

광명시 정보보안 규정

제정	2015. 8. 31	훈령	제357호
일부개정	2016. 5. 20	훈령	제370호
전부개정	2019. 9. 27	훈령	제408호(제명개정)
전부개정	2022. 7. 28	훈령	제429호
일부개정	2023. 7. 31	훈령	제436호

제1장 총칙

제1조(목적) 이 규정은 다음 각 호의 법령 및 지침에 따라 광명시 정보보안 기본업무를 규정함을 목적으로 한다.

1. 「국가정보원법」 제4조제1항제1호마목 및 같은 항 제4호 직무에 관련된 정보 및 보안업무의 기획·조정
2. 「사이버안보 업무규정」 제8조에 따른 사이버안보 기본대책의 수립·시행
3. 「정보 및 보안업무 기획·조정규정」 제4조제6호에 따라 수립하는 기본지침 중에서 정보보안에 관한 사항
4. 「보안업무규정」 제3조의2에 따라 수립하는 기본정책 중에서 정보보안에 관한 사항
5. 「전자정부법」 제56조제3항에 따른 「전자정부법 시행령」 제69조제3항 및 같은 영 제70조제3항에 따른 지침의 작성
6. 「정보통신기반보호법」 제6조제4항에 따른 공공분야 보호대책·보호계획 수립지침의 작성
7. 「공공기록물 관리에 관한 법률 시행령」 제5조에 따른 보안조치
8. 「국가사이버안전관리규정」 제9조제2항에 따른 지침의 작성
9. 「국가 정보보안 기본지침」 제4조에 따른 보안대책 수립·시행

제2조(정의) 이 규정에서 사용하는 용어의 뜻은 다음과 같다. <개정 2023. 7. 31>

1. “정보보안” 또는 “정보보호”라 함은 광명시(이하 “시”라 한다)의 기능 유지를 주 목적으로 정보통신망 및 정보시스템을 통해 수집, 가공, 저장, 검색, 송·수신되는 정보의 유출, 위·변조, 훼손 등을 방지하기 위하여 관리적·물

리적·기술적 수단을 강구하는 일체의 행위로서 다음 각 목에 따른 사항을 포함한다.

- 가. 「국가정보원법」 제4조제1항제4호에 따른 사이버공격 및 위협에 대한 예방 및 대응
 - 나. 「전자정부법」 제56조에 따른 정보통신망과 행정정보 등의 보안
 - 다. 「정보통신기반 보호법 시행령」 제5조제4항제1호 각 목에 해당하는 주요 정보통신기반시설의 보호
 - 라. 「공공기록물 관리에 관한 법률 시행령」 제5조에 따른 전자기록물의 보안
 - 마. 「국가사이버안전관리규정」 제2조제3호에 따른 사이버안전
2. “정보보안담당관”이라 함은 시의 정보보안 업무를 총괄하기 위하여 광명시장(이하 “시장”이라 한다)이 임명한 사람을 말한다.
 3. “분임정보보안담당관”이라 함은 시장이 부서 내 정보보안업무를 관장하기 위하여 임명한 사람을 말한다.
 4. “정보통신망”이라 함은 「사이버안보 업무규정」 제2조제1호에 따른 정보통신망을 말한다.
 5. “내부망”이라 함은 시장이 기관의 업무 수행을 위하여 인터넷과 별도로 분리하여 구축한 업무 전용(專用) 정보통신망을 말한다.
 6. “기관 인터넷망”이라 함은 시장이 소속 공무원 등의 업무 활용 또는 공개 서버 운용을 주(主) 목적으로 인터넷과 연동하여 구축한 정보통신망을 말한다.
 7. “상용 인터넷망”이라 함은 시장이 기관 인터넷망과 별개로 소속 공무원 등이나 민원인 등의 보편적인 편의성을 위하여 인터넷에 연동하여 구축한 정보통신망을 말한다.
 8. “정보시스템”이라 함은 「전자정부법」 제2조제13호에 따른 정보시스템을 말한다.
 9. “휴대용 저장매체”라 함은 CD·외장형 하드디스크·USB메모리 등 정보를 저장할 수 있는 것으로 PC·서버 등의 정보시스템과 분리할 수 있는 기억장치를 말한다.
 10. “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 공무원 등이 직무상 작성·취득하였거나 보유·관리하는 자료로서 전자적으로 처리되어 부호·문자·음성·음향·영상 등으로 표현된 것
11. “비밀”이라 함은 업무자료 중에서 「보안업무규정」 제4조에 따라 분류된 비밀을 말한다.
 12. “대외비”라 함은 업무자료 중에서 「보안업무규정 시행규칙」 제16조제3항에 따라 분류된 대외비를 말한다.
 13. “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. 「지방자치법」 제37조에 따른 지방의회 소속 공무원의 직무상 요구에 따라 작성 또는 취득한 자료
 - 다. 가목에 따른 비공개 대상 정보의 주요 내용이 기술된 문장 또는 문구
 14. “공개 업무자료”라 함은 업무자료 중에서 비밀 및 대외비와 비공개 업무자료를 제외한 모든 자료 또는 정보(「공공데이터의 제공 및 이용 활성화에 관한 법률」 제19조에 따라 공표된 공공데이터를 포함한다)를 말한다.
 15. “정보통신실”이라 함은 서버·스위치·라우터·교환기 등 전산 및 통신장비 등이 설치·운용되는 장소 또는 전산실·통신실·데이터센터 등을 말한다.
 16. “정보보호시스템”이라 함은 「지능정보화 기본법」 제2조제15호에 따른 정보보호시스템을 말한다.
 17. “국가용 보안요구사항”이라 함은 「사이버안보 업무규정」 제9조제2항에 따른 정보보호시스템 등의 도입·운영에 관한 보안대책의 일환으로 국가정보원장이 정하는 보안 관련 필수사항을 말한다.
 18. “국가용 보호프로파일(Protect Profile)”라 함은 「지능정보화 기본법」 제58조제1항 및 같은 법 시행령 제51조에 따라 과학기술정보통신부장관이 고

- 시한 「정보보호시스템 평가·인증 지침」에 따른 보호프로파일 중에서 국가정보원장이 국가용 보안요구사항을 만족한다고 인정한 것을 말한다.
19. “안전성 검증필 제품”이라 함은 국가정보원장이 국가용 보안요구사항 만족여부 등 안전성을 확인하여 「국가 정보보안 기본치침」 제21조에 따른 안전성 검증필 제품 목록에 등재한 정보통신제품을 말한다.
20. “보안적합성 검증”이라 함은 제20조제1항제3호의 보안기능이 있는 정보통신제품에 대하여 실제 적용·운용 이전에 시험 등의 방법으로 안전성을 검증하는 활동을 말한다.
21. “공무원 등”이라 함은 다음 각 목의 어느 하나에 해당하는 사람을 말한다.
- 가. 「지방공무원법」 제2조에 따른 지방공무원
 - 나. 「병역법」 제2조에 따른 상근예비역, 승선근무예비역, 사회복무요원, 공중보건지사, 공익법무관, 병역판정검사전담의사, 공중방역수의사 및 전문연구요원
 - 다. 공공기관 임직원
 - 라. 공무원 근로자 및 기간제 근로자
22. “개별사용자”라 함은 시장으로부터 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 공무원 등과 계약에 의하여 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 사람을 말한다.
23. “전자파 보안”이라 함은 정보통신시설 및 기기 등을 대상으로 전자파에 의한 정보유출을 방지하고 파괴·오작동 유발 등의 위협으로부터 정보를 보호하는 일체의 행위를 말한다.
24. “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.
25. “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.
26. “정보보안 관리실태 평가”라 함은 「사이버안보 업무규정」 제13조 및

- 「전자정부법」 제56조 등에 따라 국가정보보안 정책에 대한 이행 여부를 확인하기 위하여 실시하는 평가를 말한다.
27. “암호자재”라 함은 비밀의 보호 및 정보통신 보안을 위하여 사용되는 암호기술이 적용된 장치나 수단으로서 I급, II급 및 III급 비밀 소통용 암호자재로 구분되는 장치나 수단을 말한다.
 28. “암호장비”라 함은 암호자재 중에서 국가정보원장이 승인하여 개발·제작·보급되는 암호자재를 말한다.
 29. “암호알고리즘”이라 함은 정보의 유출, 위·변조, 훼손 등을 방지하기 위하여 기밀성·무결성·인증·부인방지 등의 기능을 제공하는 수학적 논리를 말한다.
 30. “암호가 주기능인 제품”이라 함은 검증필 암호모듈을 사용해 정보의 암호화를 주된 목적·기능으로 하는 제품을 말한다.
 31. “상용 암호모듈”이라 함은 암호알고리즘을 소프트웨어, 하드웨어, 펌웨어 또는 이를 조합한 형태로 구현한 것으로서 비밀이 아닌 업무자료를 보호하기 위하여 민간이 상용(商用)으로 판매하는 것을 말한다.
 32. “검증필 암호모듈”이라 함은 「사이버안보 업무규정」 제9조제2항 및 제3항, 「전자정부법 시행령」 제69조와 「암호모듈 시험 및 검증지침」(국가정보원 지침)에 따라 국가정보원장이 안전성을 확인하여 「국가 정보보안 기본지침」 제22조에 따른 목록에 등재한 상용 암호모듈을 말한다.
 33. “암호장비 제작업체”라 함은 암호장비 연구개발 결과물을 실용화하기 위하여 암호장비의 제작권을 획득한 업체를 말한다.
 34. “사이버공격”이라 함은 「사이버안보 업무규정」 제2조제2호에 따른 행위를 말한다.
 35. “안보위해(危害) 공격”이라 함은 사이버공격 중에서 다음 각 목의 어느 하나에 해당하는 행위 또는 활동을 말한다.
 - 가. 국제 및 국가배후 해킹조직의 활동 등 사이버안보 위협 행위
 - 나. 국가안보와 국익에 반하는 북한, 외국 및 외국인·외국단체·초국가행위자 또는 이와 연계된 내국인의 활동
 - 다. 「산업기술의 유출방지 및 보호에 관한 법률」 제2조에 따른 국가핵심기술 또는 국가연구개발사업으로 개발한 산업기술 또는 「방위산업기술 보

- 호법」 제2조제1호에 따른 방위산업기술을 부정한 방법으로 취득하는 행위
- 라. 「북한이탈주민의 보호 및 정착지원에 관한 법률 시행령」 제42조의2에 따른 보호대상자의 개인정보 유출 또는 신변을 위해(危害)할 우려가 있는 해킹
- 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 주요정보통신기반시설에 대한 같은 법 제12조에 따른 침해행위
36. “보안관제”라 함은 사이버공격을 실시간으로 즉시 탐지 및 분석, 대응하는 일련의 활동을 말한다.
37. “보안관제센터”라 함은 일정한 수준의 시설 및 장비와 이를 운영하기 위한 전문 또는 전담인력을 갖추고 보안관제업무를 수행하는 조직을 말한다.
38. “국가보안관제체계”라 함은 「사이버안보 업무규정」 제14조제1항에 따른 정부보안관제체계를 포함하여 국가정보원장이 각급기관의 장과 합동으로 보안관제를 실시하거나, 사이버공격 탐지·대응 조치 이행여부 확인을 위하여 구축·운영하는 실시간 탐지·대응체계를 말한다.
39. “부문보안관제센터”라 함은 「사이버안보 업무규정」 제14조제2항에 따라 설치·운영되는 보안관제센터 중에서 다음 각 목에 해당하는 기구를 말한

다.

가. 「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

나. 행정안전부장관이 지방자치단체의 정보통신망을 대상으로 운영하는 보안관제센터

다. 「전자정부법」 제54조제3항에 따라 행정안전부장관이 지정한 통합관리기관이 운영하는 보안관제센터

라. 한국인터넷진흥원이 운영하는 침해사고대응센터

40. “단위보안관제센터”라 함은 「사이버안보 업무규정」 제14조제2항에 따라 설치·운영되는 보안관제센터 중에서 경기도지사(이하 “도지사”라 한다), 시장이 해당 기관의 정보통신망을 대상으로 운영하는 보안관제센터를 말한다.

41. “취약점”이라 함은 사이버공격에 악용되어 관리자가 설정한 접근 권한외 정보를 열람·취득하게 하거나 보안기능을 회피 가능하게 하는 정보통신망·정보시스템의 결함을 말한다.

42. “클라우드컴퓨팅(Cloud Computing)”이란 직접·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원을 이용자의 요구나 수요변화에 따른 정보통신망을 통하여 신축적으로 이용할 수 있도록 하는 정보처리체계를 말한다.

43. 공공클라우드센터란 외교·안보, 수사·재판, 행정업무 처리 등 정보시스템을 통합관리하기 위해 각급기관 등의 장이 설치·운영중인 데이터센터를 말한다.

제3조(적용범위) 이 규정은 시 본청, 직속기관, 사업소 및 하부 행정기관, 의회사무국에 적용한다.

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

② 시장은 소속 공무원 등에 대한 근무성적 또는 성과평가를 실시할 경우 「정보보안 내규」 준수여부 등을 반영할 수 있다.

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

② 시장은 다음 각 호에 해당하는 업무를 전담할 정보보안담당관을 임명하여야 한다. 이 경우 「정보통신기반 보호법 시행령」 제9조제1항에 따른 정보보호 책임자, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3에 따른 정보보호 최고책임자, 「개인정보 보호법」 제31조제1항에 따른 개인정보 보호 책임자(같은 법 제29조에 따른 안전성 확보 조치를 수행하는 경우를 말한다)를 정보보안담당관으로 겸임시킬 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 및 ‘사이버보안진단의 날’ 운영
9. 시의 정보보안 감사
10. 시의 정보보안업무 감독
11. 부서 분임정보보안담당관 업무 감독
12. 그 밖에 정보보안과 관련한 사항

③ 시장은 정보보안담당관이 직무를 원활히 수행할 수 있도록 조직, 인력(정보화업무 담당인력 대비 10% 이상) 및 예산(정보화 예산 대비 15% 이상)을 운영할 수 있도록 노력하여야 한다.

④ 시장은 정보보안담당관이 직무를 효율적으로 수행할 수 있도록 각 부서의 장을 부서 정보보안업무를 수행할 분임정보보안담당관으로 임명하여야 한다. 별도로 임명하지 아니할 경우 부서의 장을 분임정보보안담당관으로 임명한 것으로 본다.

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

제6조(분임정보보안담당관 임무) ① 분임정보보안담당관은 부서 소관 정보보안 업무를 관장하며 임무는 다음 각 호와 같다.

1. 부서 소관 정보보안 업무 전반에 관한 사항
2. 부서 소관 정보화사업에 관한 사항
3. '사이버 보안진단의 날' 내 PC지키미 이행 및 지도·관리에 관한 사항
4. 악성코드 유무 및 인터넷망 PC에 업무자료 무단 사용의 주기적 점검에 관한 사항
5. 업무용 PC, 휴대용 저장매체 등 정보자산 및 네트워크 현황 관리
6. 부서 내 무선네트워크(인터넷) 무단사용 금지에 관한 사항
7. 그 밖에 부서 내 정보보안에 관한 사항

② 분임정보보안담당관은 업무를 효율적으로 수행하기 위하여 부서정보보안담당자를 둔다. 부서정보보안담당자를 별도 지정하지 않을 경우 서무업무담당자가 부서정보보안담당자가 된다.

③ 부서정보보안담당자는 분임정보보안담당관의 업무를 보좌하여 소관부서의 정보보안업무를 수행한다.

제7조(연도 추진계획 수립) ① 정보보안담당관은 매년 시에 대한 「당해연도 정보보안업무 추진계획」(「국가사이버안전관리규정」 제9조에 따른 사이버안전대책을 포함한다.)을 수립·시행하여야 한다.

② 정보보안담당관은 도지사가 정보보안 안전성 확보 확인 등을 위해 정보보안업무 추진계획을 요청할 경우 이에 응해야 한다.

제8조(정보보안감사 등) ① 시장은 소속기관의 정보보안업무 및 활동을 조사·점검하기 위하여 연1회 이상 정보보안감사를 실시하여야 하며, 이를 위해 정보보안 인력을 감사·감찰부서에 배속시킬 수 있다.

② 시장은 제1항에 따른 정보보안감사를 실시할 경우 제92조제1항 각 호의 사항을 활용할 수 있다.

③ 시장은 정보보안감사를 효율적으로 수행하기 위하여 국가정보원장에게 감사의 방향 및 중점사항, 감사관 지원 등 협조를 요청할 수 있다.

④ 시장은 정보보안감사 이외 필요한 경우 소속기관에 대하여 정보보안 점검

방문을 실시할 수 있으며, 점검방식 등은 제2항부터 제3항까지를 준용한다.

⑤ 시장은 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) 제4조 제4호에 따른 근무여건 개선 및 사기제고

제9조(정보보안 교육) ① 정보보안담당관은 정보보안에 대한 경각심을 제고 하기 위하여 정보보안 교육계획을 수립하여 연1회 이상 모든 소속 공무원 등을 대상으로 교육을 실시하여야 한다.

② 제1항에 따라 모든 공무원 등은 특별한 사유가 없는 한 연1회 이상 정보보안교육을 이수하여야 한다.

③ 정보보안담당관은 정보보안교육을 실시할 경우 해당 기관의 실정에 맞는 교육자료를 작성 활용하여야 하며 필요한 경우 국가정보원장에게 자료 또는 강사 지원 등 협조를 요청할 수 있다.

④ 정보보안담당관은 정보보안 담당직원의 업무 전문성을 제고하고 소속 공무원 등의 정보보안 지식을 함양하기 위하여 전문기관의 교육 이수나 학술회의 참가 등을 장려하여야 한다.

제10조(사이버보안진단의날) ① 정보보안담당관은 매월 세 번째 수요일을 ‘사이버보안진단의 날’로 지정·운영한다. 다만, 부득이한 사유로 해당 일에 시행하지 못할 경우 같은 달 다른 날에 시행하여야 한다.

② 분임정보보안담당관은 ‘사이버보안진단의 날’에 부서에서 운영하는 정보통신시스템, 정보통신망, 업무용 단말기(PC), 정보기기 등에 대해 보안진단을 실시하여야 한다. 이 경우 진단항목은 다음 각 호와 같다.

1. 정보통신시스템의 운영체제 및 응용프로그램에 대한 최신 보안패치 실시
2. 최신 백신 프로그램을 이용한 악성코드 감염여부 확인
3. 정보시스템 및 업무용 단말기(PC) 저장된 고유식별번호(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호), 비밀번호 등의 검색 및 암호화

4. 보안진단 프로그램(내PC지키미 등)을 실행하여 보안취약점 발굴 및 조치
 5. 관리대장에 등록된 보안·일반 USB메모리의 실물 및 저장된 전자정보 점검
 6. 정보보안담당관이 지정하는 “월별 중점 점검사항” 등
- ③ 정보보안담당관은 특별한 사유 없이 제2항의 보안취약점 진단을 실시하지 않은 정보시스템에 대해서는 정보자원 보호를 위하여 인터넷 사용을 차단할 수 있으며 관리자에게 시정요구를 할 수 있다.

제2장 정보화사업 보안

제1절 사업계획

제11조(보안책임) ① 정보통신망 또는 정보시스템을 개발·구축·운영·유지 보수하는 사업(「지능정보화 기본법」 제11조제1항에 따른 지능정보화계획에 따른 사업을 포함한다. 이하 “정보화사업”이라 한다)을 담당하는 분임정보보안담당관은 해당 정보화사업에 대한 보안관리를 수행하여야 한다.

② 분임정보보안담당관은 정보화사업에 대한 보안관리 책임을 지고 관리·감독하여야 한다.

③ 정보보안담당관은 각종 정보화사업과 관련한 보안대책의 적절성을 평가하고 정보화사업 수행 전반에 대하여 보안대책의 이행여부를 점검하여 필요한 경우 분임정보보안담당관에게 시정을 요구할 수 있다.

제12조(보안대책 수립) 분임정보보안담당관은 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, 검증필 암호모듈 및 정보보호시스템 도입·운영계획

5. 긴급사태 대비 및 재난복구 계획
6. 용역업체 작업 장소에 대한 보안대책
7. 온라인 개발 또는 온라인 유지보수가 필요하다고 판단할 경우 제28조의2 또는 제51조에 따른 보안대책
8. 누출금지정보 보안관리 방안

제13조(제안요청서 기재사항) ① 분임정보보안담당관은 용역업체에 정보화사업을 발주하기 위하여 제안요청서를 작성할 경우 다음 각 호의 사항을 포함하여야 한다.

1. 용역업체 작업 장소에 대한 보안 요구사항
2. 온라인 개발 또는 온라인 유지보수가 필요하다고 판단할 경우 제28조의2 또는 제51조에 따른 보안 준수사항
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. 해당 기관의 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, 암호가 주 기능인 제품 및 정보보호시스템 도입·운영 현황
7. 정보보호시스템 및 네트워크장비 설정 정보
8. 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따라 비공개 대상 정보로 분류된 해당 기관의 내부문서
9. 「개인정보보호법」 제2조제1호에 따른 개인정보
10. 「보안업무규정」 제4조에 따른 비밀 및 「보안업무규정 시행규칙」 제16조제3항에 따른 대외비
11. 그 밖에 시장이 공개가 불가하다고 판단한 자료

제2절 보안성 검토

제14조(검토 시기 및 절차) ① 분임정보보안담당관은 정보화사업과 관련한 보안대책의 적절성을 평가받기 위하여 사업 계획단계(사업 공고 전)에서 보안성 검토 절차를 이행하여야 한다.

② 분임정보보안담당관은 제15조제1항 및 제2항에 따른 정보화사업에 대해 정보보안담당관에게 보안성 검토를 의뢰하여야 한다.

③ 정보보안담당관은 제15조제1항 각 호에 해당하는 정보화사업에 대하여 국가정보원장에게 보안성 검토를 의뢰하고자 할 경우 도지사를 거쳐 국정원장에게 의뢰하여야 한다.

④ 보안성 검토는 서면 검토를 원칙으로 하며 보안성 검토 시 정보보안담당관이 필요하다고 판단하는 경우 현장 확인을 병행할 수 있다.

제15조(검토 기관 및 대상) ① 정보보안담당관이 국가정보원장에게 보안성 검토를 의뢰할 대상사업은 다음 각 호와 같다. 다만, 국가정보원장이 사업의 규모·중요도 등을 고려하여 도지사에게 보안성 검토를 위임한 경우 그러하지 아니하다.

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 고유식별 정보를 처리하는 정보시스템 구축
5. 주요정보통신기반시설로 지정이 필요한 정보통신기반시설 구축
6. 제52조의2에 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. 제2조제6호에 따른 기관 인터넷망 등 소속 공무원 등이 업무상 목적으로 활용하도록 하기 위한 인터넷망(제42조제1항제1호에 따른 업무용 무선랜 형태를 포함한다) 및 이동통신망(HSDPA, WCDMA, LTE, 5G 등)의 구축
 15. 제58조제4항에 따른 원격근무시스템 구축
 16. 「전자정부법」 제54조의2 및 「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 정보보안담당관은 다음 각 호에 해당하는 정보화사업에 대해 도지사에게 보안성 검토를 의뢰하여야 한다.
1. 제1항 단서에 따라 국가정보원장이 도지사에게 보안성 검토를 위임한 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. 제2조제7호에 따른 상용 인터넷망(제42조제1항제2호 또는 제3호에 따른 무선랜 형태를 포함한다)의 구축
 6. 내부망에 구축하는 공무원 등의 인사·복지시스
 7. 주요정보통신기반시설 취약점 분석·평가, 정보보안컨설팅 등 용역사업
 8. 기존 분리된 내부망·기관 인터넷망간 자료전송시스템 구축 등 후속사업

9. 대규모 백업·재해복구센터 구축
 10. 제44조제1항에 따른 영상회의시스템을 내부망 또는 기관 인터넷망과 분리하여 구축하는 경우
 11. 제84조에 따른 영상정보처리기기를 같은 조 제3항 본문에 따라 인터넷과 분리하여 구축하는 경우
 12. 백업시스템 구축
 13. 대민(對民) 콜센터시스템 구축
 14. 기타 시장이 필요하다고 판단하는 정보통신망 또는 정보시스템 구축
- ③ 정보보안담당관은 도지사가 제2항제10호부터 제14호까지에 해당하는 정보화사업에 대한 보안성 검토를 시장에게 위임할 경우 정보보안내규에 따라 자체 보안성 검토를 실시한다.

제16조(검토 생략) ① 분임정보보안담당관은 다음 각 호에 해당하는 정보화사업에 대하여는 국가정보원장이 정하는 바에 따라 보안성 검토 절차의 이행을 생략할 수 있다. 이 경우 분임정보보안담당관은 관련 매뉴얼·가이드라인 등을 준수하는 등 자체 보안대책을 수립·시행하여야 한다.

1. 제15조제1항 및 제2항 각 호의 정보화사업에 해당하지 아니하는 단순 장비·물품 도입
2. 제15조에 따른 보안성 검토를 완료한 정보화사업에 대하여 정보통신망 구성을 변경하지 아니하는 범위 내에서 다음 각 목의 사항을 포함한 후속 운영·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
 - 다. 기존 운용하던 정보보호시스템을 동일한 보안기능을 보유한 다른 정보보호시스템으로 교체
3. 다년도에 걸쳐 계속되는 사업으로 사업 착수 당시 보안성 검토를 완료한 후 사업 내용의 변동 없이 계속 추진하는 운영·유지사업
4. PC·프린터 및 상용 소프트웨어 등 단순 제품 교체

② 분임정보보안담당관은 제1항제2호부터 제4호까지에 해당하는 정보화사업

을 수행할 경우 기존 보안성 검토결과에 따른 보안대책을 준수하여야 한다.

제17조(제출 문서) 분임정보보안담당관은 제14조제2항에 따라 보안성 검토를 의뢰할 경우 다음 각 호의 사항이 포함된 문서를 제출하여야 한다.

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

제18조(검토결과 조치) ① 분임정보보안담당관은 제15조에 따라 보안성 검토 결과를 통보받은 경우 검토결과를 반영하여 보안대책을 보완하여야 한다.

② 정보보안담당관은 제1항에 따른 보안성 검토결과 반영여부를 확인하기 위하여 현장 점검을 실시할 수 있다.

제19조(현황 제출) 정보보안담당관은 전년도에 실시한 정보화사업에 대한 보안성 검토 결과 현황을 다음 연도 1. 25.까지 도지사를 거쳐 국가정보원장에게 제출하여야 한다.

제3절 제품 도입

제20조(정보통신제품 도입) ① 분임정보보안담당관은 정보 및 정보통신망 등을 보호하기 위하여 보안기능이 있는 다음 각 호의 정보통신제품을 도입할 수 있다.

1. 「국가 정보보안 기본방침」 제21조에 따른 안전성 검증필 제품 목록에 등재되어 있는 제품
2. 비밀이 아닌 업무자료의 암호·복호화를 목적으로 한 경우 별표 1 암호가 주기능인 제품 도입요건을 만족하는 제품
3. 제1호 및 제2호에 해당하지 않는 정보통신제품 중에서 국가정보원장이 별도로 공지하는 도입요건을 만족하는 제품
4. 제품유형의 특성상 보안기능의 비중이 미미하여, 분임정보보안담당관이 자유롭게 도입·운용이 가능한 ‘단순 보안기능 제품유형’으로 국가정보원장이 공지한 제품

5. 제93조에 따라 취약 정보통신제품을 긴급 대체하기 위하여 도입하는 제품
② 제1항제3호에 해당하는 제품은 실제 적용·운용 이전에 제2장제5절에 따른 보안적합성 검증을 받아야 한다.

③ 제1항제5호에 해당하는 긴급 대체 제품을 도입한 분임정보보안담당관은 빠른 시일내에 원(原) 제품과 동일 수준의 안전성 확인이 이루어질 수 있도록, 대체 제품에 대하여 제1항제1호 및 제2호에 따른 도입요건을 갖추도록 하거나 제3호 및 제2장제5절에 따른 보안적합성 검증 절차를 거치도록 하여야 하며, 필요시 국가정보원장에게 추가적인 검증을 요청할 수 있다.

제21조(검증필 암호모듈 도입) 분임정보보안담당관은 상용 암호모듈을 도입하여 정보시스템 등에 적용하고자 할 경우 「국가 정보보안 기본지침」 제22조에 따른 국가정보원장이 안전성을 확인한 검증필 암호모듈 목록에 올라 있는 상용 암호모듈을 도입하여야 한다.

제22조(영상정보처리기기 도입) 분임정보보안담당관은 제84조제1항에 따른 영상정보처리기기를 도입하고자 할 경우 한국정보통신기술협회(TTA)의 공공기관용 보안 성능품질 인증 등 일정한 보안성능이 확인된 제품을 도입하여야 한다. <개정 2023. 7. 31>

제23조(도입현황 제출) 정보보안담당관은 분임정보보안담당관이 분기 내 도입한 제20조에 따른 정보통신제품에 대하여 별지 제2호서식에 따른 정보통신제품 도입 확인서(현황)와 국가정보원장이 「국가 정보보안 기본지침」 제146조제2항의 방식으로 배포하는 제품유형별 운용점검사항을 매 분기 말에 도지사에게 제출하여야 한다.

제23조의2(상용소프트웨어 도입) 분임정보보안담당관은 「상용소프트웨어 제3자단가계약 추가특수조건」(조달청 지침) 제2조제2호에 따른 제3자단가계약으로 상용소프트웨어를 도입하고자 할 경우, 같은 지침 제10조제4항에 따른 판매중지 여부에 유의하여야 한다.

제4절 계약 및 사업수행

제24조(계약 특수조건) ① 분임정보보안담당관은 「지방자치단체를 당사자로

하는 계약에 관한 법률 시행령」 제92조제2항제3호나목 및 「전자정부법」 제2조제10호에 따른 정보화사업을 발주할 경우 계약 이행과정에서 다음 각 호의 행위를 금지하도록 계약서에 계약특수 조건으로 명시하여야 한다.

1. 정보통신망 또는 정보시스템에 허가 없이 접속하거나 무단으로 정보를 수집할 수 있는 비인가 프로그램을 설치하는 행위
2. 제1항에 따른 행위에 악용될 수 있는 정보통신망 또는 정보시스템의 취약점을 고의로 생성 또는 방치하는 행위
- ② 분임정보보안담당관은 계약기간(하자 보증기간을 포함한다) 내에 발생한 보안 취약점 등에 대해서는 계약업체로 하여금 개선 조치하도록 하여야 한다.
- ③ 분임정보보안담당관은 필요한 경우 계약업체로부터 제1항과 관련한 행위가 없다는 대표자 명의의 별지 제7호서식 확약서를 요구할 수 있다.

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

1. 제13조제1항 각 호에 따른 제안요청서에 포함된 사항
2. 제28조에 따른 원격지 개발, 제28조의2에 따른 원격지에서의 온라인 개발, 제51조에 따른 온라인 유지보수를 허용할 경우 보안 준수사항
3. 소프트웨어 개발보안에 필요한 사항
4. 사업 참여인원의 보안관련 준수사항과 위반할 경우 손해배상 책임에 관한 사항
5. 사업 수행과 관련한 보안교육, 보안점검 및 사업기간 중 참여인원 임의 교체 금지
6. 정보통신망 구성도·IP주소 현황 등 업체에 제공하는 자료는 자료 인계 인수대장을 비치하여 보안조치 후 인계·인수하고 무단 복사 및 외부반출 금지
7. 업체의 노트북·휴대용 저장매체 등 관련 장비는 반출·반입 시마다 악성코드 감염여부, 누출금지정보 무단 반출여부 등 점검
8. 사업 종료 시 업체의 노트북·휴대용 저장매체 등 관련 장비는 저장 자료 복구가 불가하도록 완전 삭제
9. 사업 종료 시 누출금지정보 전량 회수
10. 그 밖에 시장이 보안관리가 필요하다고 판단하는 사항 또는 국가정보원

장이 보안조치를 권고하는 사항

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

1. 「지방공무원법」 제31조제3호부터 제6의4호까지에 해당하는 사람
2. 「지방자치단체를 당사자로 하는 계약에 관한 법률」 제31조제1항 각 호의 행위를 한 사람

③ 분임정보보안담당관은 다음 각 호에 따른 보안 준수사항의 이행여부를 정기 또는 수시로 점검(불시 점검을 포함한다)하고 미비점을 발견한 경우 용역업체로 하여금 시정 조치하도록 하여야 한다. 이 경우 분임정보보안담당관이 점검한 후 그 결과를 정보보안담당관에게 통보하여야 한다.

1. 제1항에 따라 계약서에 명시된 보안 준수사항
2. 제27조에 따른 발주기관 내 작업장소 보안 준수사항
3. 제28조에 따른 원격지 개발 보안 및 제28조의2에 따른 원격지에서의 온라인 개발 시 보안 준수사항
4. 제50조에 따른 정보시스템 유지보수 및 제51조에 따른 온라인 유지보수 시 보안 준수사항

④ 정보보안담당관은 해당 기관 및 관할 하급기관에 대하여 용역업체 보안관리 실태 점검을 실시할 수 있으며, 필요한 경우 국가정보원장에게 지원을 요청할 수 있다.

⑤ 분임정보보안담당관은 제3항 및 제4항에 따른 점검 결과 용역업체 보안대책 준수가 미흡하고 시정조치가 어렵다고 판단할 경우 제28조에 따른 원격지 개발, 제28조의2에 따른 원격지에서의 온라인 개발 또는 제51조에 따른 온라인 유지보수 허가를 취소할 수 있다.

⑥ 분임정보보안담당관은 제28조의2에 따른 원격지에서의 온라인 개발, 제51조에 따른 온라인 유지보수를 허용하고자 할 경우에는 용역업체의 온라인 접속을 통제하기 위한 온라인 용역 통제시스템을 구축·운영하여야 한다.

⑦ 그 밖에 용역업체 보안과 관련한 사항은 국가정보원장이 배포한 「국가·공공기관 용역업체 보안관리 가이드라인」을 준수하여야 한다.

제26조(소프트웨어 개발보안) 분임정보보안담당관은 정보시스템을 개발할 경

우 「전자정부법」 제45조제3항에 따라 규정된 「행정기관 및 공공기관 정보시스템 구축·운영지침」(행정안전부 고시) 제50조부터 제53조까지에 따라 보안 취약점이 발생하지 아니하도록 개발(이하 “소프트웨어 개발보안”이라 한다)하고 정보시스템 감리 등을 통해 보안취약점을 진단하여야 한다.

제27조(발주기관 내 작업장소 보안) ① 분임정보보안담당관은 발주기관 내(분임정보보안담당관이 임차한 외부 사무실을 포함한다) 용역업체 작업장소를 설치할 경우 보안 통제가 가능한 공간을 마련, 운영하여야 한다.

② 발주기관 내 용역업체 작업장소에 설치 운영하는 정보통신망은 발주기관의 정보통신망과 분리 구성하여야 한다. 다만, 용역업체가 사업 수행을 위하여 발주기관 정보시스템 이용이 불가피할 경우에는 필요한 정보시스템에 한해 지정된 단말기로부터의 제한적 접근을 허용하는 등 보안대책을 수립·시행하여야 하며, 이 경우 내부망 정보시스템에 대한 접근 허용에 관하여는 국가정보원장과 사전 협의하여야 한다.

③ 작업장소 내 정보시스템은 용역사업 수행을 위해 필요한 경우 해당 분임정보보안담당관의 보안통제 하에 인터넷에 연결할 수 있다. 다만, 제2항 단서에 따른 발주기관 정보시스템 접근용 단말기의 경우에는 인터넷 연결을 금지한다.

④ 분임정보보안담당관은 용역업체가 발주기관 내 작업장소에서 개발 작업을 수행하더라도 개발용 서버가 민간 클라우드컴퓨팅서비스를 이용하는 등으로 원격지에 위치할 경우 제28조에 따른 원격지 개발로 간주하고 제28조제1항에 따른 보안대책을 수립·시행하여야 한다.

제28조(원격지 개발보안) ① 분임정보보안담당관은 「소프트웨어 진흥법」 제49조제3항 및 제4항, 「소프트웨어사업 계약 및 관리감독에 관한 지침」 제14조에 따라 용역업체가 발주기관 이외 장소(이하 “원격지”라 한다)에서 개발 작업(유지보수는 제외한다)을 수행하고자 요청할 경우 제13조제1항제1호에 따른 용역업체 작업장소에 대한 보안요구사항 등을 포함한 관리적·기술적 보안대책을 수립·시행하여야 한다. 이 경우 분임정보보안담당관은 보안대책을 수립한 후 정보보안담당관의 승인을 받아야 한다.

② 원격지 내 정보시스템은 개발 작업을 위하여 필요한 경우 해당 분임정보보안담당관의 보안 통제 하에 인터넷에 연결할 수 있다.

제28조2(원격지에서의 온라인 개발) 제28조에 따른 원격지 개발에서 분임정보 보안담당관이 필요하다고 판단하고 용역업체가 다음 각 호에 따른 보안대책에 서면으로 동의하는 경우에 한하여, 분임정보보안담당관은 정보보안담당관의 승인 후 용역업체에게 원격지에서 인터넷을 통해 발주기관 정보시스템에 온라인 접속한 상태의 개발 작업을 허용할 수 있다.

1. 지정된 단말기에서만 접속 및 해당 단말기에 대한 접근인원 통제
2. 지정 단말기는 제3호에 따른 온라인 용역 통제시스템 접속 전용(專用)으로 운용하고 다른 목적의 인터넷 접속은 차단
3. 발주기관 내 설치된 온라인 용역 통제시스템을 경유하여 개발에 필요한 정보시스템에 접속하는 등 소통구간 보호·통제
4. 접속사실이 기록된 로그기록을 1년 이상 보관
5. 계약 시행일로부터 종료 후 30일이 경과하는 날까지의 기간 중에 정보보안담당관, 도지사 및 국가정보원장의 정기 또는 수시 보안점검(불시 점검을 포함한다) 수검
6. 기타 국가정보원장이 배포한 「국가·공공기관 용역업체 보안관리 가이드라인」에서 제시된 온라인 개발에 관련된 보안대책의 준수

제29조(소프트웨어 산출물 제공) ① 분임정보보안담당관은 용역업체가 「소프트웨어 진흥법」 제59조 및 「(계약예규)용역계약일반조건」(기획재정부 계약예규) 제56조에 따른 지식재산권을 행사하기 위하여 소프트웨어 산출물의 반출을 요청할 경우 제안요청서 또는 계약서에 명시된 누출금지정보에 해당하지 아니하면 제공하여야 한다.

② 분임정보보안담당관은 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 별지 제7호서식 확인서를 받아야 한다.

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

④ 그 밖에 소프트웨어 산출물 제공과 관련한 사항은 「소프트웨어사업 계약 및 관리감독에 관한 지침(과학기술정보통신부 고시)」 제32조를 준수하여야 한다.

제30조(누출금지정보 유출 시 조치) ① 분임정보보안담당관은 용역업체가 제 안요청서 또는 계약서에 명시된 누출금지정보를 유출한 사실을 인지한 경우 업체를 대상으로 계약 위반에 따른 조치를 취하여야 한다. 이 경우 용역업체의 누출금지정보 유출 사실을 인지한 경우 즉시 정보보안담당관을 거쳐 시장에게 보고하여야 한다.

② 제1항에 따라 용역업체의 누출금지정보 유출 사실을 인지하거나 보고를 받은 정보보안담당관은 그 사실을 도지사 및 국가정보원장에게 통보하여야 하고, 「지방자치단체를 당사자로 하는 계약에 관한 법률 시행령」 제92조에 따라 입찰 참가자격 제한 등 관련조치를 취하여야 한다.

제5절 보안적합성 검증

제31조(대상 제품) 분임정보보안담당관은 제20조제1항제3호에 따른 보안기능이 있는 정보통신제품을 도입하는 경우 실제 적용·운용 이전에 안전성을 확인하기 위하여 보안적합성 검증을 받아야 한다.

제32조(검증기관 및 신청) ① 분임정보보안담당관은 제31조에 따라 보안적합성 검증을 받고자 할 경우 정보보안담당관을 거쳐 다음 각 호의 기관(이하“검증기관”이라 한다)의 장에게 검증을 신청하여야 한다.

1. 주요정보통신기반시설 관리기관 : 국가정보원
2. 시(주요정보통신기반시설 관리기관을 제외한다) : 경기도

② 제1항제2호에도 불구하고 시장이 필요하다고 판단하는 경우 도지사와 협의하여 자체적으로 검증을 실시할 수 있다.

③ 제1항에 따라 검증을 신청한 분임정보보안담당관은 국가정보원장이 필요하다고 판단하여 추가 자료를 요청할 경우 이를 제출하여야 한다.

제33조(검증 신청 시 제출물) ① 분임정보보안담당관은 제32조에 따라 보안적합성 검증을 신청할 경우 정보보안담당관을 통하여 검증기관의 장에게 별표 2의 보안적합성 검증 신청 시 제출물에 해당하는 문서 등을 제출하여야 한다.

② 제1항에 따라 검증을 신청한 분임정보보안담당관은 정보보안담당관 및 검증기관의 장이 필요하다고 판단하여 추가 자료를 요청할 경우 이를 제출하여

야 한다.

제34조(안전성 시험) ① 정보보안담당관은 제33조에 따라 제출된 문서 내용의 적절성을 검토한 후 검증대상 제품에 대하여 보안기능 정상 동작여부 등 안전성을 시험한다. 이 경우 정보보안담당관은 시험에 필요한 사항을 추가로 요청할 수 있다.

② 정보보안담당관은 검증대상 제품의 제출 지연 등의 사유로 시험을 진행할 수 없을 경우 검증 절차를 중단할 수 있다.

제35조(검증결과 통보 및 조치) ① 정보보안담당관은 「국가 정보보안 기본지침」 제35조에 따라 검증기관의 장으로부터 통보 받은 검증결과를 분임정보보안담당관에게 통보하여야 한다.

② 제1항에 따라 검증결과를 통보받은 분임정보보안담당관은 해당 조치를 실시하고 그 결과를 정보보안담당관을 거쳐 검증기관의 장에게 통보하여야 한다.

제36조(취약점 조치) 분임정보보안담당관은 보안적합성 검증이 완료된 제품에서 새로운 취약점이 발견되거나, 정보보안담당관 및 국가정보원장으로부터 취약점 제거 또는 보완조치를 요청받은 경우 이를 조치하고 그 결과를 정보보안담당관을 거쳐 국가정보원장에게 통보하여야 한다.

제37조(형상변경 및 용도변경 시 조치) 분임정보보안담당관은 보안적합성 검증이 완료된 제품의 보안기능 등 형상 변경이 필요하거나 도입 목적 이외의 용도로 운용이 필요한 경우 검증기관의 장과 협의하여 재검증 등 필요한 조치를 취하여야 한다.

제38조(이행여부 확인) ① 분임정보보안담당관은 보안적합성 검증을 받은 제품의 운용 실태, 개선 조치 이행여부 등을 정보보안담당관, 도지사 또는 국가정보원장이 확인하려 할 경우 이에 응하여야 한다.

② 분임정보보안담당관은 정보보안담당관, 도지사 또는 국가정보원장이 제1항에 따른 이행여부를 확인한 결과 미비점이 발견되어 시정 조치를 요청하는 경우 이에 응하여야 한다.

제3장 정보통신망 및 정보시스템 보안

제1절 정보통신망 보안

제39조(내부망·인터넷망 분리) ① 정보보안담당관은 내부망과 기관 인터넷망을 분리·운영하여야 한다.

② 정보보안담당관은 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 차단 대책
4. 내부망과 기관 인터넷망간 안전한 자료전송 대책
5. 기타 국가정보원장이 배포한 「국가·공공기관 업무전산망 분리 및 자료전송 보안가이드라인」에서 제시하는 보안대책

③ 정보보안담당관은 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 정보보안담당관은 분리된 내부망과 기관 인터넷망 간 자료전송을 위한 접점이 불가피한 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 침입차단·탐지시스템 설치·운영
2. 내부망과 기관 인터넷망 간 점점 최소화
3. 내부망과 기관 인터넷망 간 일방향 전송장비 등을 이용한 자료전송체계를 구축·운영하고 원본파일은 3개월 이상, 전송기록은 6개월 이상 유지
4. 정기적으로 전송실패 기록을 확인하고 악성코드 유입 여부 등 점검
5. 내부망 자료를 기관 인터넷망으로 전송할 경우 부서 분임정보보안담당관 또는 결재권자의 사전 또는 사후 승인절차 마련

⑤ 정보보안담당관은 제1항에도 불구하고 예산 부족 등 사유로 부득이한 경

우 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 통제 대책
2. 인터넷 PC의 악성코드 감염 최소화를 위한 인터넷 사용 통제 대책
3. 인터넷 PC의 악성코드 감염에 따른 내부망으로의 피해확산 차단 대책
4. 사이버공격 탐지·대응 등 안전한 업무환경을 위한 보호 대책
- ⑥ 정보보안담당관은 내부망과 기관 인터넷망의 IP주소 현황을 정기적으로 확인하고 갱신하여야 한다.
- ⑦ 본 조에 따른 보안대책은 「공공데이터의 제공 및 이용 활성화에 관한 법률」 제17조에 따른 국민제공 공공데이터 범위 산정에는 영향을 미치지 아니하며, 국민에게 제공하는 공공데이터의 범위를 축소하는 것으로 해석하여서는 아니된다.

제40조(클라우드컴퓨팅 보안) ① 분임정보보안담당관은 클라우드컴퓨팅(공공 클라우드센터를 포함)을 자체 구축·운영하고자 할 경우 국가정보원장이 배포한 「국가·공공기관 클라우드 컴퓨팅 보안 가이드라인」에 명시된 기관 자체 클라우드컴퓨팅 구축 보안기준에 따라 보안대책을 수립·시행하여야 한다.
(개정 2023. 7. 31)

② 분임정보보안담당관은 민간 클라우드컴퓨팅서비스를 이용하고자 할 경우 다음 각호에 해당하는 사항을 준수하여야 한다. <개정 2023. 7. 31>

1. 국내에 위치한 정보시스템(인증서버, 로그 및 백업서버 등)·관리주체에 의해 데이터가 저장·관리되는 서비스의 이용
2. 다음 각목의 요건에 따라 일반 이용자용 서비스와 영역이 분리되어 제공되는 서비스(이하 “공공 전용(專用) 민간클라우드”라 한다)의 이용
 - 가. 영역 분리는 일반 이용자용 서비스와 데이터 및 프로세스 등의 간섭없이 국가정보원 및 이용기관의 보안관제, 사고조사, 예방보안활동 유지를 위한 제반 환경을 만족해야 함
 - 나. 영역 분리는 ‘시스템 중요도’에 따라 물리적 또는 논리적으로 구현
 - 다. ‘시스템 중요도’ 분류는 [별표 4]의 기준 준용
3. 국가정보원장이 배포한 「국가·공공기관 클라우드 컴퓨팅 보안 가이드라

인」에서 정하는 바에 따라 국가정보원장이 게시하거나 게시 예정인 민간 클라우드컴퓨팅서비스 이용

4. '내부망·인터넷망 분리' 원칙 등 여타 보안 관련사항은 「국가정보보안기본지침」 및 「국가 클라우드 컴퓨팅 보안가이드라인」 준수
5. 민간 클라우드컴퓨팅서비스 사업자와 계약시 해킹사고 및 장애 대응, 재발 방지 등에 필요한 조치를 위해 국가정보원 및 이용기관의 보안관제 및 사고조사, 사이버공격 및 위협에 대한 예방 및 대응활동 등에 적극 협조하도록 하는 내용의 명시

③ 내부망과 연동된 공공 전용(專用) 민간클라우드에는 이 규정을 적용함에 있어 내부망으로 본다.

④ 기관 인터넷망과 연동된 공공 전용(專用) 민간클라우드에는 이 규정을 적용함에 있어 기관 인터넷망으로 본다.

⑤ 분임정보보안담당관은 제2항에 따라 민간 클라우드컴퓨팅서비스를 이용하는 경우 클라우드컴퓨팅서비스제공자에 의하여 누출금지정보가 유출된 경우 제30조에 따른 조치를 취하여야 한다.

⑥ 제2항에 따라 분임정보보안담당관이 이용하는 민간 클라우드컴퓨팅서비스의 제공자는 공공 전용(專用) 민간클라우드 영역에 대해 정부 기관에 준하는 보안관리 책임을 진다. <신설 2023. 7. 31>

제41조(보안·네트워크장비 보안) ① 분임정보보안담당관은 침입차단·탐지시스템, 스위치·라우터 등 기관 정보통신망 구성 또는 정보보안 정책 전반에 영향을 미치는 보안·네트워크장비를 설치·운용하고자 할 경우 다음 각 호의 사항을 포함한 보안대책을 수립·시행하여야 한다.

1. 물리적으로 안전한 장소에 설치하여 비(非)인가자의 무단접근 통제
2. 콘솔에서 관리함을 원칙으로 하되, 다음 각 목의 경우 청사 내 지정 단말기로부터의 접속·관리 허용
 - 가. 장비 관리자의 접속
 - 나. 제27조제2항 단서에 따른 발주기관 내 용역업체 작업장소에서의 접속
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 보안·네트워크 장비 관리자는 로그기록을 1년 이상 유지하여야 하고 비(非)인가자의 접속여부를 정기적으로 점검하여 그 결과를 정보보안담당관에게 통보하여야 한다.

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

제42조(무선랜 보안) ① 정보보안담당관은 내부망을 제외한 정보통신망에서 다음 각 호의 경우와 같이 청사 내에 무선랜(WiFi)을 구축·운영할 수 있다.

1. 기관 인터넷망에 중계기(AP)를 설치하여 제73조제1항에 따라 해당 기관의 장이지급한 단말기의 접속만을 허용하는 업무용 무선랜
2. 상용 인터넷망에 중계기(AP)를 설치하여 제78조제1항 각 호에 따라 반입한 공무원 등의 개인 소유 이동통신단말기의 접속만을 허용하는 무선랜
3. 상용 인터넷망에 중계기(AP)를 설치한 외부인 전용(專用) 무선랜

② 정보보안담당관은 제1항에 따라 무선랜을 구축·운영하고자 할 경우 국가정보원장이 배포한 「국가·공공기관의 무선랜 구축 및 RFID 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 해당무선랜에 접속되지 아니하도록 하는 기술적 보안대책

8. 그 밖에 무선랜 단말기·중계기(AP) 등 구성요소별 분실·탈취·훼손·오용등에 대비한 관리적·물리적 보안대책

④ 정보보안담당관은 제2항 및 제3항에 따른 보안대책의 적절성을 수시로 점검·보완 하여야 한다.

제43조(이동통신망보안) ① 정보보안담당관은 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 정보보안담당관은 제1항에 따라 이동통신망을 이용한 시스템을 구축·운영할 경우 해당 기관의 정보통신망과 혼용되지 않도록 하여야 한다.

제44조(영상회의 보안) ① 정보보안담당관은 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.

③ 분임정보보안담당관은 다음 각 호의 구분에 따라 상용 소프트웨어에 탑재된 영상회의 서비스를 이용할 수 있다.

1. 비공개 업무자료를 취급하거나 회의 내용이 비공개 업무자료에 준하다고 판단할 경우 : 영상·음성·업로드 데이터가 국내 서버로만 전송되는 상용 영상회의의 소프트웨어(이하 “국내 영상회의 솔루션”이라 한다)를 활용
2. 공개 업무자료를 취급하거나, 회의 내용이 공개 업무자료에 준하다고 판단할 경우 : 국내 영상회의의 솔루션 또는 그 밖의 영상회의의 소프트웨어를 활용

④ 전항 제1호에도 불구하고, 분임정보보안담당관은 다음 각 호의 어느 하나에 해당하는 등 정당한 사유가 있는 경우 국가정보원장과 협의하여 국내 영상회의의 솔루션 외의 소프트웨어를 일시적 또는 정기적으로 활용할 수 있다.

1. 안보·국익상 필요한 외국기관(외국軍을 포함한다)과의 영상회의 시에 상대방이 국내 영상회의의 솔루션을 활용할 수 없거나, 상대방이 국내 영상회의의 솔루션 외의 소프트웨어 활용을 제안할 경우

2. 정책자문 등의 목적으로 민간인과 영상회의 시에 상대방이 국내 영상회의 솔루션을 활용할 수 없는 경우

⑤ 기타 영상회의 보안과 관련한 사항은 국가정보원장이 배포한 「원격업무 통합보안매뉴얼」을 준수하여야 한다.

제45조(인터넷전화 보안) ① 정보보안담당관은 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 정보보안담당관은 민간 인터넷전화 사업자망을 이용할 경우 해당 사업자로 하여금 서비스 제공 구간에 대한 보안대책을 수립하도록 하여야 한다.

③ 외교·국방 등 국가안보 관련 기관의 장은 인터넷전화시스템을 구축·운영하고자 할 경우 국가정보원장이 별도로 정한 암호기술 규격을 준수하여야 한다.

④ 기타 인터넷전화 보안과 관련한 사항은 국가정보원장이 배포한 「국가·공공기관 인터넷전화 보안 가이드라인」을 준수하여야 한다.

제46조(인터넷 사용제한) ① 정보보안담당관은 국가비상사태 및 대형 재해·재난의 발생, 사이버공격 등으로부터 정보통신망과 정보시스템의 정상적인 운영을 보장하기 위하여 소속 공무원 등에 대한 인터넷 사용을 일부 제한할 수 있다.

② 정보보안담당관은 기관 인터넷망의 효율적인 운영 관리 및 악성코드 유입 차단을 위하여 게임·음란·도박 등 업무와 관련이 없는 인터넷 이용을 차단하여야 하며, 악성코드 유입 차단을 위하여 필요할 경우 제65조제4항에 따른 상용 정보통신서비스의 접속을 제한할 수 있다.

제47조(외교통신 보안) ① 정보보안담당관은 재외공관과 비밀 등 중요자료를

소통하고자 할 경우 국가정보원장이 개발하거나 안전성을 확인한 암호자재를 사용하는 외교정보통신망을 사용하여야 한다.

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

③ 정보보안담당관은 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 보안 대책을 준수하여야 한다.

제47조의2(파견사용 정보통신망) ① 시장은 다른 기관에 파견된 소속 공무원 등의 활용을 위하여 파견기관의 장과 협의하여 원(原) 소속 기관의 정보통신망 전용(專用) 단말기를 파견기관에 설치·운영할 수 있다.

② 정보보안담당관은 제1항에 따라 단말기를 설치할 경우 단말기와 기관 정보통신망 간 소통내용을 보호하여야 한다.

③ 제1항에 따라 각급기관 내부망과 연동된 단말기는 이 규정을 적용함에 있어 원(原) 소속 기관의 내부망 단말기로 본다.

④ 제1항에 따라 각급기관 인터넷망과 연동된 단말기는 이 규정을 적용함에 있어 원(原) 소속 기관의 인터넷망 단말기로 본다.

제48조(재외사무소 정보보안점검) ① 정보보안담당관은 외국에 사무소를 개설·운영할 경우 해당 사무소의 정보통신망 및 정보시스템에 대한 보안관리 실태를 점검하고 취약요인을 개선하도록 하여야 한다.

② 정보보안담당관은 제1항에 따른 보안관리 실태 점검을 위하여 필요한 경우 국가정보원장에게 중점 점검사항, 전문 인력 지원 등 협조를 요청할 수 있다.

제2절 정보시스템 보안

제49조(정보시스템 보안책임) ① 분임정보보안담당관은 정보시스템(PC·서버·네트워크장비·정보통신기기 등을 포함한다)을 도입·운영할 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 별지 제3호서식에 따른 정보시스템 관리대장을 수기 또는 전자적으로 작성·관리하여야 한다.

④ 정보시스템 관리책임자는 해당 부서의 별지 제3호서식에 따른 정보시스템 관리대장에 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.

제50조(정보시스템 유지보수) ① 정보시스템의 유지보수와 관련한 절차, 주기, 문서화 등을 수립할 경우 고려사항은 다음 각 호와 같다.

1. 유지보수 인원에 대한 보안서약서 집행, 보안교육 등을 포함한 유지보수 인가절차를 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 제27조제1항에 따른 발주기관 내 용역업체 작업장소로 반출·입할 경우 악성코드 감염여부 및 자료 무단 반출여부 확인 등 보안조치를 실시하고 그 결과를 분임정보보안담당관에게 제출하여야 한다.

③ 정보시스템 관리자는 직접 또는 용역업체를 활용하여 정보시스템을 유지보수할 경우 콘솔 또는 지정된 단말기로부터의 접속만을 허용하여야 한다.

④ 정보보안담당관은 소관 정보시스템에 대하여 중요도·가용성 등에 따라 등급을 분류하고 해당 등급에 맞게 정보 보존 및 관리, 장애관리, 보안관리 등을 수행하여야 한다.

제51조(지정 단말기를 통한 온라인 유지보수) ① 제50조제3항에 따른 지정된 단말기를 통해 유지보수를 함에 있어 분임정보보안담당관이 필요하다고 판단하고 용역업체가 다음 각 호에 따른 보안대책에 서면으로 동의하는 경우에만 한하여, 분임정보보안담당관은 정보보안담당관의 승인 후 용역업체에게 내부망을 포함하여 소관 정보시스템(제41조제1항에 따른 보안·네트워크장비는 제외한다)에 대하여 인터넷을 통한 온라인 유지보수를 허용할 수 있다.

1. 지정된 장소에 설치된 지정된 단말기에서만 접속 및 해당 단말기에 대한 접근인원 통제
2. 지정 단말기는 제3호에 따른 온라인 용역 통제시스템 접속 전용(專用)으로 운용하고 다른 목적의 인터넷 접속은 차단
3. 발주기관 내 온라인 용역 통제시스템을 경유하여 유지보수 대상 정보시스템에 접속하는 등 소통구간 보호·통제
4. 접속사실이 기록된 로그기록을 1년 이상 보관
5. 유지보수 계약 시행일로부터 종료 후 30일이 경과하는 날까지의 기간 중에 발주기관, 도지사 및 국가정보원장의 정기 또는 수시 보안점검(불시 점검을 포함한다) 수검
6. 기타 국가정보원장이 배포한 「국가·공공기관 용역업체 보안관리 가이드라인」에서 제시된 온라인 유지보수에 관련된 보안대책의 준수

② 분임정보보안담당관은 전항 제2호 및 제3호에도 불구하고 온라인 용역 통제시스템이 구축되지 않았으나 온라인 유지보수를 즉시 실시하지 않고서는 기관 업무수행에 현저한 손해가 있다고 예상되는 경우에는 인터넷망 정보시스템에 한하여 직접 접속하는 온라인 유지보수를 일시적으로 허용할 수 있다.

③ 기타 정보시스템 온라인 유지보수 보안과 관련한 사항은 제25조(용역업체 보안)를 준용한다.

제52조(서버 보안) ① 분임정보보안담당관은 서버를 도입·운용하고자 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 접근 권한 차등 부여
2. 개별사용자별 자료 접근범위를 서버에 등록하여 인가여부를 식별하도록 하고 인가된 범위 이외의 자료 접근통제
3. 서버 운용에 필요한 서비스 포트 이외에 불필요한 서비스 포트 제거 및 관리자용 서비스와 개별사용자용 서비스 분리·운용
4. 관리자용 서비스 접속 시 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 연1회 이상 서버 설정 정보와 저장자료의 절취 및 위·변조 가능성 등 보안 취약점을 점검·보완하여야 한다.

제52조의2(제어시스템 보안) ① 분임정보보안담당관은 공항·항만·전력·가스·운송설비 등을 중앙에서 감시·제어하기 위한 정보시스템(이하 “제어시스템”이라 한다)을 구축·운용하고자 할 경우 최신 백신 소프트웨어 설치, 응용 프로그램 보안패치 및 침해사고 대응방안 등 보안대책을 수립·시행하고 정기적으로 취약점을 점검·제거하여야 한다. 다만, 백신 소프트웨어 등 보안소프트웨어를 설치함으로써 제어시스템의 정상 운영에 차질을 초래할 경우 국가정보원장과 협의하여 설치하지 아니할 수 있다.

② 분임정보보안담당관은 교통·에너지·원전 등 국가안보상 중요한 제어시스템을 운용할 경우 인터넷 및 일반 사무용 내부망과 분리·구축하여야 한다.

③ 분임정보보안담당관은 제2항에도 불구하고 제어시스템을 기관 인터넷망과 연동할 필요가 있는 경우 연동 구간에 일방향 전송장비 설치 등 안전한 망(網)연동 수단을 설치·운용하여야 하며, 국민의 생명 구조 등 국민안전에 불가피한 경우에는 국가정보원장과 협의하여 양방향 통신방식으로 연동할 수 있다.

④ 기타 제어시스템 보안과 관련한 사항은 국가정보원장이 배포한 「국가·공공기관 제어시스템 보안가이드라인」을 준수하여야 한다.

제53조(공개서버 보안) ① 분임정보보안담당관은 외부인에게 공개할 목적으로 웹서버 등 공개서버를 구축·운영하고자 할 경우 내부망과 분리된 영역(DMZ)에 설치하여야 한다.

② 분임정보보안담당관은 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 무단 접근을 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 제52조(서버 보안)를 준용한다.

제54조(로그기록 유지) ① 분임정보보안담당관은 정보시스템의 효율적인 통제·관리 및 사고 발생 시 추적 등을 위하여 개별사용자의 정보시스템 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 분임정보보안담당관을 거쳐 정보보안담당관에게 통보하여야 한다.

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

제55조(업무용 통신단말기 보안) ① 정보보안담당관은 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 정보보안담당관은 제1항에 따른 보안대책을 수립하기 위하여 국가정보원 장에게 취약점 점검 및 기술 지원을 요청할 수 있다.
- ③ 정보보안담당관은 제1항제1호에 따른 통신단말기 개별사용자를 대상으로 인증 및 암호화에 필요한 디지털정보를 발급할 수 없을 경우 국가정보원장이 배포한 「정보통신기 암호기술 적용지침」을 준수하여야 한다.
- ④ 정보보안담당관은 해당 기관의 주요 보직자가 안전한 통화를 위하여 사용하는 공용(公用) 휴대폰(이하 “안보폰”이라 한다)이 분실·훼손되지 않도록 현황을 관리하여야 한다. 이 경우 정보보안담당관은 국가정보원장이 예외로 허용하는 운용방식 이외에는 제113조(운용 및 관리)에 따라 보안대책을 수립·시행하여야 한다

제56조(모바일 업무 보안) ① 정보보안담당관은 휴대폰·태블릿 PC 등을 이용한 모바일 업무환경(내부 행정업무, 현장 행정업무 및 대민서비스 업무 등)을 구축·운영하고자 할 경우 보안대책을 수립·시행하여야 한다.

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

제57조(사물인터넷 보안) ① 정보보안담당관은 사물인터넷을 이용한 시스템을 구축·운영하고자 할 경우 사물인터넷 기기 및 중요 데이터 등을 보호하기 위하여 보안대책을 수립·시행하여야 한다.

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

③ 정보보안담당관은 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.

제58조(원격근무 보안) ① 정보보안담당관은 소속 공무원 등이 재택근무, 출장지 현장 근무 또는 파견 근무(제47조의2에 따라 기관 정보통신망 전용(專用) 단말기를 설치 운영하는 경우는 제외한다)시 인터넷을 통해 본인 인증을 거쳐 기관 정보시스템에 접속하여 온라인상으로 업무를 수행(이하 “원격근무”라 한다)하게 할 수 있다.

② 제1항에 따른 원격근무를 위해 접속할 수 있는 기관 정보시스템은 다음 각 호와 같다.

1. 기관 인터넷망에 위치한 서버 및 서버에서 구동되는 가상 PC
2. 제39조제2항제4호에 따른 방법을 통해 접속할 수 있는 내부망 서버 및 서버에서 구동되는 가상 PC

③ 제1항에 따른 원격근무로 취급할 수 있는 업무자료의 범위는 공개 및 비공개 업무자료로 한다.

④ 정보보안담당관은 원격근무를 시행하고자 할 경우 다음 각 호의 사항을 포함한 보안대책이 강구된 정보시스템(이하 “원격근무시스템”이라 한다)을 구축·운영하여야 한다.

1. 검증필 암호모듈이 탑재된 정보보호시스템을 사용해 원격근무시스템과 원격근무자의 단말기 간 소통구간 암호화
2. 문서 암호화제품(DRM) 사용 등 문서 보호대책 강구
3. 원격근무자를 식별·인증하기 위하여 공인인증서, 생체인증 기술 및 일회용 비밀번호 생성기(OTP) 등 보안성을 강화한 사용자 인증방식 적용
4. 원격근무자로 하여금 원격근무시스템 접속과정에서 제1호부터 제3호까지의 보안대책을 준수토록 조치
5. 원격근무시스템에 대한 보안취약점 정기 점검

⑤ 원격근무자는 정보보안담당관이 원격근무용 단말기(개인 소유의 정보통신기기를 포함한다)의 보안을 위하여 취하는 다음 각 호의 조치에 적극 협조하여야 한다.

1. 제4항에 따라 정보보안담당관이 제공하는 보안소프트웨어 설치·운영
2. 사이버공격 등으로 인한 자료유출 사고 발생 시 정보보안담당관이 요청하는 점검 및 제135조제3항에 따른 자료제출 요청 협력
3. 소속된 기관에서 지급받은 단말기의 경우 제73조에 따른 단말기 보안대책

준수

⑥ 정보보안담당관은 원격근무자에게 제5항에 따른 보안조치 등이 포함된 보안서약서를 징구하고 직위·임무에 부합한 정보시스템 접근권한 부여 및 보직변경·퇴직 등 변동사항이 발생 시 접근권한 조정 등의 절차를 마련·시행하여야 한다.

⑦ 기타 원격근무 보안과 관련한 사항은 국가정보원장이 배포한 「원격업무 통합보안매뉴얼」을 준수하여야 한다.

제59조(국제회의 보안) ① 정보보안담당관은 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.

제60조(저장매체 불용처리) ① 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 분임정보보안담당관 협의하여야 한다.

② 제1항에 따라 자료를 삭제할 경우 저장매체별·자료별 차별화된 삭제 방법을 적용할 수 있으며 자료 복구가 불가하도록 완전 삭제하여야 한다.

③ 제2항에도 불구하고 저장장치 전체를 암호화하여 사용한 반도체 기반 저장장치(SSD)의 경우에는 비밀·대외비를 저장하지 아니한 경우에 한하여 완전삭제 소프트웨어를 활용하여 불용 처리할 수 있다. 다만, 비밀·대외비를 저장한 경우와 암호화 키는 완전 폐기하여야 한다.

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

제3절 자료 보안

제61조(비밀의 전자적 처리) ① 분임정보보안담당관은 「보안업무규정」에 따라 비밀의 생산, 분류, 보관, 열람, 출력, 송·수신, 이관, 파괴 등을 전자적으로 처리할 수 있다.

② 분임정보보안담당관은 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.

제62조(비밀관리시스템 운용) ① 정보보안담당관은 국가정보원장이 비밀관리시스템을 개발·보급할 경우 비밀을 전자적으로 안전하게 처리하기 위하여 이 시스템을 도입·운용할 수 있다.

② 정보보안담당관은 관리할 비밀이 적은 경우 「보안업무규정」 제21조제3항에 따라 국가정보원장이 구축·운영하는 통합 비밀관리시스템을 활용할 수 있다.

③ 정보보안담당관은 비밀관리시스템을 구축·운용할 경우 비밀의 생산·보관·유통 등 전반에 대하여 비밀관리시스템을 활용하여 비밀을 안전하게 관리하여야 한다.

④ 정보보안담당관은 국가정보원장이 비밀관리시스템의 안전한 운용·관리를 위하여 필요한 사항을 정하여 보급한 가이드라인 등을 활용할 수 있다.

⑤ 정보보안담당관은 비밀관리시스템을 자체적으로 개발·운용하고자 할 경우 제63조에 따른 비밀의 전자적 처리 규격을 준수하여 개발하여야 한다.

⑥ 정보보안담당관은 「보안업무규정」 제3조의2에 따라 자체적으로 개발한 비밀관리시스템에 대하여 국가정보원장에게 보안성 및 적절성 확인을 요청할

수 있다.

제63조(비밀의 전자적 처리 규격) 국가정보원장이 정한 비밀관리시스템의 개발에 필요한 비밀의 전자적 처리 규격은 다음 각 호와 같다.

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

제64조(대외비 전자적 처리) ① 분임정보보안담당관은 대외비를 전자적으로 처리하고자 할 경우에는 검증필 암호모듈을 사용하여 위조·변조·훼손 및 유출 등을 방지하기 위한 보안대책을 강구하여야 하며, 보호기간이 만료된 대외비는 제65조에 따른 비공개 업무자료의 처리 기준을 준용하여야 한다.

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

제65조(비공개 업무자료 처리) ① 공무원 등은 비공개 업무자료를 다음 각 호의 어느 하나에 해당하는 방법으로만 처리하여야 한다.

1. 소속 또는 근무 중인 기관의 내부망 PC 및 서버에 작성 및 저장·보관
2. 소속 또는 근무 중인 기관의 장이 지급한 휴대용 저장매체에 작성 및 저장·보관
3. 다음 각 목의 어느 하나에 해당하는 수단(이하 “업무자료 공식 소통수단”이라 한다)을 이용한 수·발신 또는 등재·열람
 - 가. 소속 또는 근무 중인 기관의 장이 자체적으로 구축·운영하는 전자우편 시스템(이하 “기관 전자우편”이라 한다)
 - 나. 공무원 등이 공동으로 사용할 목적으로 문화체육관광부 장관이 구축·운영하는 전자우편시스템(이하 “공직자통합메일”이라 한다)
 - 다. 공무원 등이 다른 공무원 등과 자료를 공유하거나 소통하기 위하여 사용하는 전용(專用) 소프트웨어(이하 “공공 전용(專用) 메신저”라 한다)

라. 국회사무처가 구축·운영하는 의정자료전자유통시스템 등 기관 간 업무 자료의 소통 또는 공동 활용을 위해 구축한 정보시스템

4. 그 밖에 다른 법규에 따라 허용되는 처리방법

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

1. 업무자료 공식 소통수단의 발신 또는 등재 기능을 이용하여 제2조제13호 다목의 문장 또는 문구 작성

2. 업무자료 공식 소통수단의 수·발신 또는 등재·열람 과정에서의 일시적 저장

3. 제39조제5항에 따른 기관 인터넷망 PC에 작성·저장

4. 제44조제3항 및 제4항에 따라 영상회의 솔루션을 활용하여 비공개 업무자료의 화면 영상을 공유하기 위한 일시적 저장

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

1. 업무자료 공식 소통수단의 발신 기능 또는 등재 기능을 이용하여 제2조제13호다목의 문장 또는 문구 작성

2. 업무자료 공식 소통수단의 수·발신 또는 등재·열람 과정에서의 일시적 저장

3. 제58조제4항에 따른 원격근무시스템에 접속하여 작성

4. 「감염병의 예방 및 관리에 관한 법률」 제34조제1항에 따른 감염병 위기관리 조치 등 대규모 질병·재난 발생 등 특별한 사정으로 재택근무를 명받았으나 소속 또는 근무 중인 기관에 제58조제4항에 따른 원격근무시스템이 구축되지 아니한 경우

5. 제44조제3항 및 제4항에 따라 영상회의 솔루션을 활용하여 비공개 업무자료의 화면 영상을 공유하기 위한 일시적 저장

6. 국민의 생명·신체, 국가안보 및 공공의 안전 등을 위하여 긴급히 작성, 저장, 수·발신이 필요하다고 소속 또는 근무 중인 기관의 장이 인정하는 경우

④ 공무원 등은 제3항제5호 및 제6호에 해당하는 경우를 제외하고는 「정보통신망 이용촉진 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 작성, 저장, 수·발신하여서는 아니 된다.

⑤ 공무원 등은 제2항부터 제4항까지에 따라 작성·저장한 비공개 업무자료는 활용이 종료된 후에는 삭제하여야 한다.

제65조의2(특정 상황별 비공개 업무자료 처리) ① 모든 공무원 등은 「국회법」 제128조제2항, 「국정감사 및 조사에 관한 법률」 제10조제2항, 「국회증언감정법」 제2조 및 제4조에 따라 국회·정부 간 비공개 업무자료를 소통할 경우에는 우선적으로 제65조제1항제3호라목의 의정자료전자유통시스템을 활용하여 처리하여야 하며, 시스템 장애 등 부득이한 사유로 활용이 곤란할 경우에 한해 제65조에 허용된 다른 방법으로 처리할 수 있다.

② 감독·감사·조사 등의 관계 법령에 따라 비공개 업무자료를 제출받을 권한이 있는 공무원 등은 업무자료를 제출할 상대방 공무원등에게 제65조에 위반되는 방법으로 자료 제출을 요구하여서는 아니 된다.

③ 공무원 등이 자문 등의 목적으로 비공개 업무자료를 업무자료 공식 소통수단을 활용할 수 없는 민간인에게 발신하거나 민간인으로부터 수신 받고자 할 경우에는 공무원 등의 소속 기관 전자우편 또는 공직자 통합메일을 활용하여 발신하거나 수신 받아야 한다.

제66조(행정전자서명 인증서 등 관리) ① 공무원 등은 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 공무원 등은 행정전자서명 인증서 및 인증서의 비밀번호, 기관 전자우편 또는 공직자통합메일의 비밀번호 등을 상용 정보통신서비스를 이용하여 수·발신하거나 저장·보관하여서는 아니 된다.

제67조(비공개 업무자료 유출방지) ① 정보보안담당관은 제65조에 따른 비공개 업무자료 처리 절차 준수여부를 관리·통제할 수 있는 보안체계를 구축·운영하여야 하며, 검증필 암호모듈 등을 사용하여 비공개 업무자료의 위조·

변조·훼손 및 유출 등을 방지하기 위한 보안대책을 강구하여야 한다.

② 정보보안담당관은 행정안전부장관이 다음 각 호에 해당하는 비공개 업무자료 관리·통제용 소프트웨어를 개발·보급할 경우 이를 활용할 수 있다.

1. 제1항에 따른 보안체계 구축·운영을 위한 공통 소프트웨어
2. 원격근무시스템 구축·운영을 위한 소프트웨어
3. 공공 전용(專用) 메신저

③ 정보보안담당관은 소속 공무원 등이 공공 전용(專用) 메신저 이용을 활성화할 수 있도록 노력하여야 한다.

제68조(공개 업무자료 처리) 공무원 등은 관계 법규에 위배되지 않는 범위 내에서 인터넷 PC나 개인이 소유한 PC·휴대용 저장매체·휴대폰(기관 청사 내에서는 제78조제1항 각 호에 따라 반입한 경우를 말한다), 상용 정보통신서비스(기관 청사 내에서는 제46조제2항에 따른 제한이 없는 경우를 말한다) 등을 이용하여 공개 업무자료를 처리할 수 있다.

제69조(홈페이지 등 게시자료 보안) ① 정보보안담당관은 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 분임정보보안담당관은 해당 부서에서 홈페이지 등에 업무자료를 게시하고자 할 경우 자료 내용을 사전 검토하여 비공개 업무자료가 게시되지 아니하도록 하여야 한다.

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

④ 분임정보보안담당관은 홈페이지 등에 비공개 업무자료가 무단 게시된 사실을 인지한 경우 즉시 삭제 또는 차단 등 보안조치를 취하여야 한다.

제70조(정보통신망 현황자료 관리) ① 정보보안담당관은 다음 각 호에 해당하는 자료를 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따른 비공개 대상 정보로 지정·관리하여야 한다.

1. 정보통신망 구성현황(IP주소 할당현황을 포함한다. 이하 본 조에서 같다.)
2. 정보시스템 운용현황
3. 취약점 분석·평가 결과물(「정보통신기반 보호법」 제9조에 따른 취약점

분석·평가결과를 포함한다. 이하 본 조에서 같다.)

4. 주요 정보화사업 추진현황

② 제1항에도 불구하고 정보보안담당관은 다음 각 호에 해당하는 자료는 「보안업무규정 시행규칙」 제17조에 의거 국가정보원장이 배포한 「비밀세부분류지침」에 따라 비밀로 분류·관리하여야 한다.

1. 국방 연구개발 및 정보통신 관련자료
2. 암호자재 운용현황
3. 「보안업무규정」 제32조에 따른 국가보안시설 및 국가보호장비의 운영·관리에 필요한 정보통신망 구성현황 및 그에 대한 취약점 분석·평가 결과물
4. 그 밖에 제1항 각 호에 해당하는 자료 중에서 국가정보원장이 비밀로 분류할 것을 요청한 자료

③ 정보보안담당관은 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.

제71조(빅데이터 보안) ① 분임정보보안담당관은 빅데이터와 관련한 시스템을 구축·운영하고자 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) 권한부여 체계 수립
6. 데이터 파기절차 수립

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

제4절 사용자 보안

제72조(개별사용자 보안) ① 분임정보보안담당관은 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 취급 시 비밀취급 인가, 보안서약서 징구 등 보안 조치
3. 암호자재 취급 시 제99조에 따라 암호취급자 지정·관리
4. 보직변경, 퇴직 등 변동사항 발생 시 정보시스템 접근권한 조정

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

제73조(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 비밀번호의 정기적 변경 사용
2. 단말기 작업을 일정 시간 중단 시 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) 획득 시 신뢰할 수 있는 인터넷사이트를 활용하고 자료(파일) 다운로드 시 최신 백신 소프트웨어로 검사 후 활용
7. 인터넷 파일공유·메신저·대화방 프로그램 등 업무상 불필요한 프로그램의 설치 금지 및 공유 폴더 삭제
8. 웹브라우저를 통해 서명되지 않은 액티브-X 등이 다운로드·실행되지 않도록 보안 설정
9. 내부망과 기관 인터넷망이 분리된 기관의 인터넷 PC에서는 정보보안담당관이 정한 특별한 사유가 없는 한 문서프로그램을 읽기 전용(專用)으로 운

용

10. 그 밖에 국가정보원장이 안전성을 확인하여 배포한 프로그램의 운용 및 보안권고문 이행

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

제74조(계정 관리) ① 분임정보보안담당관은 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 공용(公用) 정보시스템 관리자는 개별사용자가 시스템 접속(로그온)에 5회 이상 실패할 경우 접속이 중단되도록 시스템을 설정하고 비(非)인가자의 침입 여부를 점검하여야 한다.

③ 공용(公用) 정보시스템 관리자는 개별사용자의 보직변경, 퇴직, 계약종료 등 변동사항이 발생할 경우 신속히 사용자 계정을 삭제하거나 부여된 접근권한을 회수하여야 한다.

④ 공용(公用) 정보시스템 관리자는 사용자 계정 부여 및 관리의 적절성을 연 2회 이상 점검하고 그 결과를 정보보안담당관에게 통보하여야 한다.

⑤ 공용(公用) 정보시스템 관리자는 제1항 및 제3항에 의한 접근권한 부여, 변경, 회수 또는 삭제 등에 대한 내역을 기록하고 3년 이상 보관하여야 한다.

제75조(비밀번호 관리) ① 개별사용자 및 공용(公用) 정보시스템 관리자는 각종 비밀번호를 다음 각 호에 해당하는 사항을 반영하고 숫자·문자·특수문자 등을 혼합하여 안전하게 설정하고 정기적(분기 1회)으로 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 공용(公用) 정보시스템 관리자는 서버 등 정보시스템에 보관되는 비밀번호가 복호화 되지 아니하도록 일방향 암호화하여 저장하여야 한다.
- ③ 정보보안담당관은 공용(公用) 정보시스템에서 개별사용자를 식별 또는 인증하기 위하여 비밀번호에 같음하거나 병행하여 지문인식 등 생체인증 기술 및 일회용 비밀번호 생성기(OTP) 등을 안전성 확인 후 사용할 수 있다. 이 경우 생체인증 정보는 안전하게 보관하여야 한다.

제76조(전자우편 보안) ① 정보보안담당관은 전자우편을 컴퓨터바이러스·트로이목마 등 악성코드로부터 보호하기 위하여 백신 소프트웨어 설치, 해킹메일 차단시스템 구축 등 보안대책을 수립·시행하여야 한다.

② 정보보안담당관은 기관 전자우편을 구축·운영할 경우 다른 전자우편과 자료를 안전하게 소통하기 위하여 전자우편시스템에 암호화 기술을 적용하여야 한다.

③ 정보보안담당관은 기관 전자우편을 구축·운영할 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 행정안전부장관에게 통보하여야 한다.

⑥ 정보보안담당관은 전자우편 발신자 조작 등을 통한 기관 사칭 전자우편의 유포를 차단하기 위하여 보안대책을 수립·시행하여야 한다.

제77조(휴대용 저장매체 보안) ① 분임정보보안담당관은 휴대용 저장매체를

사용하여 업무자료를 보관하고자 할 경우 자료의 위·변조, 저장매체의 훼손·분실 등에 대비한 보안대책을 수립·시행하여야 한다.

② 정보보안담당관은 휴대용 저장매체 관리시스템을 운용하고자 할 경우 국가정보원장이 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 휴대용 저장매체 관리자는 휴대용 저장매체를 비밀용·일반용으로 구분·관리하고 수량 및 보관 상태를 정기적으로 점검하며 외부 반출·입을 통제하여야 한다.

⑤ 휴대용 저장매체 관리자는 비밀이 저장된 휴대용 저장매체는 매체별로 비밀등급 및 관리번호를 부여하고 비밀관리기록부에 등재·관리하여야 한다. 이 경우 매체 전면에 비밀등급 및 관리번호가 표시되도록 하여야 한다.

⑥ 휴대용 저장매체 관리자는 비밀용 휴대용 저장매체를 다른 등급의 비밀용 또는 일반용으로 변경 사용하고자 할 경우 저장자료가 복구 불가하도록 완전 삭제 소프트웨어 등을 이용하여 삭제하여야 한다. 다만, 완전 삭제가 불가할 경우 변경 사용하여서는 아니 된다.

⑦ 휴대용 저장매체 관리자는 휴대용 저장매체를 폐기·불용 처리하고자 할 경우 저장자료가 복구 불가하도록 완전 삭제 소프트웨어 등을 이용하여 삭제하여야 한다. 다만, 완전 삭제가 불가할 경우 파쇄하여야 한다.

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

⑨ 그 밖에 휴대용 저장매체 보안과 관련한 사항은 국가정보원장이 배포한 「USB메모리 등 휴대용 저장매체 보안관리지침」을 준수하여야 한다.

제78조(비인가 기기 통제) ① 공무원 등은 다음 각 호의 경우를 제외하고는 개인 소유의 정보통신기기를 소속된 기관으로 무단 반입·사용하여서는 아니 된다.

1. 보편적 통신 목적의 개인 소유 이동통신단말기(LTE·5G 등 이동통신망 접속기능이 있는 휴대폰·태블릿·스마트워치) : 반입하여 개인 용도로만

사용. 이 경우 반입 장비를 도크스테이션(dock station)·마우스·모니터·키보드 등 PC와 유사하게 활용토록 하는 장치와의 연결 사용을 금한다.

2. 제1호를 제외한 정보통신기기 : 제1호에 따른 반입·사용만으로는 보편적 통신 곤란 등 특별한 사정이 있는 경우에 한하여 소속 부서의 분임정보보안담당관을 거쳐 정보보안담당관의 승인을 받아 반입 후 개인 용도로만 사용

② 공무원 등은 제1항 각 호에 따라 반입한 개인 소유의 정보통신기기를 소속된 기관의 내부망 및 기관 인터넷망(제42조제1항제1호에 따른 무선랜 형태를 포함한다)에 연결하여서는 아니 되며, 내부망 및 기관 인터넷망 정보시스템을 다른 정보통신망에 연결하는 수단으로 사용하여서는 아니 된다. 분임정보보안담당관은 이에 대하여 수시로 점검하여야 한다.

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

제79조(위규자 처리) ① 시장은 「보안업무규정 시행세칙」 제46조제4항에 따라 보안사고 발생자 또는 사고의 발생을 인지하고도 보고하지 아니한 자는 징계 조치하여야 하며, 같은 세칙 제47조 및 제48조에 따라 보안감사 결과 불량하다고 지적된 책임자 및 지적된 사항은 그 지적 내용의 경중에 따라 행정조치를 취해야 한다.

② 시장은 제1항에 따른 징계조치 및 행정조치를 취할 경우 「지방공무원 징계규칙」 별표 1에 따른 징계기준 및 이 규정 별표 3 정보보안 사고(위규)자 처리기준을 적용할 수 있다

제5절 주요정보통신기반시설 보호

제80조(보호대책 수립) ① 분임정보보안담당관은 「정보통신기반 보호법」 제5조에 따른 주요정보통신기반시설을 관리할 경우 같은 법 제5조 및 같은 법 시행령 제8조에 따라 주요정보통신기반시설(이하 “주요기반시설”이라 한

다)에 대한 보호대책을 수립·시행하여야 한다.

② 분임정보보안담당관은 제1항에 따른 보호대책을 수립할 경우 다음 각 호에 해당하는 사항을 포함하고 전년도 추진실적 평가 및 개선사항을 다음 연도의 보호대책에 반영하여야 한다.

1. 소관 주요기반시설별 시스템 현황 및 기능
2. 전년도 보호업무 추진실적 및 해당 연도 추진계획
3. 취약점 분석·평가 결과 및 도출된 문제점에 대한 개선사항
4. 「정보통신기반 보호법」 제2조제2호에 따른 전자적 침해행위 예방을 위한 관리적·물리적·기술적 보안대책
5. 「정보통신기반 보호법」 제2조제3호에 따른 침해사고가 발생할 경우 대응 및 복구대책

③ 정보보안담당관은 매년 소관 주요기반시설의 지정 범위 및 기능변경 여부를 평가하여 변경사항을 보호대책에 반영하여야 한다.

④ 분임정보보안담당관은 「정보통신기반 보호법」 제5조의2에 따른 보호대책 이행여부의 확인이 필요하다고 국가정보원장이 판단하여 의뢰하는 경우 적절성 검토를 위해 사전 보호대책 등을 제출할 수 있다.

제81조(취약점 분석·평가 결과물 관리) ① 분임정보보안담당관은 「정보통신기반 보호법」 제9조제3항 각 호의 기관에 소관 주요기반시설의 취약점 분석·평가를 의뢰하고자 할 경우 정보통신망 구성도 등 중요자료의 유출 방지를 위한 보안대책을 수립·시행하여야 한다.

② 분임정보보안담당관은 제1항에 따른 취약점 분석·평가를 완료한 경우 취약점 분석·평가 결과물에 대하여 적절성을 검증하여야 한다.

③ 분임정보보안담당관은 제2항에 따른 취약점 분석·평가 결과물을 중요성 및 가치의 정도를 평가하여 비밀 또는 비공개 대상 정보로 지정·관리하고 인터넷·학회지 등 외부에 공개하거나 발표하여서는 아니 된다. 다만, 기술 교류나 학문 연구 등을 목적으로 하는 비공개 회의 등의 경우에는 자체 보안성 검토 후 발표할 수 있다.

④ 분임정보보안담당관은 취약점 분석·평가의 효율적인 수행을 위하여 필요한 경우 국가정보원장에게 평가 방향 및 중점사항, 평가 결과물의 적절성 검증, 취약점 분석·평가기관 보안점검 등의 지원을 요청할 수 있다.

제4장 융합 보안

제1절 정보통신시설 및 기기 보호

제82조(정보통신시설 보호대책) ① 분임정보보안담당관은 다음 각 호의 어느 하나에 해당하는 정보통신시설 및 장소를 「보안업무규정」 제34조에 따른 보호지역으로 지정·관리하여야 한다.

1. 암호실·정보통신실
2. 통합데이터센터
3. 암호자재 개발·설치 및 정비 장소
4. 국가비상통신 등 중요통신망의 교환국, 회선집중국 또는 중계국
5. 보안관제센터, 백업센터 및 중요 정보통신시설을 집중 제어하는 국소
6. 그 밖에 보안관리가 필요하다고 인정되는 정보시스템 설치장소

② 분임정보보안담당관은 제1항에 따라 보호지역으로 지정된 정보통신시설 및 장소에 대한 보안대책을 수립하고자 할 경우 다음 각 호에 해당하는 사항을 포함하여야 한다.

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

③ 여러 기관의 정보자원을 통합·운영하는 분임정보보안담당관은 해당 기관의 보안요구사항을 반영하여 보안대책을 수립한 후 이를 국가정보원장과 협의하여 시행하여야 한다.

제83조(정보통신실 출입관리) ① 분임정보보안담당관은 외부인이 정보통신시설을 방문할 경우 반드시 신원을 확인하고 보안교육 및 보안검색 후 출입을 허용하여야 한다.

② 분임정보보안담당관은 불가피한 경우를 제외하고는 정보통신시설에 대한 관람 및 견학은 지양하고 외국인의 출입은 금지한다. 다만, 외국인의 출입이 꼭 필요한 경우 국가정보원장과 사전 협의하여 출입을 허용할 수 있다.

제84조(영상정보처리기기 보안) ① 분임정보보안담당관은 업무상 목적으로 불특정 사람 또는 사물을 촬영한 영상을 유·무선 정보통신망으로 전송·저장·분석하는 CCTV·IP카메라·이동형 영상촬영장비·중계서버·관제서버·관리용 PC 등의 기기·장비(이하 “영상정보처리기기”이라 한다)를 설치·운영하고자 할 경우 운영자의 계정·비밀번호 설정 등 인증대책을 수립하고 특정 IP주소에서만 접속 허용 등 비(非)인가자 접근 통제대책을 수립·시행하여야 한다.

② 분임정보보안담당관은 영상정보처리기기를 통합·운영하는 시설(이하 “영상관제상황실”이라 한다)을 운영하고자 할 경우 영상관제상황실을 「보안업무규정」 제34조제2항에 따른 제한구역 또는 통제구역으로 지정·관리하고 출입통제 장치를 운용하여야 한다. 다만, 단순 시설물 관리를 위하여 운영하는 경우에는 출입통제장치만으로 운영 할 수 있다.

③ 영상정보처리기기 관리자는 영상정보처리기기를 인터넷과 분리·운영하여야 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 「국가 공공기관 영상정보 처리기기 도입·운영 가이드라인」 및 「안전한 정보통신 환경 구현을 위한 네트워크 구축 가이드라인」을 준수하여야 한다.

제85조(RFID 보안) ① 분임정보보안담당관은 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 호

의 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.

제86조(디지털복합기 보안) ① 분임정보보안담당관은 디지털복합기(디지털복사기 등도 포함한다. 이하 “복합기”라 한다)를 설치·운영하고자 할 경우 복합기 내 저장매체가 있거나 장착이 가능한 경우 자료유출을 방지하기 위하여 자료 완전삭제 또는 디스크 암호화 기능이 탑재된 복합기를 도입하여야 한다.

② 복합기 관리자는 제1항에 따라 복합기를 설치·운영할 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 분임정보보안담당관의 입회·감독 하에 실시하고 저장매체의 무단 교체 등을 예방하여야 한다.

⑤ 복합기 관리자는 복합기를 통해 내부망과 기관 인터넷망 간 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.

제87조(재난 방지대책) ① 정보보안담당관은 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애 발생에 대비하여 정보시스템의 이중화, 백업관리 및 복구 등 종합적인 재난 방지대책을 수립·시행하여야 한다.

② 정보보안담당관은 재난 방지대책을 정기적으로 시험·검토하고 재난으로 인해 업무에 지장이 초래될 가능성에 대한 영향평가를 실시하여야 한다.

③ 정보보안담당관은 정보통신망의 장애 발생에 대비하여 정보시스템 백업시설을 확보하고 정기적으로 백업을 실시하여야 한다.

④ 정보보안담당관은 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

제88조(대도청 측정) ① 정보보안담당관은 다음 각 호의 어느 하나에 해당하는 시설·장소에 대하여 각종 수단에 의한 도청으로부터 정보유출을 방지하기 위한 정책 또는 계획 수립 등 관리적 보안대책, 도청을 예방 또는 탐지·발견할 수 있는 물리적·기술적 보안대책을 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 정보보안담당관은 제1항에 따른 시설·장소에 대하여 자체 또는 「통신비밀보호법」 제10조의3에 따른 불법감청설비탐지업자 활용 등을 통해 대도청

측정을 실시하여야 한다. 다만, 다음 각 호에 해당하는 시설·장소에 대하여는 국가정보원장에게 대도청 측정을 요청할 수 있다.

1. 국가기관의 장 또는 도지사가 관리하는 시설·장소
2. 시장이 관리하는 시설·장소 중에서 도지사가 국가안보 및 국익 보호를 위하여 필요하다고 판단하는 시설·장소
- ③ 제2항에 따라 자체 또는 불법감청설비탐지업자 등을 활용하여 측정을 실시한 결과 취약요인이 발견된 경우 그 결과를 도지사를 거쳐 국가정보원장에게 통보하여야 하고 기술 지원 및 추가 측정을 요청할 수 있다.
- ④ 제2항에 따라 국가정보원장이 측정을 실시한 결과 취약요인이 발견된 경우 정보보안담당관은 개선대책을 수립·시행하여야 한다.
- ⑤ 정보보안담당관은 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.

제89조(무선통신망 보안) ① 정보보안담당관은 무선통신망(제42조에 따른 무선랜(WiFi)을 제외한다. 이하 본 조에서 같다)을 구축·운영하거나 이동통신망을 이용하여 관련 시스템을 구축·운용할 경우와 무선국을 관리할 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 전파월경 등 통신보안 준수
4. 접경지역에 설치된 전파 차단시설 점검
- ② 정보보안담당관은 제1항에 따른 무선통신망 구축·운영 또는 이동통신망을 이용하여 관련 시스템을 구축·운용할 경우와 무선국을 관리할 경우 연간 전파측정 계획을 수립하여 연1회 이상 전파측정을 실시하여야 한다.
- ③ 정보보안담당관은 제2항에 따른 연간 전파측정 계획서를 매년 1. 25.까지 국가정보원장에게 제출하고 측정·점검 후 20일 이내에 별지 제4호서식에 따른 결과보고서를 제출하여야 한다.

제90조(고출력 전자파 보안) ① 분임정보보안담당관은 소관 주요기반시설을 고출력 전자파(EMP)로부터 안전하게 보호하기 위한 예방·백업·복구 등 물리적·기술적 대책을 포함한 보호대책을 수립·시행하여야 한다.

② 분임정보보안담당관은 제1항에 따른 보호대책을 수립하기 위하여 취약점 분석·평가를 실시할 수 있으며 이를 위하여 담당자 지정 또는 전담반을 구성할 수 있다.

③ 분임정보보안담당관은 제1항에 따른 보호대책을 수립할 경우 국가정보원장에게 기술 지원을 요청할 수 있다.

제5장 훈련 및 평가

제1절 훈련 및 진단

제91조(사이버공격 대응훈련) 정보보안담당관은 「사이버안보 업무규정」 제11조에 따라 매년 대응훈련을 실시 해야하고, 분임정보보안담당관에 대하여 대응훈련 및 시정조치가 원활히 이루어질 수 있도록 지도·감독하여야 한다.

제92조(정보통신망 보안진단) ① 정보보안담당관은 「사이버안보 업무규정」 제12조제1항에 따른 진단·점검 또는 그 밖의 법규에 따라 정보통신망 보안진단·점검을 실시할 경우, 국가정보원장이 배포하는 다음 각 호의 가이드라인 등을 참고하여야 하며, 이에 필요한 관련예산 확보 등을 위하여 노력하여야 한다.

1. 사이버보안 강화를 위한 길라잡이(정보통신시스템 보안진단 및 대응방법)
2. 홈페이지·네트워크·시스템·DBMS 취약점 점검매뉴얼
3. 정보보안점검 체크리스트

② 정보보안담당관은 국가정보원장이 정보통신망 안전성을 확인하기 위하여 다음 각 호에 따른 보안진단을 실시할 경우 이에 응해야 한다.

1. 「사이버안보 업무규정」 제9조제1항 후단에 따른 보안성 검토 결과의 이행 여부 확인 또는 같은 조 제5항에 따른 보안컨설팅을 수행하는 경우
2. 「전자정부법」 제56조제3항 및 「공공기록물 관리에 관한 법률 시행령」 제5

- 조 등에 따른 보안조치 이행여부를 확인하고자 하는 경우
- 3. 「보안업무규정」 제35조에 따른 보안측정을 실시하는 경우
- 4. 시장이 정보통신망에 대한 보안취약점 점검 또는 종합진단이 필요하다고 판단하여 요청하는 경우
- 5. 그 밖에 국가정보원장이 국가안보상 필요하다고 판단하는 경우

제93조(취약 정보통신제품의 긴급 대체) 「국가 정보보안 기본지침」 제97조의3제1항에 따라 국가정보원장이 운용중지를 요청한 경우 분임정보보안담당관은 가능한 예산 범위에서 지체없이 운용을 중단하고 동일 성능의 정보통신 제품을 도입하여 대체해야 한다.

제2절 정보보안 관리실태 평가

제94조(평가 실시) ① 정보보안담당관은 도지사가 「사이버안보 업무규정」 제13조, 「전자정부법」 제56조 및 같은 법 시행령 제69조·제70조, 「공공기록물 관리에 관한 법률 시행령」 제5조 등에 따라 정보보안 관리실태에 대한 평가를 실시할 경우 이에 응해야 한다.

② 정보보안담당관은 제1항에 따라 도지사가 매년 평가대상·일정·지표 등을 정하여 통보할 경우 분임정보보안담당관에게 통보하여야 한다.

제95조(자체 평가) ① 정보보안담당관은 제94조제2항에 따른 도지사가 배포한 평가지표에 따라 자체평가를 실시하여야 한다.

② 정보보안담당관은 자체 평가의 적절성을 입증하기 위하여 필요하다고 판단하는 경우 평가지표별 증빙자료를 도지사에게 제출할 수 있다.

제96조(현장 실사) ① 정보보안담당관은 도지사가 정보보안 관리실태 평가에 대한 객관성·공정성 확보 등을 위하여 정보보안 관리실태를 검증(이하 “현장 실사”라 한다)하고자 할 경우 이에 응하여야 한다.

② 정보보안담당관은 도지사가 현장 실사를 효율적으로 수행하기 위하여 자체 평가에 대한 증빙자료 제출, 담당자 면담 등을 요청할 경우 이에 응하여야 한다.

③ 정보보안담당관은 도지사가 현장 실사를 할 경우 다음 각 호에 해당하는

사항에 협조하여야 한다.

1. 사이버위기 대응능력 점검
 2. 정보통신망 및 정보시스템 보안진단
 3. PC 등 단말기·휴대용 저장매체 보안관리 실태 확인
 4. 공무원 등의 정보보안 기본수칙 숙지여부 확인 등
- ④ 정보보안담당관은 도지사가 현장실사를 종료한 경우 제출한 자료를 반납 받아야 한다. 다만, 필요한 경우 사본 1부를 제출할 수 있다.

제97조(평가결과 통보) 정보보안담당관은 도지사로부터 정보보안 관리실태 평가 결과를 통보받은 경우 평가 결과에 따른 미비점을 개선·보완하여 정보보안 수준을 제고하여야 한다.

제6장 암호자재 및 암호알고리즘

제1절 기본사항

- 제98조(사용 원칙) ① 정보보안담당관은 비밀을 소통·보호하고자 할 경우 국가정보원장이 개발하거나 안전성을 확인한 암호자재를 사용하여야 한다. 또한 비밀이 아닌 중요자료를 보호하고자 할 경우에도 암호자재를 사용할 수 있다.
- ② 정보보안담당관은 제1항에 따라 암호자재를 사용하고자 할 경우 국가정보원장에게 제108조에 따라 암호자재 지원을 요청하여야 한다. 다만, 암호장비의 경우에는 제109조에 따라 암호장비 사용 승인을 요청하여야 한다.
- ③ 정보보안담당관은 국가정보원장이 승인하지 아니한 암호자재나 외국에서 생산된 암호기능 탑재 시스템을 무단으로 사용하여서는 아니 된다.

- 제99조(취급인가자 지정) ① 정보보안담당관은 암호자재를 개발·배부·운용·반납 등 취급하는 인원을 암호자재 취급인가자(이하 “암호취급자”라 한다)로 지정·관리하여야 한다.
- ② 제1항에 따른 암호취급자는 대한민국 국적 소유자로서 비밀취급 인가자에 한하여 「보안업무규정」 제9조에 따른 암호자재 취급 인가권자에 의하여 지정된다.

③ 정보보안담당관은 별지 제5호서식에 따라 암호취급자 현황을 관리하여야 한다.

제100조(정·부책임자 운영) 정보보안담당관은 각 암호자재에 대하여 운용·관리를 담당하는 정·부책임자 및 실무 담당자를 임명하여야 한다.

제101조(암호자재 설치·운영 장소) ① 정보보안담당관은 「보안업무규정」 제34조 제2항에 따른 통제구역으로 지정된 장소에서 암호자재를 설치·운영하여야 한다. 다만, I·II급 비밀 소통용 암호자재 중 국가정보원장이 지정한 암호자재는 제102조에 따른 암호실에서 설치·운용하여야 한다.

② 정보보안담당관은 제1항에도 불구하고 국가정보원장과 사전 협의를 거쳐 승인된 장소 및 운영방식에 따라 암호자재를 설치·운영할 수 있다.

제102조(암호실 관리) ① 정보보안담당관은 암호실을 「보안업무규정」 제34조 제2항에 따른 통제구역으로 지정하여야 하며 암호취급자 및 국가정보원장이 인가한 자 이외에는 암호실 출입을 허용하여서는 아니 된다.

② 정보보안담당관은 별지 제5호서식에 따른 암호실 및 암호취급자 현황 및 별지 제11호서식에 따른 암호실 출입자 기록부에 따라 암호실 출입을 통제하고 그 내용을 기록·유지하여야 한다.

③ 정보보안담당관은 암호실에 출입제한표시 이외의 암호취급을 나타내는 어떠한 표시도 하여서는 아니 되며 무장 경비원을 두어 암호실을 경비하여야 한다. 다만, 무장 경비원을 둘 수 없을 경우에는 이에 준하는 보안대책을 수립·시행하여야 한다.

④ 정보보안담당관은 연1회 이상 암호실에 대한 보안점검을 실시하여야 한다. 이 경우 국가정보원장에게 지원을 요청할 수 있다.

⑤ 정보보안담당관은 암호실을 자체 절차에 따라 폐쇄할 수 있다. 이 경우 암호실 폐쇄로 인하여 더 이상 사용하지 않는 암호자재는 즉시 배부기관의 장에게 반납하여야 한다.

⑥ 정보보안담당관은 암호실을 설치하거나 폐쇄한 경우 그 내용을 국가정보원장에게 통보하여야 한다.

제103조(암호문 관리) ① 정보보안담당관은 암호문을 평문과 분리 보관하여야 한다.

② 정보보안담당관은 동일 내용을 암호문과 평문으로 이중 송신하거나 암호

문을 전송한 후 이를 다시 평문으로 문의하는 등 암호문과 평문을 혼용하여서는 아니 된다.

제104조(제공 및 반출) ① 정보보안담당관은 어떠한 경우에도 암호자재를 복제·복사하거나 다른 기관이나 개인에게 임의로 대여하여서는 아니 된다.

② 정보보안담당관은 암호자재를 외국인·외국기관(주한 외국인·외교공관 및 외국군을 포함한다)에 제공하거나 외국으로 무단 반출하여서는 아니 된다. 다만, 불가피한 경우 국가정보원장에게 사전 승인을 받은 후 제공하거나 반출할 수 있다.

제105조(관련사항 공개 및 토의) ① 정보보안담당관은 암호자재와 관련한 사항을 비(非)인가자에게 공개하거나 공개된 장소에서 토의하여서는 아니 된다.

② 정보보안담당관은 암호자재와 관련한 사항을 학술·논문지, 간행물, 전시회 또는 공개된 정보통신망 등을 통해 공개하여서는 아니 된다.

③ 정보보안담당관은 제1항 및 제2항에도 불구하고 관련사항 공개나 토의가 필요한 경우에는 국가정보원장에게 사전 승인을 받은 후 참석자들로 하여금 별지 제6호서식에 따른 서약서 징구 등 보안조치를 실시하여야 한다.

제106조(관련문서 생산·제출) ① 정보보안담당관은 암호자재의 사용승인 및 지원, 운용관리 등에 관한 문서를 생산하고자 할 경우 「보안업무규정 시행규칙」 제17조에 따른 기본분류지침표에 따라 Ⅲ급 비밀로 생산하여야 한다. 다만, I·Ⅱ급 비밀로 분류된 내용이 포함될 경우 I·Ⅱ급 비밀로 생산할 수 있다.

② 정보보안담당관은 암호자재 및 암호알고리즘과 관련한 문서를 국가정보원장에게 제출하고자 할 경우 도지사를 거쳐 제출하여야 한다.

제2절 개발 및 제작

제107조(개발 및 제작) ① 정보보안담당관은 국가정보원장이 필요하다고 인정하는 경우 Ⅲ급 비밀 소통용 암호자재에 대하여 자체적으로 개발·제작할 수 있다.

② 정보보안담당관 신규 암호자재의 개발 또는 기존 암호자재의 성능개선 등

이 필요하다고 판단하는 경우 국가정보원장에게 개발 또는 성능 개선을 요청할 수 있다.

③ 정보보안담당관은 제1항에 따라 III급 비밀 소통용 암호자재를 자체적으로 개발·제작할 경우 사전에 다음 각 호의 사항을 포함한 개발 계획을 국가정보원장에게 제출하여야 한다.

1. 필요성
2. 용도 및 보호대상
3. 개발 계획 및 추진 일정
4. 개발 관련 보안대책

④ 정보보안담당관은 제3항에 따라 암호자재를 자체적으로 개발할 경우 최종 완료 이전에 다음 각 호의 사항을 포함한 개발 결과를 국가정보원장에게 제출하여 안전성 확인 및 승인을 받아야 한다. 국가정보원장이 안전성을 확인한 결과 미비점이 발견된 경우 정보보안담당관은 이를 개선 조치하여야 한다.

1. 암호자재 명칭
2. 개발 업체
3. 암호알고리즘
4. 설계서 및 소스코드
5. 그 밖에 국가정보원장이 요청하는 자료

⑤ 정보보안담당관은 제4항에 따라 III급 비밀 소통용 암호자재를 개발 완료하거나 개발된 암호자재를 변경하는 경우 국가정보원장에게 해당 결과물을 제출하여야 한다.

⑥ 기타 암호자재의 개발 및 제작과 관련한 절차는 「보안업무규정」 제7조 및 국가정보원장이 배포한 「국가보안기술 연구개발 지침」을 준수하여야 한다.

제3절 지원요청 및 사용승인

제108조(암호자재 지원 요청) ① 정보보안담당관은 국가정보원장이 제작·지원하는 암호자재가 필요할 경우 다음 각 호의 사항을 포함한 문서를 제출하

고 지원을 요청할 수 있다.

1. 사용목적 및 보호대상
2. 암호자재 종류 및 명칭
3. 소요량 및 산출근거
4. 사용기간 및 장소
5. 사용(운용)자 직책·성명
6. 보안대책

② 정보보안담당관은 국가정보원장이 제작·지원하는 암호자재를 매년 반복하여 지원받는 경우 별지 제8호서식에 따른 암호자재 신청서를 매년 1.25.까지 국가정보원장에게 제출하여야 한다. 이 경우 제1항의 절차를 생략할 수 있다.

제109조(암호장비 사용 승인) ① 정보보안담당관은 암호자재 제작업체로부터 암호자재를 구입하여 사용하고자 할 경우 다음 각 호의 사항을 포함한 문서를 국가정보원장에게 제출하고 사용 승인을 받아야 한다.

1. 사용목적 및 보호대상
2. 암호장비 종류 및 명칭
3. 소요량 및 산출근거
4. 설치장소, 사용(운용)자 직책·성명
5. 정보통신시스템 제원
6. 정보통신망 구성도
7. 보안대책

② 정보보안담당관은 제1항에 따라 암호장비 사용 승인을 받은 이후 암호자재 사용목적 및 보호대상 변경 등 변동사항이 발생할 경우 국가정보원장에게 변경사용 승인을 받아야 하며 승인받은 후 6개월 이내에 설치하지 아니할 경우 관련내용을 국가정보원장에게 통보하여야 한다.

③ 정보보안담당관은 제1항 및 제2항에 따른 암호장비를 이용한 응용시스템을 개발하고자 할 경우 국가정보원장이 개발한 암호응용프로그램 인터페이스를 적용하여야 하며 연동되는 부분에 대해서는 안전성을 확인한 후 운용하여야 한다.

제110조(검사) 정보보안담당관은 제109조에 따라 암호자재를 도입하는 과정에

서 검사가 필요할 경우 시장의 책임 하에 실시할 수 있다. 다만, 암호처리부에 대한 검사는 국가정보원장에게 요청하여야 한다.

제111조(외국산 암호자재·장비 사용) ① 정보보안담당관은 외국기관 또는 외국군(軍)과의 통신을 위하여 외국산 암호자재·장비를 사용하고자 할 경우 사전 국가정보원장과 추진 경위·현황 및 보안대책에 대하여 협의하여야 한다.

② 제1항에 따라 외국산 암호자재·장비를 설치·사용할 경우 해당 국가와의 협정에 따라 시장 책임 하에 운용·관리한다.

제112조(목적 외 사용금지) 정보보안담당관은 제108조 및 제109에 따라 암호자재·장비를 사용할 경우 국가정보원장이 지원하거나 사용 승인한 목적 이외 교육·시험 등 다른 목적으로 사용하여서는 아니 된다. 다만, 국가정보원장이 필요하다고 인정하는 경우에는 그러하지 아니할 수 있다.

제4절 운용 및 관리

제113조(운용 및 관리) ① 정보보안담당관은 암호자재를 운용할 경우 다음 각 호의 사항을 준수하여 운영 및 관리하여야 한다.

1. 「보안업무규정 시행규칙」 제5조제2항 및 같은 규칙 별지 제3호서식에 따른 암호자재 관리기록부의 기록·유지
2. 「보안업무규정 시행규칙」 제5조제5항에 따른 주1회 점검 및 같은 규칙 별지 제4호서식에 따른 암호자재 점검기록부 기록·유지와 월 1회 확인
3. 이 규정 별지 제9호서식에 따른 지편자재 사용기록부의 기록·유지
4. 암호자재를 배부·반납 등 취급할 경우에는 「보안업무규정 시행규칙」 제4조제4항 및 같은 규칙 별지 제2호서식에 따른 암호자재 증명서 작성

② 정보보안담당관은 제1항에 따른 기록부 및 증명서를 다음 각 호에 따라 보관하여야 한다.

1. 암호자재 관리기록부 : 새로운 관리부철로 옮겨서 관리할 경우, 기존 관리부철 5년간 보관
2. 암호자재 점검기록부 : 최근 5년간 점검기록 보관
3. 지편자재 사용기록부 및 암호자재 증명서 : 해당 암호자재를 반납하거나

과기한 후 5년간 보관

- ③ 정보보안담당관은 암호자재 외부에 운용상의 기능, 형식승인 번호, 기관번호 및 일련번호를 제외한 어떠한 표지도 하여서는 아니 된다. 다만, 암호자재가 다른 장비에 내장되어 오인 파기나 관리 소홀이 우려되는 경우 경고 문구 등 표지를 부착할 수 있다.
- ④ 정보보안담당관은 암호자재의 암호체계 및 키 운용체계와 관련된 문서와 암호자재의 고유명칭, 제원, 대상국소 및 수량 등 운용 현황이 기록된 문서를 비밀로 분류·관리하여야 한다.
- ⑤ 정보보안담당관은 암호자재를 업무 시간에 사용 가능하도록 별도 관리하되 업무 종료 이후에는 이중 캐비닛 또는 금고에 보관하여야 한다. 다만, 국가정보원장과 사전 협의를 통해 승인된 장소 및 운영 방식에 따라 설치·운영하는 암호자재는 그러하지 아니할 수 있다.
- ⑥ 정보보안담당관은 암호자재를 보관함에 보관할 경우 암호자재 이외의 비밀 또는 문건을 혼합 보관하여서는 아니 되며 현용 암호자재는 예비용 및 운용 기간이 만료된 암호자재와 구분·보관하여야 한다.

제114조(기록부 등의 전자적 관리) ① 정보보안담당관은 제113조제1항에 따른 각종 기록부 및 증명서를 전자적 방법으로 작성·관리할 수 있으며, 이를 위하여 관리시스템을 구축·운영할 수 있다.

② 정보보안담당관은 제1항에 따라 기록부 및 증명서를 전자적 방법으로 관리할 경우 내용의 위조·변조·훼손 및 유출 등을 방지하기 위하여 암호화 등 보안대책을 수립·시행하여야 한다.

③ 정보보안담당관은 국가정보원장이 「보안업무규정」 제3조의2에 따라 제2항에 따른 보안대책의 적절성을 확인할 경우 이에 응하여야 한다.

제115조(배부·반납 및 운반) ① 정보보안담당관은 암호자재를 배부·반납할 경우 암호취급자가 직접 취급하도록 하여야 한다. 다만, 부득이한 경우 국가정보원장이 지정하는 방법으로 배부·반납할 수 있다.

② 정보보안담당관은 암호취급자가 직접 배부·반납할 수 없을 경우 비밀취급 인가자 중 정책임자의 위임장을 소지한 자에게 이를 대행하게 할 수 있다.

③ 정보보안담당관은 암호자재를 운반·전시 등을 하고자 할 경우 분실·피탈 등을 방지하기 위한 보안대책을 수립·시행하여야 한다.

- ④ 암호취급자는 암호자재를 배부·반납하고자 할 경우 암호자재 증명서 2부를 작성하여 배부(반납)자 및 수령자가 각각 서명한 후 1부씩 보관하여야 한다.
- ⑤ 암호자재 배부(반납)자 및 수령자는 암호자재 증명서상의 명칭·수량·등록번호 등이 실물과 일치하는지를 반드시 확인하여야 한다.
- ⑥ 정보보안담당관은 암호자재의 운반·전시 도중 보호조치가 필요할 경우가 가까운 경찰서나 군(軍)부대에 지원을 요청할 수 있다.
- ⑦ 정보보안담당관은 암호자재의 운반·전시 도중 사고가 발생한 경우 즉시 국가정보원장에게 통보하여 필요한 조치를 취할 수 있도록 하여야 한다.

제116조(변경 사용) ① 암호자재를 제작한 기관의 장은 정기적인 교체, 사고 발생 등의 사유로 예비용 암호자재를 현용으로 변경·사용하고자 할 경우 관련내용을 Ⅲ급 비밀로 작성하여 해당 암호자재를 사용하는 정보보안담당관에게 통보하여야 한다.

- ② 제1항에 따라 변경 내용을 통보 받은 경우 해당 암호자재를 사용하는 부서 및 소속·산하기관에 신속히 전달하고 운용 기간이 만료된 암호자재는 정보보안담당관을 거쳐 제작기관의 장에게 반납하여야 한다.

제117조(인계인수) ① 분임정보보안담당관은 암호자재를 운용·관리하는 정·부책임자 및 실무 담당자를 교체할 경우 다음 각 호의 사항을 포함한 운용 현황에 대하여 인계인수를 실시하여야 하며 암호자재 관리기록부의 최종 기록 여백에 인계인수 사항을 기록·유지하여야 한다

- 1. 암호자재 종류 및 수량
- 2. 납봉 또는 봉인표지 이상(異常) 유무
- 3. 암호자재 정상 작동여부
- 4. 암호자재 운용법 등 관련자료 이상(異常) 유무

② 분임정보보안담당관은 암호자재를 운용·관리하는 정·부책임자 및 실무 담당자가 1개월 이상 직무를 수행할 수 없을 경우 암호취급자 중에서 그 직무를 대행할 정·부책임자 및 실무 담당자를 별도로 지정하고 제1항에 따른 인계인수를 실시하여야 한다..

③ 제1항 및 제2항에 따른 인계인수 관련 사항은 분임정보보안담당관 또는 정보보안담당관이 확인하여야 한다.

제118조(운용현황 통보) 정보보안담당관은 별지 제10호서식에 따른 암호자재 운용관리 현황을 작성하여 매년 1.25까지 국가정보원장에게 제출하여야 한다.

제119조(운용관리실태 점검) ① 정보보안담당관은 국가정보원장이 각급기관의 암호자재 운용·관리실태에 대하여 정기 또는 수시로 점검할 경우 이에 응해야 한다.

② 정보보안담당관은 국가정보원장이 제1항에 따라 점검한 결과를 통보할 경우 취약요인에 대하여 개선 조치하여야 한다.

③ 정보보안담당관은 국가정보원장이 암호자재 운용취약성 점검이 필요하다고 판단하여 해당 기관 책임 하에 자체 점검을 실시하도록 요청할 경우 이에 응해야 한다.

④ 정보보안담당관은 국가정보원장이 제3항에 따른 점검결과에 따라 개선이 필요하다고 판단하여 개선 조치를 요청할 경우 이에 응하여야 한다. 이 경우 정보보안담당관은 특별한 사유가 없는 한 개선 조치하여야 하며 국가정보원장이 그 이행여부를 확인할 경우 이에 응하여야 한다.

⑤ 정보보안담당관은 국가정보원장이 운용취약성 점검을 수행하는데 필요한 가이드라인을 배부할 경우 이를 활용할 수 있다.

⑥ 정보보안담당관은 제3항에도 불구하고 국가정보원장에게 합동점검을 요청하여 지원 받을 수 있다.

제120조(사고발생 시 조치) 정보보안담당관은 암호자재의 분실·유출 및 오인 파기 등 사고 발생을 알게 된 경우 관련사실을 즉시 국가정보원장에게 통보하여 암호자재 사용 중지 등 조치방법을 지원받아야 한다.

제5절 정비 및 파기

제121조(정비) ① 정보보안담당관은 암호자재를 정비하고자 할 경우 암호자재 제작업체를 통해 정비하여야 한다. 다만, 국가정보원장이 제작·지원한 암호자재의 경우 예비용 암호자재로 교체하거나 국가정보원장에게 교체를 요청하여야 한다.

② 정보보안담당관은 암호자재 중에서 암호처리부가 아닌 일반 부분에 대하

여는 자체적으로 정비할 수 있다. 이 경우 다음 각 호의 사항을 포함한 보안 대책을 수립·시행하여야 한다.

1. 정비 장소는 「보안업무규정」 제34조제2항에 따른 통제구역으로 지정
2. 암호취급자에 의한 정비 실시
3. 자체 정비절차 수립

제122조(파기) ① 정보보안담당관은 암호자재 운용이 불필요하거나 폐기하고자 할 경우 자체 파기하지 아니하고 암호자재 제작기관의 장 또는 국가정보원장에게 반납하여야 한다.

② 정보보안담당관은 제1항에도 불구하고 자체 파기를 하고자 할 경우 다음 각 호의 사항을 포함한 문서를 국가정보원장에게 제출하고 승인을 받은 후 파기할 수 있다.

1. 파기일시 및 장소
2. 암호자재의 명칭·수량 및 등록번호
3. 파기사유 및 방법
4. 파기자 및 참여자의 직위(직급)·성명

③ 정보보안담당관은 제2항에 따라 암호자재를 자체 파기할 경우 각 파기대상 암호자재의 실물사진, 안전한 이송, 완전한 유희여부 확인 등 파기 전(全) 과정을 채증하여 국가정보원장에게 통보하여야 한다. 이 경우 정보보안담당관은 도지사를 거쳐 통보하여야 한다.

④ 정보보안담당관은 긴급사태 발생 등 사유로 암호자재를 안전하게 관리할 수 없을 경우 「보안업무규정 시행규칙」 제7조에 따라 긴급 파기할 수 있다. 이를 위하여 다음 각 호의 사항을 포함한 긴급파기 계획을 평상시 수립하여야 한다.

1. 긴급파기 지시 전달체계
2. 파기 담당관 및 채증 담당관
3. 암호자재별 반드시 파기하여야 할 부품 또는 위치·방법

제6절 암호알고리즘

제123조(개발 및 지원요청) ① 정보보안담당관은 비밀이 아닌 업무자료를 암호화하여 소통·보호하고자 할 경우 국가정보원장이 개발하거나 안전성을 확인한 암호알고리즘 또는 검증필 암호모듈을 사용하여야 한다. 다만, 필요한 경우 국가정보원장의 승인 하에 자체적으로 개발·사용할 수 있다.

② 정보보안담당관은 암호알고리즘이 필요한 경우 다음 각 호의 사항을 포함한 문서를 국가정보원장에게 제출하고 지원을 요청할 수 있다. 이 경우 정보보안담당관은 도지사를 거쳐 요청하여야 한다.

1. 사용 목적
2. 정보통신시스템 구성도, 기능 및 제원
3. 암호키 운용관리 방식
4. 개발 고려사항
5. 그 밖에 국가정보원장이 요청하는 자료

③ 정보보안담당관은 제1항에 따라 암호알고리즘을 자체적으로 개발·사용하고자 할 경우 다음 각 호의 사항을 포함한 문서를 국가정보원장에게 제출하여 안전성 확인 및 승인을 받아야 한다. 국가정보원장이 안전성을 확인한 결과 미비점이 발견될 경우 정보보안담당관은 이를 개선 조치하여야 한다.

1. 개발 배경 및 적용대상 시스템
2. 암호체계
3. 암호 알고리즘 소스코드 및 관련 설명서
4. 자체 안전성 평가 결과 등 관련자료
5. 그 밖에 국가정보원장이 요청하는 자료

제124조(적용 및 운용) 정보보안담당관은 제123조에 따라 국가정보원장으로부터 지원받거나 자체 개발한 암호알고리즘을 정보통신시스템 등에 적용·운용하고자 할 경우 적절한 보안대책을 수립·시행하고 운용 시험을 통한 정상 동작여부 등을 확인하여야 한다.

제125조(반납 및 파기) 정보보안담당관은 제123조에 따라 국가정보원장으로부터 지원받거나 자체 개발한 암호알고리즘의 실효성이 상실되거나 유효기간이 만료된 경우 지원받은 암호알고리즘은 국가정보원장에게 반납하고 자체 개발한 암호알고리즘은 시장 책임 하에 파기(소자)하고 그 결과를 국가정보원장에게 통보하여야 한다.

제7장 사이버위협 탐지 및 대응

제1절 보안관제

제126조(보안관제센터 설치·운영) ① 「사이버안보 업무규정」 제14조제2항에 따라 부문보안관제센터 또는 단위보안관제센터를 설치·운영하여야 하는 경우 해당 보안관제센터를 국가보안관제체계와 연계 운영하여야 한다. 이 경우 연계 방법은 국가보안관제체계를 운영하는 국가정보원장과 사전 협의하여 정한다.

② 제1항에 따라 보안관제센터를 운영하는 시장과 국가정보원장은 보안관제에 필요하다고 판단하는 경우 상호 간 기술·인력·장비 등의 지원을 요청할 수 있다.

③ 정보보안담당관은 보안관제센터 운영 시 야간시간대 근무자 관리 등을 위하여 필요하다고 판단하는 경우 관계부서의 장과 협의하여 근무자 일일 당직 보고를 실시할 수 있다.

제127조(보안관제 인원) ① 단위보안관제센터를 운영하는 경우 정보보안담당관은 보안관제업무를 24시간 중단없이 수행하여야 하며 이를 담당할 전담 또는 담당인력을 배치하고 교대근무 체계를 운영하여야 한다. 다만, 보안관제 대상의 범위 및 중요성, 보안관제센터의 규모 등을 고려하여 그러하지 아니할 수 있다.

② 「국가사이버안전관리규정」 제10조의2제4항에 따라 보안관제전문업체의 인원을 활용하고자 하는 경우 다음 각 호에 해당하는 사항을 준수하여야 한다.

1. 업체를 선정할 경우 과학기술정보통신부장관이 고시하는 「보안관제 전문기업 지정 등에 관한 공고」에 따른 업무수행능력 평가기준 등 준수
2. 보안관제업무를 책임 있는 수행 및 보안관리 등을 위하여 적정한 수의 공무원 또는 정규직원 상시 배치
3. 업체 인원에 대하여 제25조(용역업체 보안) 및 제30조(누출금지정보 유출시 조치) 준용
4. 업체 인원을 대상으로 매월 1회 이상 탐지규칙정보 관리 등에 관한 보안

교육 및 점검 실시

제128조(탐지규칙정보 개발 및 배포) ① 시장과 국가정보원장은 사이버공격을 탐지할 수 있는 기술정보(이하 “탐지규칙정보”라 한다)를 개발하여 보안관계 업무에 활용할 수 있다.

② 제1항에 따라 탐지규칙정보를 개발한 경우 해당 탐지규칙정보를 국가보안관계체계를 이용하여 다른 보안관계센터를 운영하는 기관의 장과 공유할 수 있다.

③ 국가정보원장으로부터 탐지규칙정보를 배포 받은 정보보안담당관은 이를 소속·산하기관의 장에게 다시 배포할 수 있다.

④ 정보보안담당관은 제1항에 따른 탐지규칙정보를 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따른 비공개 대상 정보 및 「국가정보자료관리규정」 제2조제1호에 따른 국가정보자료로서 취급·관리하여야 한다.

⑤ 제3항에 따라 탐지규칙정보를 배포받은 정보보안담당관은 탐지규칙정보를 다음 각 호에 해당하는 방법으로 관리하고 매월 1회 이상 보안관리 실태를 점검하여야 한다.

1. 암호화 저장·전송
2. 인터넷을 통한 평문 송·수신 금지
3. 인터넷 등 외부유출 금지
4. 탐지규칙정보 관리시스템의 원격 접속 금지

⑥ 제3항에 따라 탐지규칙정보를 배포받은 정보보안담당관은 탐지규칙정보가 유출된 경우 즉시 그 사실을 국가정보원장에게 통보하여야 한다.

제129조(공격정보 탐지·처리) ① 시장과 국가정보원장(「사이버안보 업무규정」 제14조제3항에 따라 합동으로 보안관제를 수행하는 경우를 말한다. 이하 이 절에서 같다)은 보안관계 대상기관에 대한 사이버공격에 관한 정보를 탐지·처리하여야 한다.

② 시장과 국가정보원장은 제1항의 업무를 수행하기 위하여 보안관계 대상기관의 장과 협의하여 사이버공격에 관한 정보를 실시간 탐지하는 장비[암호화된 사이버공격 패킷을 가시화(可視化)하는 장비를 포함한다]를 보안관계 대상기관의 정보통신망에 설치·운용하거나 탐지규칙정보를 제공하여 관련 정보를 실시간 처리할 수 있다.

③ 시장과 국가정보원장은 탐지한 사이버공격에 관한 정보를 보안관제 대상 기관의 장에게 실시간 제공하여야 한다.

④ 시장과 국가정보원장은 보안관제 과정에서 자동적으로 처리되는 다음 각 호의 정보를 수집·이용할 수 있다

1. 사이버공격으로 인하여 발생한 패킷
2. 공격 주체 및 피해자를 식별하기 위한 IP주소 및 MAC주소, 전자우편 주소, 정보통신서비스 이용자 계정 정보, 피해자의 성명 및 연락처
3. 그 밖에 사이버공격의 방법 및 피해 확인·식별에 필요한 정보

제130조(초동 조치) ① 정보보안담당관은 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

② 시장과 국가정보원장은 사이버공격으로 인한 피해를 최소화하기 위하여 필요한 경우 보안관제 대상기관의 장에게 피해 시스템과 사용자에 관한 정보 제공을 요청할 수 있다.

③ 행정안전부장관이 사이버공격으로 인한 피해 최소화 및 확산 방지를 위한 국가정보원장의 요청 등 필요하다고 판단하여 「전자정부법」 제56조의3에 따라 국가정보통신망의 운영을 일부 제한할 경우 정보보안담당관은 이에 응하여야 한다.

제131조(조치결과 통보) ① 제129조제3항에 따라 사이버공격에 관한 정보를 제공받은 보안관제 대상기관의 장은 제공받은 날로부터 5일 이내에 대응조치 결과를 국가정보원장 및 행정안전부장관에게 통보하여야 한다.

② 정보보안담당관은 국가정보원장이 별도로 요청한 안보위해(危害) 공격을 초동 조치한 경우 관련내용을 즉시 도지사와 국가정보원장 및 행정안전부장관에게 통보하여야 한다.

제132조(운영현황 통보) ① 제126조제1항에 따라 정보보안담당관은 별지 제12호서식에 따른 보안관제센터 운영현황을 작성하여 매년 1. 25.까지 도지사를

거쳐 국가정보원장에게 통보하여야 한다.

② 정보보안담당관은 도지사 또는 국가정보원장이 국가보안관제체계의 운영을 위하여 필요하다고 판단하여 제1항에 따른 운영현황과 관련된 추가 자료를 요청할 경우 이에 응하여야 한다.

③ 정보보안담당관은 제1항 및 제2항에 따라 작성되거나 통보받은 자료는 보안관제와 관련한 목적으로만 사용하여야 한다.

제133조(직원 교육) ① 정보보안담당관은 보안관제업무 담당직원에 대한 교육 계획을 수립·시행하여야 한다.

② 정보보안담당관은 보안관제업무 담당직원이 격년 20시간 이상 보안관제 관련 교육을 이수하도록 하여야 한다.

제2절 사고 대응

제134조(사이버공격으로 인한 사고) ① 「사이버안보 업무규정」 제16조제1항에 따라 사고조사를 실시할 경우 국가정보원장은 안보위해(危害) 공격으로 인한 사고에 대하여 조사를 실시하며, 정보보안담당관은 안보위해(危害) 공격을 제외한 사이버공격으로 인한 사고에 대하여 조사를 실시한다.

② 제1항에 따른 정보보안담당관이 사이버공격으로 인한 사고의 원인 분석 및 재발 방지를 위하여 피해 부서의 장에게 다음 각 호에 해당하는 자료 제출을 요청할 경우 이에 응해야 한다. 사이버공격으로 인하여 「보안업무규정」 제38조 및 제45조, 「보안업무규정 시행규칙」 제65조의2에 따른 조사를 실시하는 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 제2항에 따른 자료 제출을 요청받은 피해 부서의 장은 관계 법규에 저촉

되지 않는 범위 내에서 해당 자료를 제출하여야 한다.

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

⑤ 공공 전용 민간클라우드를 이용하는 부서의 장은 공공 전용(專用) 클라우드에서 사고가 발생한 경우 국가정보원장과 합동으로 조사반을 구성하여 클라우드컴퓨팅서비스제공자에 대하여 계약의 범위 내에서 자료의 보존 및 제출 요구, 현장 조사 등 필요한 조치를 취하여야 한다.

제135조(정보통신보안 규정 위반 및 자료유출 사고) ① 정보보안담당관은 국가정보원장으로부터 「보안업무규정 시행규칙」 별표 2에 따른 정보통신보안 규정 위반사항에 대한 사실을 통보받은 경우 같은 규정 시행규칙 제66조제3항에 따라 즉시 필요한 조치를 취하고 위규자, 위규 내용 및 조치 결과를 국가정보원장에게 통보하여야 한다.

② 정보보안담당관은 비밀·대외비 등 국가 기밀에 속하는 업무자료가 유출되거나 비공개 업무자료가 유출된 사고 중 「국가정보원법」 제4조제1항제1호 나목부터 마목까지와 관련된 사안일 경우 즉시 국가정보원장에게 통보하여 합동 조사를 실시하여야 한다.

③ 공무원 등의 과실로 인하여 개인 소유의 정보통신기기 및 이동통신단말기, 상용 정보통신서비스에서 제2항에 따른 유출사고가 발생한 경우, 국가정보원장이 정보보안담당관을 거쳐 해당 공무원 등에게 저장자료·이용내역 등의 자료 제출을 요청할 경우 이에 응해야 한다.

④ 공무원 등은 제3항에 따른 요청이 위법하다고 판단하는 경우 그 사유를 소명하고 자료 제출을 거부할 수 있다.

⑤ 조사 기관의 장은 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.

제136조(재발방지 조치) ① 정보보안담당관은 국가정보원장이 제134조 및 제135조에 따른 조사 결과 및 재발방지를 위한 보안조치 사항을 통보할 경우 해당 부서에 전파하여야 한다.

② 제1항에 따라 조사 결과를 통보받은 부서의 장은 관계 법규에 따른 관련자 징계, 개선대책 수립·시행 등 필요한 조치를 취하여야 한다.

제8장 정보시스템 도입 및 보안절차

제137조(시스템 도입) ① 분임정보보안담당관은 시스템 운영 전 단계에서 별지 제13호서식 정보시스템 등록/변경/폐기 신청서 및 별지 제14호서식 정보시스템 보안점검 체크리스트를 작성하고 정보보안담당관의 승인을 받는다.

② 분임정보보안담당관은 정보자산의 식별, 정보자산의 분류, 정보자산의 중요성 평가, 등급분류 등의 과정을 거쳐 별지 제3호서식 정보시스템 관리대장에 기록하여 관리한다.

③ 분임정보보안담당관은 서버 변경, 증설 등의 서버 환경 변화뿐만 아니라, 서버의 도입·불용의 대상이 있는지 모니터링 하여야 하며, 적절한 도입시기와 수요를 파악해야 한다.

④ 분임정보보안담당관은 시스템의 신·증설 등에 대하여 보안대책을 강구하고 적절성 확인을 위하여 관련 사업 계획단계에서(사업 공고 전) 제14조부터 제17조까지를 참조하여 보안성 검토를 의뢰하여야 한다.

제138조(시스템의 설치) ① 분임정보보안담당관은 시스템을 설치할 경우 다음 각 호의 사항이 만족되도록 하여야 한다.

1. 시스템은 물리적 보안이 되어 있는 제한구역 및 통제구역에 설치한다.
2. 개발시스템은 운영시스템과 별개의 시스템으로 구축하고 내부영역과 구분되는 별도의 네트워크를 구성하여 작업하여야 한다.
3. 서비스 제공 서버에서는 개발이나 테스트를 수행하지 않는다.
4. 데이터베이스는 개별사용자의 직접 접속을 차단하고 고유식별정보, 비밀번호, 바이오정보와 같은 중요정보는 암호화하는 등 데이터베이스별 보안조치를 하여야 하며, 웹DB서버는 DMZ구간과 분리하여 외부 사설존 구성 등 침입차단시스템 내부에 위치시켜 외부로부터의 접근이 차단되도록 구성하여야 한다.
5. 업무용 서버와 대민용 서버는 물리적으로 분리하여 사용한다.

② 별도의 보안 소프트웨어 설치 시 분임정보보안담당관은 정보보안담당관의 승인을 받아야 한다.

③ 시스템에는 업무용 목적으로 사용되는 프로그램 이외의 게임이나 원격접

속 등 업무적으로 불필요한 프로그램의 설치를 금한다.

④ 운영체제를 설치한 후 분임정보보안담당관은 패치 및 보안설정을 적용한다.

⑤ 외부계약에 의한 시스템관리의 경우 발생할 수 있는 데이터의 손상, 손실 등의 보안위험을 파악하고 대책을 수립하여 계약서에 반영하도록 한다.

제139조(시스템 철수 및 폐기) ① 분임정보보안담당관은 시스템 철수 및 폐기 시 별지 제13호서식 정보시스템 등록/변경/폐기 신청서를 작성하여 정보보안담당관의 승인을 받아야 한다.

② 분임정보보안담당관은 중요 시스템의 철수 및 폐기 시, 시스템 구성과 관련된 설정 및 저장정보를 완전히 삭제하고, 별지 제3호서식 정보시스템 관리대장을 갱신하여 정보보안담당관에게 결과를 보고한 후 폐기하고, 별지 제16호서식 정보시스템 폐기 관리대장에 기록한다.

제9장 정보 협력

제140조(정보협조 요청) ① 정보보안담당관은 국제 및 국가배후 해킹조직 등 사이버안보 정보의 수집·작성 및 「국가정보원법」 제5조제2항에 따른 조사를 위하여 국가정보원장이 제134조제2항 각 호의 자료 제출 및 「국가정보원법」 제5조제1항에 따라 협조와 지원을 요청할 경우 이에 응하여야 한다.

② 제1항에 따라 요청을 받은 정보보안담당관은 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.

제141조(기관 간 정보공유 협력) 정보보안담당관은 사이버공격의 예방 및 신속한 대응을 위하여 다음 각 호에 해당하는 정보(이하 “사이버위협정보”라 한다)를 기관 간 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

제142조(정보공유시스템 운영) ① 정보보안담당관은 국가정보원장이 사이버안보 정보의 배포와 각급기관·단체 간 사이버위협정보의 체계적·효율적 공유를 위하여 국가사이버위협 정보공유시스템(「사이버안보 업무규정」 제6조에 따른 정보공유시스템을 포함한다. 이하 “정보공유시스템”이라 한다)을 구축·운영할 경우 이용하기 위하여 신청할 수 있다.

② 정보보안담당관은 제1항에 따라 국가정보원장으로부터 정보공유시스템 접근권한을 부여받았을 경우 정보공유시스템에 사이버위협 관련 정보 등을 등록하거나 등록된 정보를 업무에 활용할 수 있으며 다음 각 호에 해당하는 사항을 준수하여야 한다.

1. 정보공유시스템 전용(專用) 단말기 운용
2. 정보공유시스템 접근·활용 및 단말기 운용 등을 위한 관리자 지정·운영
3. 정보시스템 개별 이용자 등록·삭제 등 접근권한 관리
4. 정보공유시스템 전용(專用) 단말기 내 정보공유시스템 이용과 무관한 소프트웨어 설치 및 비인가 휴대용 저장매체 연결 사용 금지
5. 이용기관 간 정보공유 활성화를 위하여 월 1회 이상 정보공유시스템 접속·활용
6. 기타 국가정보원장이 제시하는 보안대책

③ 정보보안담당관은 국가정보원장이 제2항 각 호의 준수여부를 점검하고 개선 조치를 권고할 경우 이에 따라야 한다.

제143조(정보공유시스템의 정보 관리) ① 정보보안담당관은 정보공유시스템에 등록된 정보를 「공공기관의 정보공개에 관한 법률」 제9조제1항에 따른 비공개 대상 정보 및 「국가정보자료관리규정」 제2조제1호에 따른 국가정보자료로서 취급·관리함을 원칙으로 한다.

② 정보보안담당관은 정보공유시스템에 사이버위협 정보를 등록할 경우 보안성·민감성 등을 고려하여 열람권한 및 보안등급을 부여할 수 있다.

제10장 보칙

제144조(지방출자·출연기관 지도·감독) ① 정보보안담당관은 「지방공기업법」 제5조 및 「지방자치단체 출자·출연 기관의 운영에 관한 법률」 제2조에 적용을 받는 지방공사와 지방공단, 출자·출연기관에 대하여 같은 법 제25조 및 「광명시 출자·출연 기관의 운영에 관한 조례」의 범위 내에서 이 규정의 내용을 참고하여 정보보안업무를 지도·감독하여야 한다.

② 정보보안담당관은 제1항에 따른 시 산하 지방공사와 지방공단, 출자·출연기관이 「국가 정보보안 기본지침」의 내용을 참고하여 해당 기관의 지침을 제·개정할 수 있도록 지도하여야 한다. 다만, 해당기관이 「국가 정보보안 기본지침」 제7조제1항에 따라 시가 정한 지침을 준용하는 경우 별도로 제정하지 아니할 수 있다.

제145조(서약서 징구 시 고지 사항) 정보보안담당관은 이 규정에 따라 서약서를 징구·집행하는 대상자에게 다음 각 호의 어느 하나에 해당하는 경우에는 비밀·보안준수의무를 위반하지 아니하는 것으로 본다는 점을 알리기 위하여 노력하여야 한다.

1. 「부패방지 및 국민권익위원회의 설치와 운영에 관한 법률」 제55조, 제66조제3항 및 제67조에 따른 부패행위 신고 또는 공직자 행동강령 위반행위 신고
2. 「공익신고자 보호법」 제6조, 제14조제4항에 따른 공익신고

제146조(재검토 기한) 시장은 「훈령·예규 등의 발령 및 관리에 관한 규정」을 준용하여 이 규정에 대하여 최종 개정일로부터 매 3년이 되는 날이 되기 전까지 개정 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙 <2022. 7. 28 훈령 제429호 전부개정>

이 규정은 발령한 날부터 시행한다.

부칙 <2023. 7. 31 훈령 제436호>

이 규정은 발령한 날부터 시행한다.

[별표 1]

‘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(국가용 보호프로파일 준수)	
DB 암호화제품		
문서 암호화제품(DRM 등)		

※ 최신 도입요건은 국가정보원 홈페이지(암호모듈 검증) 참조

[별표 2]

보안적합성 검증 신청 시 제출물

1. 최초검증 신청 시 제출물

제출물	정보보호시스템		작성 주체
	상용 제품	자체(용역) 개발	
[서식 제1호]에 따른 보안적합성 검증 신청서	○	○	신청기관
[서식 제2호]에 따른 정보통신제품 도입확인서(현황)	○	○	
기술제안요청서 사본	○	○	
보안기능 점검표	○	○	
운용점검사항	○	○	
CC인증서 사본	○ (인증서 보유시)		업체
보안기능 운용 설명서	○	○	
기본 및 상세 설계서		○	
개발완료 보고서		○	

2. 재검증 신청 시 제출물

제출물	정보보호시스템		작성 주체
	상용 제품	자체(용역) 개발	
[서식 제1호]에 따른 보안적합성 검증 신청서	○	○	신청기관
[서식 제2호]에 따른 정보통신제품 도입확인서(현황)	○	○	
보안기능 점검표	○	○	
운용점검사항	○	○	
변경내용 분석서	○	○	업체

[별표 3]

정보보안 사고(위규)자 처리기준

□ 처리기준 정의

- 중 대 : 징계 위원회에 회부하여 『지방공무원 징계규칙』에 따라 처벌
- 보 통 : 서면 또는 구두 주의 경고 2회 이상 반복 발생 또는 정보보안 규정 위반 발생 시 피해 정도가 심각하지 않으나 재발 방지를 위한 경우 특별 보안교육을 실시하고 부서장 결재 사유서 제출
- 경 미 : 단순착오, 경미한 위반행위(최초 1회) 서면 또는 구두 주의 경고

항 목	구 분	위 반 내 용		처 리 기 준		
				중대	보통	경미
비밀/대외비 누설		적법한 절차에 의하지 않고 비밀/대외비 타인에게 제공·누설		○		
		비밀 보호조치 불이행		○		
비밀 보호조치 불이행		정당한 사유 없이 표시·고지나 그 밖에 비밀보호에 필요한 조치 불이행		○		
		정당한 사유 없이 비밀을 손괴·은닉하거나 효용을 해친 경우		○		
비밀/대외비 미분류·미등재		비밀 미분류로 유출 등 보안사고 발생		○		
		비밀 미분류			○	
		비밀 미등재(접수·결재 후 1개월 이상)			○	
		비밀 지연 등재 / 대외비 미분류·미등재·지연등재				○
비밀/대외비 분실	비밀	분실 후 미회수	미신고	○		
			신고		○	
		분실 후 회수	미신고	○		
			신고		○	
	대외비	분실 후 미회수	미신고	○		
			신고		○	
		분실 후 회수	미신고	○		
			신고		○	

구분 항 목	위반 내용		처리 기준		
			중대	보통	경미
비밀/대외비 관리	비밀 방치	고의적으로 유기·도난·분실 등 사고원인 제공	○		
		사무실 외 방치		○	
		사무실 내 방치			○
	대외비 방치	고의적으로 유기·도난·분실 등 사고원인 제공	○		
		사무실 외 방치		○	
		사무실 내 방치			○
정보통신시스템 관리위반	국가 정보통신시스템 및 전산망 대상 고의적 해킹 및 악성코드 유포		○		
	PC·서버 등 정보통신시스템 해킹으로 피해 발생	비밀 유출	○		
		대외비 유출		○	
		업무자료 유출			○
	비인가 정보통신시스템 반입·사용			○	
	해킹사고 인지 후 미신고			○	
	해킹 및 악성코드에 감염된 정보통신시스템 훼손 등 정당한 침해사고 조사행위 방해				○
	해킹·악성코드 등 침해사고 예방대책 미강구				○
	해커가 인지한 이메일 주소 변경사용 권고 후에도 지속 사용				○
	과실에 의해 악성코드가 감염되었으나 피해 심각(중요자료 대량 유출, 2개망 이상에 전파 등)			○	
과실에 의해 악성코드를 감염시켰을 때				○	

구 분 항 목	위반 내용		처리 기준		
			중대	보통	경미
	인터넷망 (외부망)	비밀을 임의저장·게시·공유·전송	○		
		대외비를 임의저장·게시·공유·전송		○	
		업무자료를 임의저장·게시·공유·전송			○
		외부인터넷망을 무단 설치·운용	○		
	행정망 (업무망)	비밀을 임의저장·게시·공유·전송		○	
		대외비를 임의저장·게시·공유·전송			○
		인터넷망과 임의 연동하거나 불법 접속		○	
	국가 정보시스템 손괴 및 부정사용, 비인가 프로그램 사용 등 고의적으로 정보시스템 장애 발생		○		
	공직기강 및 품위 훼손을 야기하는 등 업무와 무관한 자료 또는 소프트웨어 게시				○
	정보통신기기의 임의 반출			○	
	정보시스템 불용처리 시 저장매체 미삭제·미소거 처리				○
	정보시스템을 무력화·우회·편법 사용할 목적으로 관련기법을 전파 또는 공유				○
	필수 보안프로그램(안티 바이러스, USB 통제 프로그램 등) 미설치 및 우회하여 정보시스템 사용				○
	외부업체 직원의 전산망 임의 접속, 자료 열람, 악성코드 유포 등을 초래한 업무담당자				○

항 목	구 분	위반 내용	처리 기준		
			중대	보통	경미
	비인가 서버구축 및 서비스(홈페이지, 게시판, FTP, 게임 등) 운용			○	
	보안대책 검토 및 보안측정 등 보안절차를 준수하지 않거나 검토·측정결과 조치 미흡				○
	사전 승인 및 보안성검토·적합성검증 없이 정보시스템 개발·도입				○
	노트북·PC 등 단말기內 비인가된 무선통신 기능 미제거				○
	비밀번호 누설·도용 및 타인계정 무단 사용			○	
	비밀번호 운용규정 미준수				○
저장매체 무단반출	비밀용		○		
	대외비용			○	
	일반 업무용				○
저장매체 분실	비밀/ 대외비용	분실 후 미회수	미신고	○	
			신고		○
	분실 후 회수	미신고	○		
		신고		○	
	일반용	분실 후 미회수	미신고		○
			신고		○
분실 후 회수	미신고		○		
	신고		-		
저장매체 파기	비밀용 저장매체 무단 파기		○		
비인가 저장매체 반입	비밀 저장		○		
	대외비 저장			○	
	단순 반입				○

[별표 4] <신설 2023. 7. 31>

클라우드 서비스 이용 '시스템 중요도' 등급 분류기준

등급	분류기준		영역분리
상	파급영향	- 해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 치명적 악영향을 미칠 수 있음	물리적
	분류기준	- 국가 중대 이익(안보, 국가안전, 국방, 통일, 외교 등), 수사·재판 등 민감정보를 포함하거나 행정 내부업무 등을 운영하는 시스템	
중	파급영향	- 해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 심각한 영향을 미칠 수 있음	물리적
	분류기준	- 비공개 업무자료를 포함 또는 운영하는 시스템	
하	파급영향	- 해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 제한적인 영향을 미칠 수 있음	물리적 또는 논리적
	분류기준	- 개인정보를 포함하지 않고 공개된 공공데이터를 포함 또는 운영하는 시스템	

[표] 시스템 중요도 등급 분류기준 및 영역분리

- ※ 행정 내부업무의 경우 '시스템 중요도'를 고려하여 등급 조정 가능
- ※ 위 분류기준에 따른 분류 절차 및 체크리스트 등 세부사항은 '국가 클라우드서비스 보안가이드라인'을 참고한다.
- ※ 이용기관은 민간 클라우드서비스 도입시 시스템 등급을 자체 분류하고, 국정은 '보안성 검토'시 분류의 적정성을 재검토한다.

[별지 제1호서식]

보안적합성 검증 신청서

신청 기관	기관명		담당자	
	부서명		전화번호	
	사업명		이메일 ※ 상용메일 불가	
	도입 목적			
	보안성 검토명		계약 날짜	
			도입 날짜	
	검증결과 반영	취약점 등의 개선요청 이행 (<input type="checkbox"/> 반영·개선 <input type="checkbox"/> 반영불가)		
신청 제품	제품명		S/W(펌웨어) 버전	
		※ 신청 제품이 2種 이상인 경우, 별도 신청		
	제품 유형		도입 수량	대
	사전 인증 대상 여부	<input type="checkbox"/> CC인증 대상 <input type="checkbox"/> 검증필 암호모듈 탑재 <input type="checkbox"/> 해당 없음		
		※ CC인증·검증필 암호모듈 탑재 필수 제품은 국정원 홈페이지 참조		
	해시값 (SHA-512)	※ 해시값은 국정원 홈페이지에 게시된 S/W 사용		
	CC 인증기관		CC 인증등급	
	CC 인증번호		CC 만료일	
암호모듈명		암호검증 번호	CM-	
업체	업체명		대표자	
	주소			
	담당자명		전화번호	
	휴대폰번호		이메일	

※ △서식이 변경될 수 있으므로 국가정보원 홈페이지(튼튼한 안보→사이버안보→보안적합성 검증 →검증공지사항)에 게시된 양식을 참고 △'검증결과 반영'을 포함하여 기재 양식中 해당사항은 빠짐없이 기재

[별지 제4호서식]

전파측정 결과보고서

1. 일반 사항

- 가. 측정 기간 및 지역
- 나. 측정 장비
- 다. 참여기관 및 인원

2. 측정 결과

기간	측정지점	통신구간	주파수 (MHz)	신호세기 (dBm)	취약여부	비고
						디지털/ 아날로그 구분

3. 분석 및 평가

4. 조치 및 대책

[별지 제6호서식]

서 약 서

본인은 년 월 일부로 _____업무(연구개발, 제작, 입찰, 그 밖의 업무)를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 _____소관업무가 국가기밀 사항임을 인정하고 제반 보안 관계규정 및 지침을 성실히 준수한다.
2. 본인은 이 기밀을 누설함이 이적행위가 됨을 명심하고 재직 중은 물론 퇴직 후에도 알게 된 모든 기밀사항을 「부패방지권익위법」·「공익신고자 보호법」에 따른 신고의 경우를 제외하고는 일절 타인에게 누설하지 아니한다.
3. 본인은 기밀을 누설한 때에는 아래의 법령 위반으로 처벌될 수 있음을 확인한다.

- 가. 「국가보안법」 제4조제1항제2호 및 제5호(국가기밀 누설 등)
- 나. 「형법」 제99조(일반이적) 및 제127조(공무상 비밀의 누설)
- 다. 「군형법」 제80조(군사기밀 누설)
- 라. 「군사기밀보호법」 제12조(누설) 및 제13조(업무상 군사기밀 누설)
- 마. 「개인정보보호법」 제70조(벌칙) 내지 제75조(과태료)

년 월 일

서약자	소속	직급	생년월일	
		직위	성 명	(서명 또는 인)

서 약	소속	직급	성 명	
집행자(담당공무원)		직위	성 명	(서명 또는 인)

광명시장 귀하

[별지 제7호서식]

확 약 서

본인은 귀 기관과 계약한 _____용역사업의 수행을 완료함에 있어 다음 각 호의 보안사항에 대한 준수책임이 있음을 서약하며 이에 확약서를 제출합니다.

1. 업체(단체) 및 사업 참여자가 용역사업 수행 중 지득한 모든 자료를 반납 및 파기하였으며 지득한 정보에 대한 유출을 절대 금지하겠습니다.
2. 하도급업체에 대해 상기 항과 동일한 보안사항 준수책임을 확인하고 보안확약서를 징구하였으며 하도급업체가 위의 보안사항을 위반할 경우에 관리·감독의 법적 책임을 지겠습니다.
3. 상기 보안사항을 위반할 경우에 귀 기관의 사업에 참여제한 등의 불이익과 관련법규에 따른 손해배상 등의 책임을 감수하겠습니다.

년 월 일

업체명 : _____
 서약자 직 위 : _____
 (업체 대표) 생년월일 : _____
 성 명 : _____ (인)

소 속 : _____
 서약 집행자 직 위 : _____
 (담당공무원) 생년월일 : _____
 성 명 : _____ (인)

광명시장 귀하

[별지 제12호서식]

보안관제센터 운영현황

보안관제센터 개요				
개소	* 개소일자	위치		
규모	* 상황실 면적 등	예산	* 구축예산 및 운영예산	
조직 현황				
개요	* 조직구성, 인원 및 임무, 근무형태 등			
1	부서		센터장	
	직급		성명	
	이메일		연락처	전화: HP:
2	부서		직급/직책	
	담당분야		성명	
	이메일		연락처	전화: HP:
3	:	* 센터장과 탐지·분석·대응 등 분야별 대표자만 기입		
외부인력 현황				
업체명		대표이사		
인원수		근무형태		
계약기간		수행업무		
지침·매뉴얼 현황				
지침		기준		
매뉴얼		기타		
보안관제시스템 현황				
시스템명	* 주요 기능	시스템명		
시스템명		시스템명		
시스템명		시스템명		

보안장비 현황						
F/W	* 제품명 및 사용대수		IDS/IPS			
ESM			WEB F/W			
라우터			그 밖의 장비	예) NMS 1대 * 네트워크 구성도 사본 제출		
보안관제 연동기관 현황						
* 대상기관 수, 기관명, 대상목표(인터넷 또는 내부망, 홈페이지 등)						
연동기관 IP할당 현황						
1	연동기관		IP 관리자	성명		
	공인IP			연락처	전화:	HP:
	사설IP			이메일		
2						
3						
4						
5						
6						
국가사이버안보센터 탐지규칙 재배포 현황						
기관명		배포방법		기관명		

[별지 제13호서식]

정보시스템 등록/변경/폐기 신청서

유 형		1. 등록 <input type="checkbox"/> 2. 변경 <input type="checkbox"/> 3. 폐기 <input type="checkbox"/>	
구 분		변경 전	변경 후
기 본 사 항	관리부서		
	자산코드		
	시스템명		
	수 량		
	목적/기능		
	자산위치		
	소 유 자		
	관리자(운영자)		
	사 용 자		
추가 서술내용			
자산중요도 등급			

[별지 제14호서식]

정보시스템 보안점검 체크리스트

1. 정보시스템

점 검 내 용		결 과	비 고
계정관리	사용자 계정은 지침에 따라 권한을 부여하고 있는가?		
	시스템 사용자는 고유의 개인별 사용자계정을 가지고 있는가?		
	사용자 ID 및 접근권한을 점검하였는가?		
	사용되지 않는 계정(퇴직자, 전출자, 사용기간이 만료된 사용자)은 삭제되었는가?		
	패스워드는 문자, 숫자, 기호 등을 혼합하여 9자리 이상으로 사용하는가?		
	패스워드는 분기 1회 이상 변경하도록 되어 있는가?		
	비밀번호는 전산망별, 단말기별, 자료별로 구분 사용하는가?		
접근제어	관리자 및 인가된 시스템만 접근할 수 있도록 접근제한이 설정되어 있는가?		
	원격 접근을 위해 SSH 등의 암호화된 프로토콜만을 사용하고 있는가?		
로그시간	OS 및 중요 어플리케이션에 대한 운영로그를 유지하도록 설정되어 있는가?		
	모니터링을 위한 감사 기록을 생성하고 있는가?		
	모든 시스템의 시계는 적절한 기록을 위해 표준 시간에 맞추어져 있는가? (시간동기화를 하고 있는가? NTP를 사용하고있는가?)		
백업	중요한 모든 정보(설정파일(DNS, Mail), 소스파일, 데이터, DB, 중요서버 로그 정보)와 소프트웨어에 대한 주기적인 백업을 하고 기록관리 하고 있는가?		
패치	운영체제 및 각종 소프트웨어(어플리케이션)에 대한 보안패치를 적용하였는가?		
암호화	중요 데이터에 대해서 암호화를 수행하고 있는가?		
보안점검	알려진 취약점에 대해 보안대책을 적용하였는가?		

점 검 내 용		결 과	비 고
운영관리	정보통신시스템 구축 계획 시 보안대책 관련 사항을 반영하여 추진했는가?		
	정보통신망 운용현황 및 통신 소통량은 파악되고 있는가?		
	시스템에 불필요한 프로토콜이나 서비스가 존재하는가?		
	바이러스 등의 악성 소프트웨어들을 예방하고 탐지, 대응하기 위해 안티바이러스 제품이 설치되어 있는가?		
인터넷 보안	자체 전산망과 인터넷을 접속할 경우에는 인가된 침입차단시스템 설치 등 보안대책을 강구하고 있는가?		
	홈페이지에 자료를 게재할 경우 중요내용이 외부에 공개되지 않도록 자체 정보화/보안심사위원회 심의 또는 보안담당관의 통제를 거쳤는가?		
응용 프로그램 보안	소스 프로그램은 실제 운영 환경에 보관하지 않는가?		
	정보시스템의 파괴와 손상을 최소화하기 위하여 공식적인 변경관리 절차를 수립하였는가?		
전산자료 보안관리	비밀 및 중요자료의 전송 시는 기밀성을 보장하기 위하여 보안시스템 또는 암호자재를 사용하는가?		
정보보호 시스템 운영	정보보호시스템은 국가기관용의 정보보안 요구사항을 만족하는 제품을 선정하였는가?		
	정보보호시스템 구성 시 보안등급은 적절히 구현되었는가?		
	정보보호시스템은 필요한 서비스만 제공되고 설치 목적외 다른 용도로 사용되지 않는가?		
	정보보호시스템에 대한 감사기록 로그설정은 되어 있는가?		

2. 네트워크 및 정보보호시스템

점 검 내 용		결과	비고
계정관리	사용자 계정은 지침에 따라 권한을 부여하고 있는가?		
	사용자 ID 및 접근권한을 점검하였는가?		
	불필요한 계정을 삭제하였는가?		
	패스워드는 9자리 이상이며 복잡성을 만족하고 있는가?		
인증	패스워드가 암호화되어 있는가?		
	인증서버를 사용하는가?		
SNMP	별도의 snmp-server를 등록하여 사용하는가?		
	SNMP 커뮤니티로 디폴트 설정 값(public)을 변경하였는가?		
접근제어	원격 접근을 위한 관리자 소스 IP는 제한하도록 설정하였는가?		
	원격 접근을 위해 SSH 등의 암호화된 프로토콜만을 사용하고 있는가?		
	외부 접속 사용자에게 의한 접근을 통제하기 위해 적절한 암호화 통신 및 인증 방법이 사용되고 있는가?		
	정보 서비스, 사용자, 그리고 정보 시스템의 그룹들은 네트워크 상에서 분리하였는가?		
	접근제어리스트(ACL)을 설정하였는가?		
보안점검	알려진 취약점에 대해 보안대책을 적용하였는가?		
로그	로깅 기능은 활성화하고 있는가?		
	원격에서 로그를 수신하기 위한 Syslog 서버 등을 설정하였는가?		
시간	NTP 서버를 통한 정확한 시간 동기화는 이루어지고 있는가?		
백업	설정파일에 대한 주기적인 백업기능을 설정하였는가?		
패치	OS보안패치를 적용하였는가?		
운영관리	백본망, 주요노드 및 회선에 대한 트래픽을 정기적으로 모니터링하기 위한 대책이 있는가?		
	이상 징후를 알리는 경고기능을 설정하였는가?		
	통신회선 등의 장애에 대한 대책은 수립되어 있는가? (이중화, 백업플랜 등)		

