버안전센터·부문보안관제센터 등 유관기관과 보안관제시스템을 연계 운영하는가?	
6	자체 사이버위기 대응 모의훈련을 주기적으로 실시하는가?	
7	홈페이지 해킹, DDoS공격, 해킹메일 수신 등 침해사고 발생시 국가정보원·부문 보안관제센터 등 유관기관에 즉시 신고하는가?	
8	시스템 장애시 유지보수 업체 및 긴급연락체계가 최신화 되어 있는가?	
9	보안관제시스템에 대한 물리적·관리적·기술적인 보안대책을 준수하고 있는가?	
10	침해사고 발생시 사고조사내역을 작성하고 해당내용을 기관장에 보고하는가?	
11	전직원을 대상으로 해킹메일 대응방안 및 침해사고 대응절차 등 관련 교육을 수행하는가?	
12	보안취약점 발표시 산하기관 또는 담당직원과 즉시 공유하는가?	
13	국가사이버안전센터 등과 사이버위협정보, 탐지기술 등 정보를 공유하고 있는가?	
14	사이버공격 발생시 소속·산하기관에 전파할 수 있는 체계가 구비되었는가?	
15	국가사이버안전센터에서 제공한 탐지규칙정보에 대한 보안관리 및 전담관리자를 지정·운영하고 있는가?	
16	침해사고 발생시 해당 시스템을 무단 포맷할 경우 보안위규(사고조사 방해) 행위임을 시스템 관리자·사용자가 인지하고 있는가?	

[부록 2]

USB메모리 등 휴대용 저장매체 보안관리지침

제1조(목적) 이 지침은 「새만금개발청 정보보안 업무규정」 제60조제4항에 따라 USB (Universal Serial Bus)메모리 등 휴대용 저장매체 보안관리에 필요한 세부사항을 규정함을 목적으로 한다.

제2조(적용범위) 이 지침은 새만금개발청의 각 과 단위 부서에 적용한다.

제3조(정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

1. "휴대용 저장매체"라 함은 디스켓·CD·외장형 하드디스크·USB메모리 등 정보를 저장할 수 있는 것으로 PC·서버 등의 정보시스템과 분리할 수 있는 기억장치를 말한다.
2. "휴대용 저장매체 관리자"(이하 "관리자"라 한다)라 함은 각 팀 또는 과별 휴대용 저장매체 관리상의 책임을 맡은 부서의 장을 말한다.
3. "휴대용 저장매체 취급자"(이하 "취급자"라 한다)라 함은 해당 휴대용 저장매체를 사용하는 자를 말한다.
4. "휴대용 저장매체 관리시스템"(이하 "관리시스템"이라 한다)이라 함은 휴대용 저장매체의 등록, 파기, 재사용, 반출·입 및 불용처리 현황 등에 관하여 전자적으로 처리하는 시스템을 말한다.
5. "휴대용 저장매체 관리번호"(이하 "관리번호"라 한다)라 함은 사용 중인 휴대용 저장매체의 식별 및 관리를 용이하게 하기 위하여 부여한 번호를 말한다.

제4조(USB메모리 및 관리시스템 도입절차) ① 청장은 상용 암호모듈이 탑재된 휴대용 저장매체 및 휴대용 저장매체 관리시스템을 도입할 경우 그 제품의 안전성을 검증하기 위하여 「국가 정보보안 기본지침」 제2장 제4절에 따라 보안적합성 검증 절차를 이행하여야 한다.

② 보안적합성 검증기관의 장은 다음 각 호에 해당하는 필수 보안기능의 유무를

검토한 후 그 결과를 적합성 검증결과에 반영한다.

1. 사용자 식별·인증기능
2. 저장데이터 암호·복호화 기능
3. 저장된 자료의 임의 복제 방지기능
4. 분실시 저장데이터의 보호를 위한 삭제 기능

③ 제2항제2호의 저장데이터 암호·복호화 기능은 자료를 휴대용 저장매체에 보관하는 경우로 한한다.

④ 청장은 운용중인 휴대용 저장매체를 별지 제1호부터 별지 제6호까지의 서식으로 관리하여야 하며 전자적 관리시스템으로 갈음할 수 있다.

제5조(휴대용 저장매체 사용) ① 휴대용 저장매체를 등록한 후 사용하여야 한다.

② 휴대용 저장매체의 등록방법은 제4조제4항에 따른 서식 또는 전자적 관리시스템으로 등재하는 것을 말한다.

제6조(휴대용 저장매체 사용제한) ① 등록된 휴대용 저장매체만 사용할 수 있다.

② 각 부서의 장은 그 소속직원이 국제회의에 참가시 출장 전 회의 대상국에서 제공한 USB메모리 등 휴대용 저장매체를 사용하지 않도록 보안교육을 실시한다.

③ 각 부서의 장은 그 소속직원에게 공지·교육을 통하여 미등록 휴대용 저장매체 사용을 제한하여야 하고 이에 대해 주기적인 점검을 실시하여야 한다.

제7조(관리자) ① 관리자는 소관 부서에서 휴대용 저장매체를 사용할 경우, 제4조제4항에 따른 서식 또는 전자적 관리시스템에 등재하여야 하며, 서식일 경우 사본 1부를 정보보안담당관에게 제출하여야 한다.

② 관리자는 정기적으로 휴대용 저장매체의 수량 및 보관상태를 점검하고 별지 제3호 서식 또는 전자적 관리시스템으로 관리하여야 한다.

③ 관리자는 휴대용 저장매체의 반·출입을 통제하여야 하며 별지 제4호 서식 또는 전자적 관리시스템에 따라 기록하여야 한다. 다만, 청장이 보안강화를 위하여 중앙에서 휴대용 저장매체의 반·출입 통제가 필요하다고 판단하는 경우에는

정보보안담당관 또는 분임정보보안담당관에게 그 역할을 부여할 수 있다.

④ 관리자는 소속직원이 휴대용 저장매체를 무단 반출하거나 미등록 휴대용 저장매체를 사용하지 않도록 감독하여야 하며 이를 위반한 사실을 발견 또는 확인하는 즉시 정보보안담당관에게 통지하여야 한다.

제8조(정보보안담당관의 책무) ① 정보보안담당관은 소속기관 내에서 사용하는 휴대용 저장매체 등록현황을 파악하여야 한다.

② 정보보안담당관은 휴대용 저장매체가 무단 반·출입되거나 미등록 휴대용 저장매체에 업무자료를 보관하는지 여부 등을 주기적으로 점검하여야 하며, 관련 위규 사례를 인지한 경우에는 경위조사를 실시하여야 한다.

③ 정보보안담당관은 제2항에 따라 조사를 실시한 결과, 비밀 유출이 우려되거나 유출 징후가 있는 경우에는 지체 없이 국가정보원장에게 보안사고 조사를 의뢰하여야 한다.

제9조(휴대용 저장매체의 구분 및 관리요령) ① 휴대용 저장매체는 일반용, 비밀용으로 구분한다.

② 일반용 휴대용 저장매체(이하 "일반용"이라 한다)의 관리요령은 다음과 같다.

1. 일반자료는 일반용에 보관할 수 있다. 다만, 대외비 자료는 국가정보원장이 안전성을 확인한 상용 암호모듈을 사용한 일반용에 보관하여야 한다.
2. 일반용에는 업무관련 일반자료(공개 또는 비공개 자료)만 보관하여야 하며 별지 제1호 서식의 관리대장에 기록하여야 한다.
3. 일반용은 개인서랍, 캐비닛 등에 안전하게 보관하여야 한다.
4. 일반용에는 별지 제5호 서식과 같이 기입·표시하여야 한다.
5. 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)

③ 비밀용 휴대용 저장매체(이하 "비밀용"이라 한다) 관리요령은 다음과 같다.

1. 비밀용을 사용할 경우에는 별지 제2호 서식의 관리대장에 기록하여야 하며

비밀관리기록부에도 등재·관리하여야 한다.

2. 비밀용은 비밀자료와 동일하게 이중 캐비닛 또는 금고에 보관하여야 한다.

3. 비밀용에는 별지 제5호 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 휴대용 저장매체를 마련해야 하며, 하나의 휴대용 저장매체에 등급이 다른 비밀 또는 일반자료를 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 등)

④ 제3항과 관련된 비밀의 전자적 처리와 관련한 그 밖의 사항에 대해서는 「새만금개발청 정보보안 업무규정」 제60조(비밀의 전자적 처리 규격)·제61조(대외비의 전자적 처리)를 준용한다.

제10조(휴대용 저장매체 불용처리 및 재사용) ① 휴대용 저장매체를 불용처리시 그 사실을 관리대장에 기록하여야 한다.

② 휴대용 저장매체를 불용처리하거나 재사용하는 경우에는 별지 제6호 서식에 따라 분임정보보안담당관의 확인을 받아야 한다.

제11조(휴대용 저장매체의 분실, 소각시 대처방안) ① 취급자는 휴대용 저장매체의 분실 또는 소각 등의 사유가 발생한 즉시 관리자에게 그 사실을 보고하여야 한다.

② 관리자는 휴대용 저장매체의 분실 또는 소각사실을 보고받은 즉시 분임정보보안담당관을 경유하여 정보보안담당관에게 통지하여야 한다.

③ 정보보안담당관은 일반용의 분실 또는 소각 사실을 통지받거나 인지한 경우에는 자체 조사를 실시하고 재발방지 대책을 강구하여야 한다. 다만 「새만금개발청 정보보안 업무규정」 제92조제2항에 따른 사안일 경우에는 지체 없이 국가정보원장에게 그 사실을 통보하여야 한다.

제12조(휴대용 저장매체 외부수리 방안) ① 휴대용 저장매체의 고장, 자료의 훼손 또는 자료의 오인삭제, 포맷으로 자료의 복구가 필요한 경우 상용 소프트웨어 활용 및 민간업체에 의뢰할 수 있다.

② 제1항에 따라 민간업체에 의뢰하는 경우에는 분임정보보안담당관 입회, 보안서약서 징구 등 적절한 보안대책을 강구하여야 한다. 다만, 비밀자료가 포함된 경우에는 우선 정보보안담당관을 경유하여 국가정보원장에게 통보하여야 한다.

[부록2) 별지 제1호 서식]

휴대용 저장매체 관리대장(일반용)

< 관리자 : 4급 이○○ >

연번	관리번호 (S/N)	매체형태	등록일자	취급자	불용처리일자	불용처리방법 (재사용 용도)	비고
1	총무과-일반-01 (E-D900-04-3705B)	USB	10.10.20	5급 홍길○	11.10.20	물리적 파기	고장
2	총무과-일반-02 (NP00T512787I)	외장형 HDD	10.10.25	6급 김정○	11.10.27	포맷후 재사용 (시설과-일반-01)	
3	총무과-일반-03 (E-D900-04-3705B)	USB	10.11.1	5급 이수○	11.10.7	물리적 파기	고장
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

[부록2) 별지 제2호 서식]

휴대용 저장매체 관리대장(비밀용)

< 관리자 : 4급 김○○ >

연번	관리번호 (S/N)	등급	매체형태	등록일자	취급자	불용처리일자	불용처리방법 (재사용 용도)	비고 (사유)
1	총무과-Ⅱ급-01 (610-RURQ-61750)	Ⅱ급	USB	10.10.20	5급 홍길○	11.10.20	자성소거 후 재사용 (총무과-일반-09)	
2	총무과-Ⅲ급-01 (5101-53RB-12589)	Ⅲ급	CD	10.10.25	7급 정약○	11.10.21	물리적 파기	고장
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								

[부록2) 별지 제3호 서식]

휴대용 저장매체 점검대장

< 관리자 : 4급 김○○ >

[illegible]

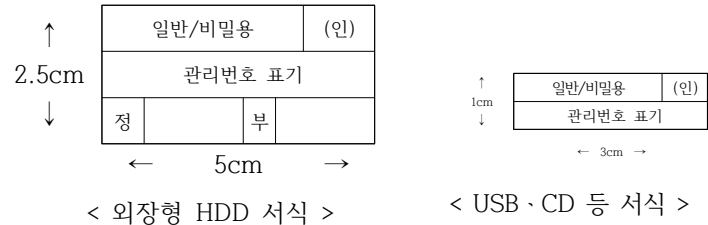
[부록2) 별지 제4호 서식]

휴대용 저장매체(전산장비 포함) 반출·입 대장

< 관리자 : 4급 김유○ >

[illegible]

휴대용 저장매체 라벨



- 가. 同 서식을 만들어 휴대용 저장매체 중앙의 적절한 위치에 부착
- 나. 첫 번째 줄에는 일반/비밀용(인)란에 분임정보보안담당관 또는 관리자의 직인을 날인
- 다. 두 번째 줄에는 휴대용 저장매체 관리번호 표기
- 라. 세 번째 줄의 '정'란에 관리자, '부'란에 취급자 표기(USB·CD의 경우 생략 가능)
- 마. 휴대용 저장매체의 크기를 고려하여 서식·글자 크기 조정 가능

< 별지 제5호 서식 예시 >

일반용		(인)	
총무과-일반-01			
정	이순○	부	홍길○

비밀용		(인)	
총무과-비밀-01			
정	이순○	부	홍길○

일반용		(인)	
총무과-일반-01			

Ⅱ 급비밀용		(인)	
총무과-Ⅱ급-01			

휴대용 저장매체 불용처리 확인서

아래와 같이 휴대용 저장매체(종 점) 불용처리 및 휴대용 저장매체 (종 점) 재사용에 대해 확인을 요청함

연번	관리번호 (S/N)	매체형태	사유	불용처리	재사용
1	총무과-일반-01 (E-D900-04-3705B)	USB	고장	물리적 파기	
2	총무과-Ⅲ급-01 (5101-53RA-12567)	CD	고장	물리적 파기	
3	총무과-Ⅱ급-01 (610-RURQ-61750)	USB	용도전환	자성소거	총무과-일반-09
4					
5					
6					
7					
8					
9					
10					

확인일자 : 년 월 일

요 청 자 : 소속·직책 O급 성명 : (인)

확 인 자 : 분임정보보안담당관 O급 성명 : (인)

정보시스템 저장매체 불용처리지침

제1조(목적) 이 지침은 「새만금개발청 정보보안 업무규정」 제57조제4항의 규정에 의하여 정보시스템 저장매체에 수록된 자료의 삭제방법과 세부 처리절차를 규정함을 목적으로 한다.

제2조(용어 정의) 이 지침에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. “저장매체”란 자기저장장치 · 광 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 보안조치 책임) 정보시스템을 폐기 · 양여 · 교체 · 반납(이하 “불용처리”라 한다)하거나 외부수리를 위하여 기관 외부로 반출할 경우 저장매체에 보관된 자료의 삭제 등 보안조치에 대한 책임을 진다.

제4조(정보시스템 불용처리시 자료 삭제) 정보시스템 저장매체에 저장된 자료를 삭제할 경우는 다음 각 호와 같다.

1. 정보시스템의 사용연한이 경과하여 폐기 또는 양여할 경우
2. 정보시스템 무상 보증기간 중 저장매체 또는 저장매체를 포함한 정보시스템을 교체할 경우
3. 정보시스템의 임대기간이 만료되어 반납할 경우
4. 고장 수리를 위한 외부 반출 등 새만금개발청이 정보시스템 저장매체를 보안 통제할 수 없는 환경으로 이동이 필요한 경우
5. 그 밖에 정보시스템 사용자 변경 등으로 저장자료 삭제가 필요하다고

판단되는 경우

제5조(저장매체 불용시 삭제방법) ① 분임정보보안담당관은 저장매체 불용 처리시 다음 분류에 따른 기준 이상으로 삭제한다.

저장 매체 \ 저장 자료	공개 자료	비공개 자료	대외비 자료	비밀 자료
자기테이프 플로피디스크	포맷	물리적 파괴	물리적 파괴	물리적 파괴
광디스크 (CD · DVD 등)	포맷	물리적 파괴	물리적 파괴	물리적 파괴
반도체메모리 (SSD · USB 등)	포맷 또는 삭제	물리적 파괴	물리적 파괴	물리적 파괴
하드디스크	포맷 또는 삭제	디가우징 또는 완전삭제 S/W	물리적 파괴	물리적 파괴

② 제1항에서 지정된 방법과 다른 방법으로 저장자료를 삭제하고자 할 때에는 사전에 국가정보원장과 협의하여야 한다.

제6조(저장자료 삭제 확인) ① 분임정보보안담당관은 정보시스템을 불용 처리할 경우 저장자료 삭제여부를 확인하여야 한다.

② 정보시스템에 저장된 자료의 삭제를 외부업체에 의뢰할 때에는 분임 정보보안담당관이 입회하여 삭제 절차 · 방법 준수여부 등을 확인 감독 하여야 한다.

제7조(정보시스템 도입시 보안조치) ① 정보화사업담당관은 정보시스템 도입시 고장수리 등을 위하여 공급업체가 저장매체를 교환 · 반출해 갈 경우에 대비, 저장자료 삭제방법 등 저장매체 보안조치 방안을 계약서상에 포함하여야 한다.

② 정보시스템을 임차 사용할 때에는 임차기간 만료 후 반납 시 해당 시스템의 저장자료 삭제방법 등 저장매체 보안조치 방안을 임차계약서 상에 포함하여야 한다.

제8조(정보시스템 외부반출시 보안조치) ① 불용처리 등을 위하여 정보시스템을 외부로 반출할 경우 사전 분임정보보안담당관의 통제를 받아야 하며 분임정보보안담당관은 그 현황을 기록 유지하여야 한다.

② 청장은 저장매체의 고장수리·자료복구 등을 위해 외부에 의뢰할 경우 저장매체에 보관된 자료의 유출 방지를 위하여 분임정보보안담당관 입회, 수리·복구 참여자에 대한 보안서약서 집행·교육 등 필요한 보안 조치를 하여야 한다.

③ 정보시스템관리자는 정보시스템을 불용 처리할 경우 해당 시스템의 사용기관·부서·사용자 등을 인식할 수 있는 표시를 모두 제거하여야 한다.

제9조(소자장비 등의 적합성 검증) 청장은 정보시스템의 저장자료를 삭제하는 장비나 소프트웨어를 도입할 경우 「국가 정보보안 기본지침」 제2장 제4절에 따른 보안적합성 검증절차를 이행하여야 한다.

[부록 4]

정보자산 도입 및 폐기 절차

제1조(목적) 새만금개발청 정보보안 업무처리 규정 제2장 정보화사업 보안 및 제4장 융합보안에 따른 정보자산획득·인가 및 폐기 절차를 정의하여, 운용 전 취약점 제거 및 폐기 전 자료완전삭제 등 보안조치를 통해 정보 누수를 방지하기 위한 절차를 규정함을 목적으로 한다.

제2조(대상) 새만금개발청에서 도입하는 복합기·서버·네트워크 장비·정보통신기기 등 모든 정보자산(단, 사무용PC는 제외)으로 하며, 정보자산 도입 및 폐기는 계획, 도입, 폐기단계별 절차에 따라 진행한다.

제3조(계획 단계) 정보화 사업을 추진하는 부서는 다음 각 호의 보안대책을 준수하여야 한다.

1. 정보화사업을 추진하는 부서는 정보화사업 추진계획을 수립할 경우 제11조제1항에 따라 보안대책을 수립·시행하여야 한다.
2. 정보화사업 발주를 위해 제안요청서를 작성할 경우 제12조(제안요청서 기재사항)의 사항을 포함하여야 한다.
3. 정보화사업을 수행하고자 할 경우 제13조(검토 시기 및 절차)에 따라 보안성 검토를 이행하여야 한다.
4. 제14조제1항에 따라 국가정보원에 보안성 검토를 의뢰할 경우 정보보안담당관에게 요청하여야 한다.
5. 제17조에 따라 정보화사업 공고 전 보안성 검토결과에 대한 보안대책을 보완하여야 한다.
6. 정보화사업을 추진하는 부서는 제30조제1항에 해당하는 제품을 도입하고자 할 경우 보안적합성 검증절차를 이행하여야 한다.

구분	정보자산 도입 정보화사업 유형
국정원 보안성 검토 대상 사업	※ 새만금개발청 정보보안 업무규정 제14조제1항 참고 가. 비밀·국가안보·국가위기·정부정책 관련 정보통신망 또는 정보시스템 구축 나. 100만 명 이상의 개인정보 처리 시스템 구축 다. 주요정보통신기반시설로 지정이 필요한 정보통신기반시설 구축 라. 여러 기관이 공동으로 활용하기 위한 정보통신망 또는 정보시스템 구축 마. 새만금개발청 정보보안 업무규정 제23조제1항에 따른 제어시스템 도입

[부록4) 별지 서식 제2호]

저장매체 파기 관리대장

관리자 : 정보보안담당관 김○○

분임정보보안담당관 박○○

[illegible]