정보보안 기본지침

제정 2014. 1. 24.
개정 2015. 5. 13.
개정 2015. 7. 14.
개정 2017. 4. 13.
전부개정 2018. 12. 28
전부개정 2020. 1. 31
개정 2021. 2. 25
개정 2022. 1. 27
개정 2022. 12. 23.

제 1 장 총 칙

제1조(목적) 이 지침은 한국인터넷진흥원(이하 “진흥원”이라 한다)의 「보안업무규칙」에서 위임한 사항과 정보보안과 관련한 기본업무를 규정함을 목적으로 한다.

제2조(적용범위) 이 지침은 과학기술정보통신부 정보보안 기본지침을 준용하여 진흥원에 적용한다.

제3조(정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다

1. “정보보안”이라 함은 각급기관의 기능 유지를 주 목적으로 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 다음 각 목에 따른 사항을 포함한다.<개정 2022.1.27>
   가.「국가정보원법」 제4조제1항제4호에 따른 사이버공격 및 위협에 대한 예방 및 대응<신설 2022.1.27>
   나.「전자정부법」 제56조에 따른 정보통신망과 행정정보 등의 보안<신설 2022.1.27>
   다.「정보통신기반 보호법 시행령」 제5조 제4항 제1호 각 목에 해당하는 주요정보통신기반시설의 보호<신설 2022.1.27>
   라.「공공기록물 관리에 관한 법률 시행령」 제5조에 따른 전자기록물의 보안<신설 2022.1.27>
   마.「국가사이버안전관리규정」 제2조 제3호에 따른 사이버안전<신설 2022.1.27>
2. “정보통신실”이라 함은 서버·스위치·라우터·교환기 등 전산 및 통신장비 등이 설치·운용되는 장소 또는 전산실·통신실·데이터센터 등을 말한다.
3. “정보시스템”이라 함은「전자정부법」 제2조 제13호에 따른 PC·서버 등 단말기, 보조기억매체, 전산·통신장치, 정보통신기기, 응용 프로그램 등 정보의 수집·가공·저장·검색·송수신에 필요한 하드웨어 및 소프트웨어 일체를 말하며 연구·개발을 위한 시스템을 포함한다.
4. “정보보호시스템”이라 함은「지능정보화 기본법」 제2조 제15호에 따른 정보의 수집, 가공, 저장, 검색, 송·수신 중 발생할 수 있는 유출, 위·변조, 훼손 등을 방지하기 위한 기술적 수단을 말한다.<개정 2022.1.27>
5. “업무전산망”(이하 “내부망”이라 한다)이라 함은 기관의 네트워크 중에서 업무용으로 사용되는

영역으로, 구축・운영하는 정보통신망 중에서 인터넷과 분리된 업무 전용(專用) 정보통신망을 말한다.
6. “인터넷서비스망”(이하 “기관 인터넷망”이라 한다)이라 함은 기관의 구축・운영하는 정보통신망 중에서 인터넷과 연동된 정보통신망을 말한다.
7. “휴대용 저장매체”라 함은 디스켓・CD・외장형 하드디스크・USB메모리 등 정보를 저장할 수 있는 것으로 PC・서버 등의 정보통신시스템과 분리할 수 있는 기억장치를 말한다.
8. “디지털복합기”라 함은 저장매체를 내장하고 네트워크 기능이 포함된 복합기・복사기・프린터 등의 복합된 사무용기기를 말한다.
9. “소속직원”이라 함은 진흥원에 근무 중인 임·직원을 말한다.
10. “개별사용자”라 함은 보안담당관으로부터 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 소속직원과 보안담당관과 계약에 의하여 정보통신망 또는 정보시스템에 대한 접근 또는 사용 허가를 받은 사람을 말한다.
11. “업무자료”라 함은 다음 각 목의 어느 하나에 해당하는 것을 말한다.
가.「전자정부법」제2조제6호에 따른 행정정보 및 동법 제2조 제7호에 따른 전자문서
나.「공공기록물 관리에 관한 법률 시행령」제2조 제2호에 따른 전자기록물
다. 기타 다른 법령에 의하여 소속직원이 직무상 작성・취득하였거나 보유・관리하는 자료로서 전자적으로 처리되어 부호・문자・음성・음향・영상 등으로 표현된 것
12. “비밀”이라 함은 업무자료 중에서 「보안업무규칙」제26조에 따라 분류된 비밀을 말한다.
13. “대외비”라 함은 업무자료 중에서 「보안업무규칙」제30조에 따라 분류된 대외비를 말한다.
14. “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. 국회 소속 공무원(「국회의원수당 등에 관한 법률」제9조에 따른 보좌직원을 포함한다) 또는 「지방자치법」제30조에 따른 지방의회 소속 공무원의 직무상 요구에 따라 작성 또는 취득한 자료
다. 가목에 따른 비공개 대상 정보의 주요 내용이 기술된 문장 또는 문구
15. “암호알고리즘”이라 함은 정보의 유출, 위・변조, 훼손 등을 방지하기 위하여 기밀성・무결성・인증・부인방지 등의 기능을 제공하는 수학적 논리를 말한다.
16. “암호자재”라 함은 비밀의 보호 및 정보통신 보안을 위하여 암호기술이 적용된 장치나 수단으로서 Ⅰ급, Ⅱ급 및 Ⅲ급비밀 소통용 암호자재로 구분되는 장치나 수단을 말한다.<개정 2022.1.27>
17. “암호장비”라 함은 암호자재 중에서 국가정보원장이 승인하여 개발・제작・보급되는 암호자재를 말한다.<개정 2022.1.27>
18. “암호가 주기능인 제품”이라 함은 검증필 암호모듈을 사용해 정보의 암・복호화를 주된 목적・기능으로 하는 제품을 말한다.<개정 2022.12.23>
19. “검증필 암호모듈”이라 함은「사이버안보 업무규정」제9조 제2항 및 제3항,「전자정부법 시행령」제69조와「암호모듈 시험 및 검증지침」(국가정보원 지침)에 따라 국가정보원장이 안전성을 확인하여 제23조에 따른 목록에 등재한 상용 암호모듈을 말한다.<개정 2022.1.27>
20. “전자파 보안”이라 함은 정보통신시설 및 기기 등을 대상으로 전자파에 의한 정보유출을 방지하고 파괴・오작동 유발 등의 위협으로부터 정보를 보호하는 일체의 행위를 말한다.
21. “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.

22. “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.

23. “주요정보통신기반시설”이라 함은 국가안전보장·행정·국방·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망을 말한다.

24. “원격근무”이라 함은 정보기술(IT) 기반을 활용하여 사무실이 아닌 자택 등의 장소에서 업무를 수행하는 근무방식을 말한다.

25. “원격지 개발”이라 함은 사업 수행시 발주기관 소재지 이외 장소에서 발주자가 제안요청서에 명시한 보안요구사항을 준수하여 용역 업무(유지보수는 제외한다)를 수행하는 개발방식을 말한다.

26. “사이버공격”이라 함은 「사이버안보 업무규정」 제2조 제2호에 따른 행위를 말한다. <개정 2022.1.27>

27. “보안관제센터”라 함은 정보보호시스템에서 탐지된 공격 및 침입정보를 종합·분석하여 침해사고에 대한 예방 및 대응 업무를 수행하는 센터를 말한다.

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

② 보안담당관은 소속직원에 대한 근무성적 또는 성과 평가를 실시할 경우 정보보안내규 준수여부 등을 반영할 수 있다.<개정 2022.1.27>

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

② 보안담당관은 제1항과 관련한 정보보안 조직을 지휘하고 정보보안 업무를 총괄하기 위하여 ‘정보보안담당관’을 임명하여야 한다.

③ 정보보안담당관에게 부여하는 기본활동은 다음 각 호와 같다.

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 총괄
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. 진흥원 및 관할 하급기관에 대한 정보보안 감사
10. 관할 하급기관의 정보보안업무 감독
11. 분임정보보안담당관 지정 및 감독·관리
12. 그 밖에 정보보안과 관련한 사항

④ 보안담당관은 정보보안담당관이 직무를 원활히 수행할 수 있도록 조직, 인력(정보화업무 담당 인력 대비 10% 이상) 및 예산(정보화 예산 대비 15% 이상)을 운영할 수 있도록 노력하여야 한다. <개정 2022.1.27>

⑤ 정보보안담당관은 정보보안 업무를 효율적으로 수행하기 위하여 부서의 장을 ‘분임정보보안담

당관'으로 임명하여야 한다.<개정 2022.12.23.>

⑥ 분임정보보안담당관은 소관업무에 대해 다음의 각 호의 임무를 수행한다.

1. 소관 업무시스템 구축·운영에 관한 보안대책 수립
2. 관련 업무 규정·지침이 있을 경우 정보보안 내용 포함
3. 제84조에 명시된 보호구역 설정 관리
4. 소관 업무시스템 정보보안 예산 및 전문인력 확보
5. 소관 주요정보통신기반시설 보호
6. 소관 업무시스템 정보보안 사고 대응 및 사고 조사 결과 처리
7. 소관 정보통신망 보안대책의 마련
8. 소관 업무시스템의 악성코드 감염 예방, 보안 취약성 제거 등 정보보안 업무
9. 기타 소관 업무시스템의 정보보안 관련 사항

⑦ 분임정보보안담당관은 소관 업무시스템 구축·운영에 따른 정보보안 개선이나 정보보안 관리실태 점검 등이 필요하다고 판단되는 경우 정보보안담당관에게 협조를 요청할 수 있다.

제6조(정보보안 전담인력) ① 보안담당관은 효율적이고 체계적인 정보보안 업무를 수행하기 위해 진흥원 규모에 적합한 정보보안 전담인력을 확보하고 별도 조직을 구성·운영하여야 한다.

② 제1항의 경우 정보통신망 또는 정보시스템에 대한 접근·사용 허가를 받아 제3조제9항의 업무를 처리하는 개별사용자를 진흥원 인원수에 반영하여야 한다.

③ 정보보안 전담인력은 제5조제4항에 따라 정보보안담당관이 직무를 원활히 수행할 수 있는 실무자(정보보안담당관은 제외한다)를 말하며, 산정기준은 다음의 각호와 같다.

1. 진흥원 인원수가 200명 미만의 경우 최소 전담인력 2명<개정 2022.1.27>
2. 진흥원 인원수가 200명~300명 미만의 경우 최소 전담인력 3명<개정 2022.1.27>
3. 진흥원 인원수가 300명~500명 미만의 경우 최소 전담인력 4명<개정 2022.1.27>
4. 진흥원 인원수가 500명 이상의 경우 최소 전담인력 5명 이상<개정 2022.1.27>

제7조(연도 추진계획 수립) ① 보안담당관은 매년 「연도 정보보안업무 추진계획」(「국가사이버안전관리규정」 제9조에 따른 사이버안전대책을 포함한다. 이하 같다)을 수립·시행하여야 한다.

② 제1항의 경우 보안담당관은 별지 제1호 서식의 정보보안업무 세부 추진계획을 작성하여 기간내(1.25限)에 과학기술정보통신부장관에게 제출하여야 한다.

③ 보안담당관은 정보보안 정책 및 계획을 수립·시행함에 있어 다른 기관과 협의·조정할 필요가 있을 경우 과학기술정보통신부장관에게 조정을 요청할 수 있다.

제8조(정보보안내규) ① 보안담당관은 정보 및 정보통신망 보호를 위한 자체 정보보안 내규(지침·시행세칙 등)를 국가정보원의 「국가 정보보안 기본지침」 및 「과학기술정보통신부 정보보안 기본지침」에 저촉되지 아니하는 범위에서 수립·시행하여야 한다.<개정 2021.2.25>

② 제1항의 경우 보안담당관은 과학기술정보통신부장관과 사전 협의하여야 한다.

제9조(정보보안 감사 등) ① 보안담당관은 진흥원 자체 정보보안 감사를 실시 할 수 있다. 다만, 국가·공공기관 정보보안 관리실태 평가 대상일 경우 연1회 이상 진흥원 자체 정보보안 감사를 실시하여야 한다.

② 제1항에 따라 필요한 경우 정보보안담당관 및 정보보안 전담인력을 감사 또는 감찰업무를 수행하는 부서에 배속하여 정보보안 감사를 합동 수행하도록 할 수 있다.
③ 정보보안 감사를 수행하는 자(이하 "정보보안 감사인"이라 한다)는 다음 각 호의 어느 하나에 해당하는 경우 정보보안 감사업무를 담당할 수 없다.
1. 징계처분을 받은 날부터 3년이 경과하지 아니한 자
2. 근무성적 및 근무태도가 불량한 자
④ 정보보안 감사인은 관계법령, 정관, 규정 등에 준거하여 정보보안 감사업무를 집행하여야 하며 다음 각 호의 사항을 준수하여야 한다.
1. 정보보안 감사를 실시함에 있어 선입감과 편견을 버리고 공정하게 하여야 한다.
2. 정보보안 감사를 실시함에 있어 피감사인의 업무상 창의력과 활동기능이 위축되거나 침체되지 아니하도록 하여야 한다.
3. 직무상 지득한 기밀을 정당한 이유 없이 누설하거나 이를 남용할 수 없다.
⑤ 정보보안감사를 실시할 경우 정보보안점검 체크리스트(부록1) 등을 활용할 수 있다.
⑥ 보안담당관은 정보보안감사를 효율적으로 수행하기 위하여 과학기술정보통신부장관에게 감사의 방향 및 중점사항, 감사관 지원 등 협조를 요청할 수 있다.
⑦ 제1항에 따라 정보보안 감사업무 수행 담당자를 다음 각 호의 법규를 적용하여 우대하여야 한다.
1. 「공공감사에 관한 법률」제18조에 따른 근무성적평정, 임용 등에서 우대
2. 「자체감사활동의 지원 및 대행·위탁감사에 관한 규칙」(감사원규칙) 제4조제4호에 따른 근무여건 개선 및 사기제고
3. 「공기업·준정부기관 감사기준」(기획재정부) 제16조에 따른 감사수당의 지급, 인사기준 별도 적용, 전보 시 희망보직 우선 고려 등 감사부서 직원과 동일한 대우
⑧ 원장은 정보보안 감사인으로 3년 이상 근무한 자가 전보될 경우 본인의 희망을 우선적으로 할 수 있으며, 정보보안 감사인에 대하여는 근무성적평정 시 우대할 수 있다.

제10조(정보보안 교육) ① 보안담당관은 정보보안에 대한 경각심을 제고하기 위하여 정보보안 교육계획을 수립하여 연2회 이상 모든 직원 등을 대상으로 교육(온라인 교육을 포함한다)을 실시하여야 한다.
② 제1항에 따라 모든 직원 등은 특별한 사유가 없는 한 연2회 이상 정보보안교육을 이수하여야 한다.
③ 보안담당관은 정보보안 교육의 효율성 제고를 위하여 진흥원 실정에 맞는 정보보안 교안을 작성 활용해야 하며 과학기술정보통신부장관 또는 국가정보원장에 전문인력 및 자료 지원을 요청할 수 있다.
④ 보안담당관은 정보보안 관련 전문기관 교육 및 기술 세미나 참석을 장려하는 등 정보보안 관련 직원들의 전문성을 제고하기 위해 노력해야 한다.
⑤ 보안담당관은 정보보안담당관, 분임정보보안담당관 및 정보보안 실무직원의 업무 전문성을 제고하고 소속직원의 정보보안 지식을 함양하기 위하여 전문기관의 교육 이수나 학술회의 참가 등을 장려하여야 한다.
⑥ 보안담당관은 신규 및 전입 직원이 발생할 경우, 직원 PC 및 스마트폰 보안수칙(부록 3) 등을 교육 받을 수 있도록 조치하여야 한다.

제11조 (사이버보안진단의 날) ① 보안담당관은 진흥원의 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 정보보안담당관은 '사이버보안 진단의 날'에 정보통신망의 악성코드 감염여부, 정보시스템의 보안 취약여부 등 정보보안업무 전반에 대하여 체계적이고 종합적인 보안진단을 실시하여야 한다.

③ 정보보안담당관 총괄 하에 '사이버보안진단의 날'에 부서의 장은 정보통신망과 정보시스템의 보안취약 여부 확인 등 보안진단을 실시하여야 한다.

제 2 장 정보화사업 보안

제 1 절 사업 계획

제12조(보안책임) ① 정보통신망 또는 정보시스템을 개발·구축·운용·유지보수하는 사업(이하 "정보화사업"이라 한다)을 수행하는 정보화사업 부서의 장은 해당 정보화사업에 대한 보안관리 책임을 지고 관리·감독하여야 한다.

② 정보보안담당관은 각종 정보화사업과 관련한 보안대책의 적절성을 평가하고 정보화사업 수행 전반에 대하여 보안대책의 이행여부를 점검하여 필요한 경우 정보화사업을 추진하는 부서의 장에게 시정을 요구할 수 있다.

제13조(보안대책 수립) ① 보안담당관은 정보통신망 또는 정보시스템을 구축·운용하기 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·운용장소 보안관리 등 물리적 보안대책
3. 정보통신망 또는 정보시스템의 구성요소별 기술적 보안대책
4. 국가정보원장이 개발하거나 안전성을 확인한 암호자재, 검증필 암호모듈 및 정보보호시스템 도입·운용계획<개정 2022.1.27>
5. 긴급사태 대비 및 재난복구 계획
6. 용역업체 작업장소에 대한 보안대책
7. 온라인 개발 또는 온라인 유지보수가 필요하다고 판단할 경우, 제29조의2 또는 제52조에 따른 보안대책
8. 누출금지정보 보안관리 방안

제14조(제안요청서 기재사항) ① 정보화사업을 추진하는 부서의 장은 용역업체에 정보화사업을 발주하기 위하여 제안요청서를 작성할 경우 다음 각 호의 사항을 포함하여야 한다.

1. 용역업체 작업장소에 대한 보안요구사항
2. 온라인 개발 또는 온라인 유지보수가 필요하다고 판단할 경우, 제29조의2 또는 제52조에 따른

보안대책

3. 누출금지정보 목록

4. 용역업체가 누출금지정보를 제외한 소프트웨어 산출물을 제3자에게 제공하고자 할 경우 발주자의 승인절차

② 제1항 제3호에 따른 누출금지정보 목록을 작성할 경우 다음 각 호의 사항을 포함하여야 한다.

1. 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·운용 현황<개정 2022.1.27>

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.「보안업무규칙」제26조에 따른 비밀 및 제30조에 따른 대외비

11. 그 밖에 보안담당관이 공개가 불가하다고 판단한 자료

제2절 보안성 검토

제15조(검토 시기 및 절차) ① 보안담당관은 정보화사업을 수행하고자 할 경우 정보화사업과 관련한 보안대책의 적절성을 평가하기 위하여 사업 계획 단계(사업 공고 전)에서 보안성 검토를 실시해야 한다.

② 보안담당관은 제1항에 따른 보안성 검토를 위해 제16조 제1항 및 제2항에 따른 보안성 검토기관의 장에게 검토를 의뢰하거나 자체적으로 실시하여야 한다. 보안담당관이 제16조 제1항 각 호에 해당하는 정보화사업에 대하여 국가정보원장에게 보안성 검토를 의뢰하고자 할 경우 과학기술정보통신부장관을 거쳐 의뢰하여야 한다.

③ 보안성 검토는 서면 검토를 원칙으로 하며 과학기술정보통신부장관이 필요하다고 판단하는 경우 현장 확인을 병행 실시할 수 있다.

제16조(검토 기관) ① 국가정보원장은 원장이 추진하는 다음 각 호에 해당하는 정보화사업에 대하여 보안성 검토를 실시한다. 다만, 국가정보원장은 정보화사업의 규모·중요도 등을 고려하여 과학기술정보통신부장관에게 보안성 검토를 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. 제25조제1항에 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. 제2조 제6호에 따른 기관 인터넷망 등 업무상 목적으로 활용하기 위한 인터넷망(제43조 제1항 제1호에 따른 업무용 무선랜 형태를 포함) 및 이동통신망(HSDPA, WCDMA, LTE, 5G 등)의 구축 <개정 2022.1.27>

15. 제59조에 따른 원격근무시스템 구축

16.「전자정부법」제54조의2 및「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제20조에 따라 클라우드컴퓨팅서비스 제공자의 클라우드컴퓨팅서비스(이하 “민간 클라우드컴퓨팅서비스”라 한다)를 이용하는 사업<개정 2022.1.27>

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 과학기술정보통신부장관은 다음 각 호에 해당하는 정보화사업에 대하여 보안성 검토를 실시한다. 다만, 제9호부터 제13호까지에 해당하는 정보화사업에 대한 보안성 검토는 보안담당관이 실시하도록 위임할 수 있다.

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. 제2조 제6호와 별로로 분리된 상용 인터넷망(제43조 제1항 제2호 또는 제3호에 따른 무선랜 형태를 포함)의 구축<개정 2022.1.27>

6. 내부망에 구축하는 공무원등의 인사·복지시스템<개정 2022.1.27>

7. 주요정보통신기반시설 취약점 분석·평가, 정보보안컨설팅 등 용역사업

8. 기존 분리된 내부망·기관 인터넷망간 자료전송시스템 구축 등 후속사업

9. 대규모 백업·재해복구센터 구축

10. 제45조 제1항에 따른 영상회의시스템을 내부망 또는 기관 인터넷망과 분리하여 구축하는 경우<개정 2022.1.27>

11. 제86조 제3항에 따라 영상정보처리기기를 인터넷과 분리하여 구축하는 경우<개정 2022.1.27>

12. 백업시스템 구축

13. 대민(對民) 콜센터시스템 구축

제17조(검토 생략) ① 보안담당관은 다음 각 호에 해당하는 정보화사업에 대하여는 보안성 검토 절차의 이행을 생략할 수 있다. 이 경우 관련 매뉴얼·가이드라인 등을 준수하는 등 자체 보안대책을 수립·시행하여야 한다.

1. 제16조 제1항 및 제2항 각 호의 정보화사업에 해당하지 아니하는 단순 장비・물품 도입
2. 제16조에 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
   다. 기존 운용하던 정보보호시스템을 동일한 보안기능을 보유한 다른 정보보호시스템으로 교체
3. 다년도에 걸쳐 계속되는 사업으로써 사업 착수 당시 보안성검토를 완료 한 후 사업 내용의 변동 없이 계속 추진하는 운영·유지사업
4. PC・프린터 및 상용 소프트웨어 등 단순 제품 교체

② 보안담당관은 제1항제2호부터 제4호까지에 해당하는 정보화사업을 수행할 경우 기존 보안성 검토 결과를 준수하여야 한다.

제18조(제출 문서) 보안담당관은 제15조제2항에 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

제19조(검토결과 조치) ① 보안담당관은 제16조에 따라 보안성 검토결과를 통보받은 경우 검토결과를 반영하여 보안대책을 보완하여야 한다.

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

제20조(현황 제출) 보안담당관은 전년도에 실시한 정보화사업에 대한 보안성 검토결과 현황을 매년 1.25까지 과학기술정보통신부장관에게 제출하여야 한다.

제3절 사업 수행

제21조(정보통신제품 도입요건) 보안담당관은 정보 및 정보통신망 등을 보호하기 위하여 정보보호시스템・네트워크장비 등 보안기능이 있는 정보통신제품을 도입・운용하고자 할 경우 [별표 3]에 따른 정보보호시스템 유형별 도입요건을 준수하여야 한다.

제22조(암호가 주기능인 제품 도입요건) 보안담당관은 정보통신망을 이용하여 유통·보관되는 중요 자료를 보호하기 위하여 암호가 주기능인 제품을 도입·운용하고자 할 경우 [별표 4]에 따른 암호가 주기능인 제품 도입요건을 준수하여야 한다.

제23조(검증필 암호모듈 도입 시 고려사항) 보안담당관은 국가정보원장이 안전성을 확인한 상용 암호모듈을 도입하여 정보시스템 등에 적용하고자 할 경우 실제 적용 이전에 해당 상용 암호모듈의 정상 동작여부, 정보시스템 적용단계에서 구동과정상 오류 발생여부 등을 점검하여야 한다. <개정 2022.1.27>

제24조(영상정보처리기기 도입 시 고려사항) 보안담당관은 제86조제1항에 따른 영상정보처리기기를 도입·운용하고자 할 경우 한국정보통신기술협회(TTA)의 공공기관용 보안 성능품질 인증 등 일정한 보안성능이 확인된 제품을 우선적으로 도입할 수 있다.

제25조(제어시스템 도입 시 고려사항) ① 보안담당관은 공항·항만·전력·가스·운송설비 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 보안 가이드라인」에 따른 보안대책을 수립·시행하여야 한다.

② 국가정보원장은 각급기관이 도입하는 제어시스템의 실제 가동 이전에 해당 제어시스템의 안전성을 확인할 수 있다.

③ 보안담당관은 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 보안소프트웨어를 설치함으로써 제어시스템의 정상 운영에 차질을 초래할 경우 국가정보원장과 협의하여 설치하지 아니할 수 있다.

④ 보안담당관은 교통·에너지·수자원 등 국가안보상 중요한 제어시스템을 운용할 경우 인터넷 및 일반 사무용 내부망과 분리·구축하여야 한다.

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

제26조(계약 특수조건) ① 보안담당관은「국가를 당사자로 하는 계약에 관한 법률 시행령」제76조 제1항 제3호 다목에 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 또는 방치하는 행위 등을 금지하는 내용의 계약 특수조건을 계약서에 명시하여야 하며 계약기간(하자 보증기간을 포함한다) 내에 발생한 보안약점 등에 대해서는 계약업체로 하여금 개선 조치하도록 하여야 한다.

② 보안담당관은 필요한 경우 계약업체로부터 제1항과 관련한 행위가 없다는 대표자 명의의 확약서를 요구할 수 있다.

제27조(용역업체 보안) ① 보안담당관은 용역업체에 정보화사업을 발주할 경우 다음 각 호의 보안 사항을 준수하도록 계약서에 명시하여야 한다.

1. 제14조제1항 각 호에 따른 제안요청서에 포함된 사항

1의2. 제28조에 따른 원격지 개발, 제28조의2에 따른 원격지에서의 온라인 개발, 제52조에 따른 온라인 유지보수를 허용할 경우 보안 준수사항<신설 2022.1.27>

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 임의교체 금지

5. 정보통신망 구성도·IP주소 현황 등 업체에 제공하는 자료는 자료 인계인수대장을 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 종료 시 업체의 노트북·휴대용 저장매체 등 관련 장비는 저장자료 복구가 불가하도록 완전 삭제

8. 사업 종료 시 누출금지정보 전량 회수

9. 그 밖에 보안담당관이 보안관리가 필요하다고 판단하는 사항 또는 국가정보원장이 보안조치를 권고하는 사항

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

1.「국가공무원법」제33조(결격사유) 제3호부터 제6의4호까지에 해당하는지 여부

2.「국가를 당사자로 하는 계약에 관한 법률」제27조제1항 각 호의 행위를 한 사람

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

1. 제1항에 따라 계약서에 명시된 보안 준수사항

2. 제28조의2에 따른 진흥원 내 작업 장소 보안 준수사항

3. 제29조에 따른 원격지 개발 보안 준수사항 및 제29조의2에 따른 원격지에서의 온라인 개발시 보안 준수사항<개정 2022.12.23.>

4. 제51조에 따른 정보시스템 유지보수 및 제52조에 따른 온라인 유지보수 시 보안 준수사항<개정 2022.12.23.>

④ 그 밖에 용역업체 보안과 관련한 사항은 국가정보원장이 배포한「국가·공공기관 용역업체 보안관리 가이드라인」을 준수하여야 한다.

제28조(소프트웨어 개발보안) 보안담당관은 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.

제28조의2(진흥원내 작업장소 보안) ① 보안담당관은 진흥원 내(진흥원장이 임차한 외부 사무실을 포함한다) 용역업체 작업장소를 설치할 경우 보안 통제가 가능한 공간을 마련·운영하여야 한다. <신설 2021.2.25>

② 진흥원 내 용역업체 작업 장소에 설치 운영하는 정보통신망은 진흥원의 정보통신망과 분리 구성하여야 한다. 다만, 용역업체가 사업 수행을 위하여 진흥원 정보시스템 이용이 불가피할 경우

필요한 정보시스템에 한해 지정된 단말기로부터의 제한적 접근을 허용하는 등 보안대책을 수립·시행하여야 하며, 이 경우 내부망 정보시스템에 대한 접근허용에 관하여는 보안담당관과 사전 협의하여야 한다.

③ 작업장소내 정보시스템은 용역사업 수행을 위해 필요한 경우 해당 보안담당관의 보안통제 하에 인터넷에 연결할 수 있다. 다만, 제2항 단서에 따른 진흥원 정보시스템 접근용 단말기의 경우 인터넷 연결을 금지한다.

④ 보안담당관은 용역업체가 진흥원 내 작업 장소에서 개발 작업을 수행하더라도 개발용 서버가 민간 클라우드컴퓨팅서비스를 이용하는 등으로 원격지에 위치할 경우 제29조에 따른 원격지 개발로 간주하고 제29조 제1항에 따른 보안대책을 수립·시행하여야 한다.

제29조(원격지 개발보안) ① 보안담당관은「소프트웨어 진흥법」제49조제3항 및 제4항,「소프트웨어사업 계약 및 관리감독에 관한 지침」제14조에 따라 용역업체가 발주기관 이외의 장소(이하 "원격지"라 한다)에서 개발 작업(유지보수는 제외한다)을 수행하고자 요청할 경우 제14조 제1항 제1호에 따른 용역업체 작업 장소에 대한 보안요구사항 등을 포함한 관리적·기술적 보안대책을 수립·시행하여야 한다. 이 경우 분임정보보안담당관은 보안대책을 수립한 후 정보보안담당관의 승인을 받아야 한다.<개정 2022.1.27>

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

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

제29조의2(원격지에서의 온라인 개발) 제29조에 따른 원격지 개발에서 보안담당관 필요하다고 판단하고 용역업체가 다음 각 호에 따른 보안대책에 서면으로 동의하는 경우에 한하여, 보안담당관은 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 3호에 따른 온라인 용역 통제시스템 접속 전용(專用)으로 운용하고 다른 목적의 인터넷 접속은 차단
3. 진흥원내 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 진흥원, 진흥원의 상급기관 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

제30조(소프트웨어 산출물 제공) ① 보안담당관은 용역업체가「소프트웨어 진흥법」제59조 및「(계약예규)용역계약일반조건」(기획재정부 계약예규) 제56조(검사)에 따른 지식재산권을 행사하기 위하여 소프트웨어 산출물의 반출을 요청할 경우 제안요청서 또는 계약서에 명시된 누출금지정보에 해당

하지 아니하면 제공하여야 한다.<개정 2022.1.27>

② 보안담당관은 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 확약서를 받아야 한다.

③ 보안담당관은 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.<개정 2022.1.27>

제31조(누출금지정보 유출시 조치) ① 보안담당관은 용역업체가 제안요청서 또는 계약서에 명시된 누출금지정보를 유출한 사실을 인지한 경우 업체를 대상으로 계약 위반에 따른 조치를 취하여야 한다. 이 경우 용역업체의 누출금지정보 유출 사실을 알게 된 정보화사업담당은 즉시 정보보안담당관을 거쳐 보안담당관 및 원장에게 보고하여야 한다.

② 제1항에 따라 용역업체의 누출금지정보 유출 사실을 인지하거나 보고를 받은 보안담당관은 그 사실을 과학기술정보통신부장관 및 국가정보원장에게 통보하여야 하고 「국가를 당사자로 하는 계약에 관한 법률 시행령」제76조에 따라 입찰 참가자격 제한 등 관련조치를 취하여야 한다.

제4절 보안적합성 검증

제32조(검증대상 제품) ① 보안담당관은 다음 각 호에 해당하는 제품을 도입하고자 하거나 도입한 경우 실제 적용·운용 이전에 안전성을 확인하기 위하여 보안적합성 검증을 받아야 한다.

1. [별표3]의 안전성 검증필 제품이나 [별표4]의 암호가 주기능인 제품 도입여건을 만족하는 제품에 해당되지 않는 정보통신제품 중에서 국가정보원장이 별도로 공지하는 도입요건을 만족하는 제품<개정 2022.1.27>
2. 제품유형의 특성상 보안기능의 비중이 미미하여, 보안담당관이 자유롭게 도입·운용이 가능한 '단순 보안기능 제품유형'으로 국가정보원장이 공지한 제품<개정 2022.1.27>
3. 취약 정보통신제품을 긴급 대체하기 위하여 도입하는 제품<개정 2022.1.27>
4. <삭제 2022.1.27>

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

1.「국가정보화 기본법」제38조제1항 및 동법 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 한다)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 기술이전한 정보통신제품

③ 보안담당관은 제2항에도 불구하고 취약점이 발견되거나 보안위협이 제기되는 제품의 경우 보안적합성 검증을 받아야 한다.

제33조(검증 기관) ① 보안담당관은 제32조에 따른 보안적합성 검증을 받고자 할 경우 다음 각 호의 기관(이하 "검증기관"이라 한다)의 장에게 검증을 신청하여야 한다.<개정 2022.1.27>

1. 상급기관 및 주요정보통신기반시설 관리기관 : 국가정보원<신설 2022.1.27>
2. 하급기관(주요정보통신기반시설 관리기관을 제외한다) : 관계 상급기관<신설 2022.1.27>

② 제1항 및 제2호에도 불구하고 보안담당관은 필요하다고 판단하는 경우 제34조에 따른 검증신청기관의 장과 협의하여 해당 기관의 장이 자체적으로 검증을 실시하게 할 수 있다.<개정 2022.1.27>

③ <삭제 2022.1.27>

제34조(검증 신청) ① 보안담당관은 제33조에 따라 보안적합성 검증을 신청할 경우 검증기관의 장에게 [별표 5] 보안적합성 검증 신청 시 제출물에 해당하는 문서 등을 제출하여야 한다.

② 제1항에 따라 검증을 신청한 보안담당관은 검증 기관의 장이 필요하다고 판단하여 추가 자료를 요청할 경우 이를 제출하여야 한다.

③ 그 밖에 보안적합성 검증 생략제품의 경우 국가정보원장이 배포한「국가·공공기관 보안적합성 검증가이드」을 준수하여 검증 기관의 장에게 자료를 제출하여야 한다.

제35조(안전성 시험) <삭제 2021.2.25>

제36조(검증결과 통보에 따른 조치) 보안담당관은 검증신청 결과 제품의 보안기능 보완 등 개선조치가 필요하다고 통보받은 경우 해당 내용에 대한 보완조치를 실시하고 그 결과를 검증기관의 장에게 통보하여야 한다.

제37조(취약점 조치) ① 보안담당관은 보안적합성 검증이 완료된 제품에서 새로운 취약점이 발견된 경우 이를 제거 또는 보완하고 그 결과를 국가정보원장에게 통보하여야 한다.

② 국가정보원장은 보안적합성 검증이 완료된 제품에서 새로운 취약점이 발견된 경우 해당 제품을 개발·유통하는 자 또는 도입·운용중인 기관의 장에게 취약점의 제거 또는 보완조치를 요청할 수 있다.<개정 2022.1.27>

③ 제2항에 따라 요청을 받은 기관의 장은 취약점의 제거 또는 보완조치를 실시하고 그 결과를 국가정보원장에게 통보하여야 한다.

제38조(형상변경 및 용도변경 시 조치) 보안담당관은 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.

제39조(도입현황 제출) 보안담당관은 매 분기마다 도입한 제32조에 따른 모든 제품에 대하여 [별지 제13호 서식]에 따른 정보통신제품 도입현황 등을 과학기술정보통신부장관에게 제출하여야 한다.

제3장 정보통신망 및 정보시스템 보안

제1절 정보통신망 보안

제40조(내부망・인터넷망 분리) ① 보안담당관은 내부망과 기관 인터넷망을 분리・운영하여야 한다.

② 보안담당관은 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 차단대책
2. 네트워크 접근관리시스템 설치 등 비(非)인가 장비의 내부망 접속 차단대책
3. 내부망 정보시스템의 인터넷 접속 차단대책
4. 내부망과 기관 인터넷망간 안전한 자료전송 대책
5. 기타 국가정보원장이 배포한「국가・공공기관 업무전산망 분리 및 자료전송 보안가이드라인」에서 제시하는 보안대책

③ 보안담당관은 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 보안담당관은 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 원본 파일은 3개월 이상, 전송기록은 6개월 이상 유지
4. 정기적으로 전송실패 기록을 확인하고 악성코드 유입여부 등 점검
5. 내부망 자료를 기관 인터넷망으로 전송할 경우 분임정보보안담당관 또는 결재권자의 사전 또는 사후 승인절차 마련

⑤ 보안담당관은 내부망과 기관 인터넷망의 IP주소 현황을 정기적으로 확인하고 갱신하여야 한다.

⑥ 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.<신설 2022.1.27>

제41조(클라우드컴퓨팅 보안) ① 보안담당관은「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제12조에 따라 클라우드컴퓨팅(「행정기관 및 공공기관 정보자원 통합기준(행정안전부 고시)」제2조 제5호에 따른 공공클라우드센터를 포함한다)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 2022.1.27>

② 보안담당관은「전자정부법」제54조의2 및「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」제20조에 따라 민간 클라우드컴퓨팅서비스(「행정기관 및 공공기관 정보자원 통합기준(행정안전부

고시)」 제2조제4호에 따른 민간클라우드센터를 포함한다)를 이용하고자 할 경우 다음 각 호에 해당하는 사항을 준수하여야 한다.<개정 2022.1.27>

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 행정안전부장관이 배포한「행정·공공기관 민간 클라우드 이용 가이드라인」에 따른 절차 이행

③ 내부망과 연동된 공공 전용(專用) 클라우드는 이 지침을 적용함에 있어 내부망으로 본다.

④ 기관 인터넷망과 연동된 공공 전용(專用) 클라우드는 이 지침을 적용함에 있어 기관 인터넷망으로 본다.

⑤ 제2항에 따라 민간 클라우드컴퓨팅서비스를 이용할 경우 보안담당관은 클라우드컴퓨팅서비스 제공자에 의하여 누출금지정보가 유출된 경우 제31조에 따른 조치를 취하여야 한다.

제42조(보안·네트워크장비 보안)

① 보안담당관은 침입차단·탐지시스템, 스위치·라우터 등 기관 정보통신망 구성 또는 기관 정보보안 정책 전반에 영향을 미치는 보안·네트워크 장비를 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 항목의 경우 지정 단말기를 통한 접속 관리 허용
   가. 장비 관리자의 접속
   나. 제28조의2 2항 단서에 따른 진흥원내 용역업체 작업장소에서의 접속

② 정보시스템 관리자는 로그기록을 1년 이상 유지하여야 하고 비(非)인가자의 접속여부를 정기적으로 점검하여 그 결과를 정보보안담당관에게 통보하여야 한다.<개정 2022.12.23.>

③ 정보시스템 관리자는 침입차단·탐지시스템의 침입차단·탐지규칙(rule)의 생성 근거를 유지하고 정기적으로 필요성 여부를 점검·갱신하여야 한다.<개정 2022.12.23.>

제43조(무선랜 보안) ① 보안담당관은 내부망을 제외한 정보통신망에서 다음 각 호의 경우와 같이 청사 내에 무선랜(WiFi)을 구축·운용할 수 있다.

1. 기관 인터넷망에 중계기(AP)를 설치하여 제74조제1항에 따라 기관이 지급한 단말기의 접속만을 허용하는 업무용 무선랜
2. 상용 인터넷망에 중계기(AP)를 설치하여 제79조제1항에 따라 반입한 소속직원이 개인 소유 이동통신단말기의 접속만을 허용하는 무선랜
3. 상용 인터넷망에 중계기(AP)를 설치한 외부인 전용(專用) 무선랜

② 보안담당관은 제1항에 따라 무선랜을 구축·운용하고자 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 할당 기록 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. 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 정보보안담당관은 제2항 및 제3항에 따른 보안대책의 적절성을 수시로 점검·보완하여야 한다.

제44조(이동통신망 보안) ① 보안담당관은 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 보안담당관은 제1항에 따라 이동통신망을 이용한 시스템을 구축·운용할 경우 기관 정보통신망과 혼용되지 않도록 하여야 한다.

제45조(영상회의시스템 보안) ① 보안담당관은 영상회의시스템을 구축·운용하고자 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 보안담당관은 다음 각 호의 구분에 따라 상용 소프트웨어에 탑재된 영상회의 서비스를 이용할 수 있다. <개정 2022.1.27>

1. 비공개 업무자료를 취급하거나 회의 내용이 비공개 업무자료에 준하다고 판단할 경우 : 영상·음성·업로드 데이터가 국내 서버로만 전송되는 상용 영상회의 소프트웨어(이하 “국내 영상회의 솔루션” 이라 한다)를 활용.<신설 2022.1.27>

2. 공개 업무자료를 취급하거나, 회의 내용이 공개 업무자료에 준하다고 판단할 경우 : 국내 영상회의 솔루션 또는 그 밖의 영상회의 소프트웨어를 활용<신설 2022.1.27>

④ 전항 제1호에도 불구하고, 다음 각 호의 어느 하나에 해당하는 등 정당한 사유가 있는 경우 국가정보원장과 협의하여 국내 영상회의 솔루션 外의 소프트웨어를 일시적 또는 정기적으로 활용할 수 있다.<개정 2022.1.27>

1. 안보·국익상 필요한 외국기관(외국軍을 포함한다)과의 영상회의 시 상대방이 국내 영상회의 솔루션을 활용할 수 없거나, 상대방이 국내 영상회의 솔루션 外의 소프트웨어 활용을 제안할 경우 <신설 2022.1.27>

2. 정책자문 등의 목적으로 민간인과 영상회의 시 상대방이 국내 영상회의 솔루션을 활용할 수 없는 경우<신설 2022.1.27>

⑤ 기타 영상회의 보안과 관련한 사항은 국가정보원장이 배포한「원격업무 통합보안매뉴얼」을 준수하여야 한다.<신설 2022.1.27>

제46조(인터넷전화 보안) ① 보안담당관은 인터넷전화시스템을 구축·운용하거나 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·운용
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·운용
6. 백업체제 구축

② 보안담당관은 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.

제47조(인터넷 사용제한) ① 보안담당관은 국가비상사태 및 대형 재해·재난의 발생, 사이버공격 등으로부터 정보통신망과 정보시스템의 정상적인 운영을 보장하기 위하여 소속직원에 대한 인터넷 사용을 일부 제한할 수 있다.

② 보안담당관은 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 제66조 제4항에 따른 상용 정보통신서비스의 접속을 제한할 수 있다.

제48조(외교통신 보안) ① 보안담당관은 재외공관과 비밀 등 중요자료를 소통하고자 할 경우 국가정보원장이 개발하거나 안전성을 확인한 암호자재를 사용하는 외교정보통신망을 사용하여야 한다.

② 보안담당관은 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 보안담당관은 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.

제48조의2(파견자용 정보통신망)

① 보안담당관은 다른 기관에 파견된 인원의 활용을 위하여 파견기관의 장과 협의하여 원(原) 소속기관의 정보통신망 전용(專用) 단말기를 파견기관에 설치·운영할 수 있다.

② 보안담당관은 제1항에 따라 단말기를 설치할 경우 단말기와 기관 정보통신망간 소통내용을 보호하여야 한다.

③ 제1항에 따라 내부망과 연동된 단말기는 이 지침을 적용함에 있어 진흥원의 내부망 단말기로 본다.

④ 제1항에 따라 기관 인터넷망과 연동된 단말기는 이 지침을 적용함에 있어 진흥원의 기관 인터넷망 단말기로 본다.

제49조(재외사무소 정보보안점검) ① 보안담당관은 외국에 사무소를 개설·운영할 경우 정보보안담당관으로 하여금 해당 사무소의 정보통신망 및 정보시스템에 대한 보안관리 실태를 점검하고 취약요인을 개선하도록 하여야 한다.

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

제2절 정보시스템 보안

제50조(정보시스템 보안책임) ① 보안담당관은 정보시스템(PC·서버·네트워크장비·정보통신기기·휴대용저장매체 등을 포함한다)을 도입·운용할 경우 해당 정보시스템에 대하여 정보시스템 관리자 및 관리책임자를 지정·운영하여야 한다.<개정 2022.12.23.>

② 정보시스템 관리자 및 관리책임자는 서버·네트워크장비 등 부서가 공동으로 사용하는 정보시스템의 운용·관리에 대한 보안책임을 진다.<개정 2022.12.23.>

③ 정보시스템 관리책임자는 정보시스템을 실제 운용하는 부서의 장이 되며, 정보시스템 관리책임자는 [별지 제3호 서식]에 따른 정보시스템 관리대장을 수기 또는 전자적으로 작성·관리하여야 한다.<개정 2022.12.23.>

④ 정보시스템 관리책임자는 해당 부서의 [별지 제3호 서식]에 따른 정보시스템 관리대장에 정보시스템의 최종 변경 현황을 유지하여야 하며 사본 1부를 정보보안담당관에게 제출하여야 한다.<개정 2022.12.23.>

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.<개정 2022.12.23.>

제51조(정보시스템 유지보수) ① 보안담당관은 정보시스템의 유지보수와 관련한 절차, 주기, 문서화 등과 관련한 사항을 자체 내규(또는 지침 등)에 포함하여야 한다. 정보시스템의 유지보수 절차 및 문서화를 수립할 경우 고려사항은 다음 각 호와 같다.

1. 유지보수 인원에 대한 보안서약서 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 제28조의2 제1항에 따른 진흥원내 용역업체 작업장소로 반출·입할 경우 악성코드 감염여부 및 자료 무단 반출여부 확인 등 보안조치를 실시하고 그 결과를 정보보안담당관에게 제출하여야 한다.<개정 2022.12.23.>

③ 정보시스템 관리자는 직접 또는 용역업체를 활용하여 정보시스템을 유지 보수할 경우 콘솔 또는 지정된 단말기로부터의 접속만을 허용하여야 한다.<개정 2022.12.23.>

④ 정보시스템 관리자는 정보시스템의 기능 개선·오류 수정 등을 위한 프로그램 개발이 완료된 경우 정상 동작여부 등 안전성을 확인한 후 적용하여야 한다.<개정 2022.12.23.>

⑤ 보안담당관은 소관 정보시스템에 대하여 중요도·가용성 등에 따라 등급을 분류하고 해당

등급에 맞게 정보 보존 및 관리, 장애관리, 보안관리 등을 수행하여야 한다.

제52조(지정 단말기를 통한 온라인 유지보수) ① 제51조 제3항에 따른 지정된 단말기를 통해 유지보수를 함에 있어 보안담당관이 필요하다고 판단하고 용역업체가 다음 각 호에 따른 보안대책에 서면으로 동의하는 경우에 한하여, 보안담당관은 용역업체에게 소관 정보시스템(제42조 제1항에 따른 보안·네트워크장비를 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. 발주기관내 설치된 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, 발주기관의 상급기관 및 국가정보원장의 정기 또는 수시 점검(불시 점검을 포함한다) 수검
6. 기타 국가정보원장이 배포한「국가·공공기관 용역업체 보안관리 가이드라인」에서 제시된 온라인 유지보수에 관련된 보안대책의 준수

② 전항 제2호 및 제3호에도 불구하고 온라인 용역 통제시스템이 구축되지 않은 경우 온라인 유지보수를 즉시 실시하지 않고서는 기관 업무수행에 현저한 저해가 있다고 예상되는 경우에는 인터넷망 정보시스템에 한하여 직접 접속하는 온라인 유지보수를 일시적으로 허용할 수 있다. <신설 2022.1.27>

③ 기타 정보시스템 온라인 유지보수 보안과 관련한 사항은 제27조(용역업체 보안)를 준용한다.

제53조(서버 보안) ① 보안담당관은 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 접근권한 차등 부여
2. 개별사용자별 자료 접근범위를 서버에 등록하여 인가여부를 식별하도록 하고 인가된 범위 이외의 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 관리용 단말기 지정·운용
5. 서버 설정 정보 및 저장자료에 대한 정기적 백업 실시
6. 데이터베이스에 대하여는 개별사용자의 직접 접속 차단, 개인정보 등 중요정보 암호화 등 데이터베이스별 보안조치 실시

② 서버관리자는 제1항에 따른 보안대책의 적절성을 수시 확인하여야 하며 연1회 이상 서버 설정 정보와 저장자료의 절취 및 위·변조 가능성 등 보안취약점을 점검·보완하여야 한다.<개정 2022.12.23.>

제54조(공개서버 보안) ① 보안담당관은 외부인에게 공개할 목적으로 웹서버 등 공개서버를 구축·운용하고자 할 경우 내부망과 분리된 영역(DMZ)에 설치하여야 한다.

② 보안담당관은 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.<개정 2022.12.23.>
④ 공개서버 관리자는 공개서버 서비스에 필요한 프로그램을 개발·시험하기 위하여 사용한 도구 (컴파일러 등) 및 서비스와 관계가 없는 산출물은 개발 완료 후 삭제하여야 한다.<개정 2022.12.23.>
⑤ 기타 공개서버 보안과 관련한 사항은 제53조(서버 보안)를 준용한다.

제55조(로그기록 유지) ① 보안담당관은 정보시스템의 효율적인 통제·관리 및 사고 발생 시 추적 등을 위하여 로그기록을 유지·관리하여야 한다.
② 제1항에 따른 접속기록에는 다음 각 호의 사항이 포함되어야 한다.
1. 접속자, 정보시스템·응용프로그램 등 접속대상
2. 로그온·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 접속기록을 생성하는 정보시스템의 경우 시간 동기화 프로토콜(NTP) 적용 등을 통해 정확한 기록을 유지하여야 한다. <개정 2022.12.23.>
④ 정보시스템 관리자는 접속기록을 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.<개정 2022.12.23.>
⑤ 정보시스템 관리자는 접속 및 로그기록을 1년 이상 보관하여야 하며 접속 및 로그기록의 위·변조 및 외부유출 방지대책을 수립·시행하여야 한다.<개정 2022.12.23.>

제56조(업무용 통신단말기 보안) ① 보안담당관은 업무용 통신단말기를 이용하여 업무자료 등 중요 정보를 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 보안담당관은 제1항에 따른 보안대책을 수립하기 위하여 국가정보원장에게 취약점 점검 및 기술 지원을 요청할 수 있다.
③ 보안담당관은 제1항제1호에 따른 통신단말기 개별사용자를 대상으로 인증 및 암호화에 필요한 디지털정보를 발급할 수 없을 경우 국가정보원장이 배포한「정보통신기기 암호기술 적용지침」을 준수하여야 한다.
④ 보안담당관은 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 제101조에 따라 보안대책을 수립·시행하여야 한다. <개정 2022.1.27>

제57조(모바일 업무 보안) ① 보안담당관은 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.

제58조(사물인터넷 보안) ① 보안담당관은 사물인터넷을 이용한 시스템을 구축・운용하고자 할 경우 사물인터넷 기기 및 중요 데이터 등을 보호하기 위하여 보안대책을 수립・시행하여야 한다.
② 보안담당관은 사물인터넷을 이용한 시스템을 구축・운용하고자 할 경우 내부망과 분리하여야 한다. 다만, 내부망과 연동이 필요한 경우에는 망간 자료전송제품 설치 등 보안대책을 수립하여야 한다.
③ 보안담당관은 사물인터넷 서비스를 위한 소프트웨어를 개발할 경우 제28조(소프트웨어 개발 보안)를 준수하여야 한다.
④ 기타 사물인터넷 보안과 관련한 사항은 국가정보원장이 배포한 「국가・공공기관 사물인터넷(IoT) 보안가이드라인」을 준수하여야 한다.

제59조(원격근무 보안) ① 보안담당관은 소속직원이 재택근무, 출장지 현장 근무 또는 파견 근무(제48조의2에 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.<개정 2021.2.25>
② 제1항에 따른 원격근무를 위해 접속할 수 있는 기관 정보시스템은 다음 각 호와 같다.<개정 2021.2.25>
1. 기관 인터넷망에 위치한 서버 및 서버에서 구동되는 가상 PC<개정 2022.1.27>
2. 제40조제2항제4호에 따른 방법을 통해 접속할 수 있는 내부망 서버 및 내부망 서버 에서 구동되는 가상 PC<개정 2022.1.27>
③ 제1항에 따른 원격근무로 취급할 수 있는 업무자료의 범위는 공개 및 비공개 업무자료로 한다.
④ 보안담당관은 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. 원격근무자는 원격근무시스템 접속과정에서 제1호부터 제3호까지의 보안대책을 준수토록 조치
5. 원격근무시스템에 대한 보안취약점 정기 점검
⑤ 원격근무자는 보안담당관이 원격근무용 단말기(개인 소유의 정보통신기기를 포함한다)의 보안을 위하여 취하는 다음 각 호의 조치에 적극 협조하여야 한다.
1. 제4항에 따라 보안담당관이 제공하는 보안소프트웨어 설치・운영
2. 사이버공격 등으로 인한 자료유출 사고 발생 시 보안담당관이 요청하는 점검 및 제118조 제3항에 따른 자료제출 요청 협력
3. 소속된 기관에서 지급받은 단말기의 경우 제74조에 따른 단말기 보안대책 준수
⑥ 보안담당관은 원격근무자에게 제5항에 따른 보안조치 등이 포함된 보안서약서를 징구하고 직위・임무에 부합한 정보시스템 접근권한 부여 및 보직변경・퇴직 등 변동사항이 발생시 접근권한 조정 등의 절차를 마련・시행하여야 한다.

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

제60조(국제회의 보안) ① 보안담당관은 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.

제61조(저장매체 불용처리) ① 보안담당관은 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 개발사용자는 분임정보보안담당관과 협의하여야 한다.<개정 2022.12.23.>

② 제1항에 따라 자료를 삭제할 경우 진흥원의 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

제62조(비밀의 전자적 처리) ① 보안담당관은 「보안업무규칙」에 따라 비밀의 생산, 분류, 보관, 열람, 출력, 송·수신, 이관, 파기 등을 전자적으로 처리할 수 있다.

② 국가정보원장은 비밀을 전자적으로 처리하는데 필요한 관련기술을 개발하여 보급할 수 있다.

③ 보안담당관은 비밀을 전자적으로 처리하는 전(全) 과정에서 기밀성, 무결성, 인증, 부인방지 등 보안성을 확보하여야 하며, 이를 위하여 국가정보원장이 개발하거나 안전성을 확인한 암호자재를 사용하여야 한다.

④ 제1항에 따라 비밀을 전자적으로 처리할 경우 내부망 PC에서 처리하여야 한다.

⑤ 종이문서로 출력된 비밀의 관리에 관하여는「보안업무규칙」을 준수하여야 한다.

제63조(비밀관리시스템 운용) ① 국가정보원장은 비밀을 전자적으로 안전하게 처리하기 위하여 비밀관리시스템을 개발·보급할 수 있으며 보안담당관은 이 시스템을 도입·운용할 수 있다.

② 비밀관리시스템을 구축한 보안담당관은 비밀의 생산·보관·유통 등 전반에 대하여 비밀관리

시스템을 활용하여 비밀을 안전하게 관리하여야 한다.

③ 국가정보원장은 비밀관리시스템의 안전한 운용·관리를 위하여 필요한 사항을 정하여 보안담당관에게 배포할 수 있다.

④ 보안담당관은 비밀관리시스템을 자체적으로 개발·운용하고자 할 경우 제64조에 따른 비밀의 전자적 처리 규격을 준수하여 개발하여야 한다.

⑤ 국가정보원장은 제4항에 따라 보안담당관이 자체적으로 개발한 비밀관리시스템에 대하여 보안성 및 적절성을 확인할 수 있다.

제64조(비밀의 전자적 처리 규격) 국가정보원장은 비밀관리시스템의 개발에 필요한 다음 각 호의 사항을 포함한 비밀의 전자적 처리 규격을 정한다.

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

제65조(대외비의 전자적 처리) ① 보안담당관은 대외비를 전자적으로 처리하고자 할 경우에는 검증필 암호모듈을 사용하여 위조·변조·훼손 및 유출 등을 방지하기 위한 보안대책을 강구하여야 한다. <개정 2022.1.27>

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

제66조(비공개 업무자료 처리) ① 소속직원은 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 보안담당관이 지급한 휴대용 저장매체에 작성 및 저장·보관<개정 2022.1.27>
3. 다음 각 목의 어느 하나에 해당하는 수단(이하 “업무자료 공식 소통수단” 이라 한다)을 이용한 수·발신 또는 등재·열람
   가. 진흥원이 자체적으로 구축·운용하는 전자우편시스템(이하 “기관 전자우편”이라 한다)
   나. 소속직원이 다른 직원과 자료를 공유하거나 소통하기 위하여 사용하는 전용(專用) 소프트웨어(이하 “사내 메신저”라 한다)
4. 그 밖에 다른 법규에 따라 허용되는 처리방법

② 소속직원은 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 경우 소속 또는 근무중인 기관의 보안담당관이 지급한 인터넷 PC 또는 출장용 노트북을 이용하여 비공개 업무자료를 처리할 수 있다.<개정 2022.1.27>

1. 업무자료 공식 소통수단의 발신 또는 등재 기능을 이용하여 제3조 제14호 다목의 문장 또는 문구 작성

2. 업무자료 공식 소통수단으로 수・발신 또는 등재・열람하는 과정에서의 일시적 저장

3. 제40조제5항에 따른 기관 인터넷망 PC에 작성・저장

4. 제45조 제3항 및 제4항에 따라 영상회의 솔루션을 활용하여 비공개 업무자료의 화면 영상을 공유하기 위한 일시적 저장<신설 2022.1.27>

③ 소속직원은 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 제3조제14호다목의 문장 또는 문구 작성

2. 업무자료 공식 소통수단으로 수・발신 또는 등재・열람 과정에서의 일시적 저장

3. 제59조제4항에 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 근무중인 기관에 제59조제4항에 따른 원격근무시스템이 구축되지 아니한 경우

5. 제45조 제3항 및 제4항에 따라 영상회의 솔루션을 활용하여 비공개 업무자료의 화면 영상을 공유하기 위한 일시적 저장<개정 2022.1.27>

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

④ 소속직원은 제3항 제4호에 해당하는 경우를 제외하고는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조 제1항 제2호에 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 소속직원은 제2항부터 제4항까지에 따라 작성・저장한 비공개 업무자료는 활용이 종료된 후에는 삭제하여야 한다.

제66조의2(특정 상황별 비공개 업무자료 처리) ① 소속직원은 「국회법」제128조제2항, 「국정감사 및 조사에 관한 법률」제10조제2항, 「국회증언감정법」제2조 및 제4조에 따라 국회・정부간 비공개 업무자료를 소통할 경우에는 우선적으로 제66조 제1항 제3호 라목의 의정자료전자유통시스템을 활용하여 처리하여야 하며, 시스템 장애 등 부득이한 사유로 활용이 곤란할 경우에 한해 제66조에 허용된 다른 방법으로 처리할 수 있다.<신설 2022.1.27>

② 감독・감사・조사 등의 관계 법령에 따라 비공개 업무자료를 제출받을 권한이 있는 소속직원은 업무자료를 제출할 상대방 공무원등에게 제66조에 위반되는 방법으로 자료 제출을 요구하여서는 아니 된다.<신설 2022.1.27>

③ 소속직원이 자문 등의 목적으로 비공개 업무자료를 업무자료 공식 소통수단을 활용할 수 없는 민간인에게 발신하거나 민간인으로부터 수신 받고자할 경우에는 소속 기관 전자우편 또는 공직자통합메일을 활용해발신하거나 수신 받아야 한다.<신설 2022.1.27>

제67조(행정전자서명 인증서 등 관리) ① 소속직원은 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 소속직원은 행정전자서명 인증서 및 인증서의 비밀번호, 기관 전자우편 비밀번호 등을 상용

정보통신서비스를 이용하여 수·발신하거나 저장·보관하여서는 아니 된다.

제68조(비공개 업무자료 유출방지) ① 보안담당관은 제66조에 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. <개정 2022.1.27>

② 보안담당관은 소속직원이 사내 메신저 이용을 활성화할 수 있도록 노력하여야 한다.

제69조(공개 업무자료 처리) 소속직원은 관계 법규에 위배되지 않는 범위 내에서 인터넷 PC나 개인이 소유한 PC·휴대용 저장매체·휴대폰, 상용 정보통신서비스 등을 이용하여 공개 업무자료를 처리할 수 있다.

제70조(홈페이지 등 게시자료 보안) ① 보안담당관은 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.<개정 2022.12.23.>

③ 분임정보보안담당관은 소속 부서에서 운용하는 홈페이지에서 비공개 업무자료가 무단 게시되었는지 여부를 정기적으로 점검하여야 한다.<개정 2022.12.23.>

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

제71조(정보통신망 현황자료 관리) ① 보안담당관은 정보통신망과 관련한 다음 각 호에 해당하는 자료를「보안업무규정 시행규칙」제17조에 의거 국가정보원장이 배포한「비밀세부분류지침」에 따라 비밀로 분류·관리하여야 한다.

1. 국방 연구개발 및 정보통신 관련자료
2. 암호자재 운용현황
3. 국가보안시설(보호장비를 포함한다)의 운영·관리에 필요한 정보통신망 구성현황(IP주소 할당 현황을 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 보안담당관은 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 보안담당관은 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.

제72조(빅데이터 보안) ① 보안담당관은 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) 권한부여 체계 수립
6. 데이터 파기절차 수립

② 그 밖에 빅데이터 보안과 관련한 사항은 개인정보위원회가 고시한「개인정보의 안전성 확보조치 기준」 및 국가정보원장이 배포한「국가·공공기관 빅데이터 보안 가이드라인」을 준수하여야 한다. <개정 2022.1.27>

제4절 사용자 보안

제73조(개별사용자 보안) ① 보안담당관은 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 보안조치<개정 2022.1.27>
3. 보직변경, 퇴직 등 변동사항 발생시 정보시스템 접근권한 조정

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

제74조(단말기 보안) ① 개별사용자는 진흥원에서 지급받은 PC·노트북·휴대폰·스마트패드·휴대용 저장매체 등 (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 중단 시 비밀번호 등을 적용한 화면보호 조치
3. 최신 백신 소프트웨어 및 침입차단·탐지시스템 등 운용 및 수시 점검
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 보안담당관이 정한 특별한 사유가

없는 한 문서 프로그램을 읽기 전용(專用)으로 운용<개정 2022.1.27>

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

③ 부서의 장은 정보보안담당관 총괄 하에 개별사용자의 제2항 각 호에 해당하는 보안대책의 준수 여부를 정기적으로 점검하고 개선 조치하여야 한다. <개정 2022.1.27>

④ 개별사용자는 업무 상 불가피한 사유로 PC 보안정책에 대하여 예외적인 적용을 받고자 할 경우, 정보보안담당관이 정하는 절차에 따라 별지 제15호 서식의 신청서를 제출하여 예외신청을 하여야 한다.

제75조(계정 관리) ① 정보시스템 관리자는 개별사용자에게 소관 정보통신망 또는 공용(公用) 정보시스템의 접속에 필요한 사용자 계정(아이디)을 부여하고자 할 경우 다음 각 호에 해당하는 사항을 준수해야 한다.<개정 2022.12.23.>

1. 개별사용자별 또는 그룹별 접근권한 부여
2. 외부인에게 계정을 부여하지 아니하되 업무상 불가피한 경우 정보시스템 관리책임자 책임 하에 보안 조치 후 필요한 업무에 한하여 일정기간 동안 접속 허용 <개정 2022.12.23.>
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 침입여부를 점검하여야 한다. <개정 2022.12.23.>

③ 정보시스템 관리자는 개별사용자의 보직변경, 퇴직, 계약종료 등 변동사항이 발생할 경우 신속히 사용자 계정을 삭제하거나 부여된 접근권한을 회수하여야 한다. <개정 2022.12.23.>

④ 정보시스템 관리자는 사용자 계정 부여 및 관리의 적절성을 연2회 이상 점검하고 그 결과를 정보보안담당관에게 통보하여야 한다.<개정 2022.12.23.>

⑤ 정보시스템 관리자는 제1항 및 제3항에 의한 접근권한 부여, 변경, 회수 또는 삭제 등에 대한 내역을 기록하고 3년 이상 보관하여야 한다.<개정 2022.12.23.>

제76조(비밀번호 관리) ① 개별사용자 및 정보시스템 관리자는 각 종 비밀번호를 다음 각 호에 해당하는 사항을 반영하고 숫자・문자・특수문자 등을 혼합하여 안전하게 설정하고 정기적으로 변경・사용하여야 한다.<개정 2022.12.23.>

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 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.<개정 2022.12.23.>

③ 정보보안담당관은 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.<개정 2022.12.23.>

제77조(전자우편 보안) ① 보안담당관은 전자우편을 컴퓨터바이러스·트로이목마 등 악성코드로부터 보호하기 위하여 백신 소프트웨어 설치, 해킹메일 차단시스템 구축 등 보안대책을 수립·시행하여야 한다.

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

③ 보안담당관은 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 과학기술정보통신부장관 및 국가정보원장에게 통보하여야 한다.

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

제78조(휴대용 저장매체 보안) ① 보안담당관은 휴대용 저장매체를 사용하여 업무자료를 보관하고자 하는 경우 자료의 위·변조, 저장매체의 훼손·분실 등에 대비한 보안대책을 수립·시행하여야 한다.

② 보안담당관은 휴대용 저장매체 관리시스템을 운용하고자 하는 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 검사하도록 기능을 설정하여야 한다.

④ 정보보안담당관는 휴대용 저장매체를 비밀용·일반용으로 구분·관리하고 수량 및 보관 상태를 정기적으로 점검하며 외부 반출·입을 통제하여야 한다.

⑤ 정보보안담당관은 비밀이 저장된 휴대용 저장매체는 매체별로 비밀등급 및 관리번호를 부여하고 비밀관리기록부에 등재·관리하여야 한다. 이 경우 매체 전면에 비밀등급 및 관리번호가 표시되도록 하여야 한다.<개정 2022.1.27>

⑥ 정보보안담당관은 비밀용 휴대용 저장매체를 다른 등급의 비밀용 또는 일반용으로 변경 사용하고자 할 경우 저장자료가 복구 불가하도록 완전삭제 소프트웨어 등을 이용하여 삭제하여야 한다. 다만, 완전삭제가 불가할 경우 변경 사용하여서는 아니 된다.

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

⑧ 정보보안담당관은 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.

제79조(비인가 기기 통제) ① 소속직원은 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 소속직원은 제1항 각 호에 따라 반입한 개인 소유의 정보통신기기를 내부망 및 기관 인터넷망(제43조 제1항 제1호에 따른 무선랜을 포함한다)에 연결하여서는 아니되며, 내부망 및 기관 인터넷망 정보시스템을 상용 인터넷망에 연결하는 수단으로 사용하여서는 아니 된다. 정보보안담당관은 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 등 보안대책을 수립・시행하여야 한다.

제80조(악성코드 감염 방지대책) ① 보안담당관은 웜·바이러스, 해킹프로그램, 스파이웨어, 랜섬웨어 등 악성코드 감염을 방지하기 위하여 다음 각 호의 대책을 수립·시행하여야 한다.

1. 사용자는 개인PC에서 작성하는 문서·데이터베이스 작성기 등 응용프로그램을 보안패치하고 백신은 최신상태로 업데이트·상시 감시상태로 설정 및 주기적인 점검을 실시하여야 한다.

2. 사용자는 출처, 유통경로 및 제작자가 명확하지 않은 응용프로그램 사용을 금지하고 인터넷 등 상용망으로 자료 입수 시 신뢰할 수 있는 인터넷사이트를 활용하되 최신 백신으로 진단 후 사용하여야 한다.

3. 사용자는 인터넷 파일공유 프로그램과 메신저·대화방 프로그램 등 업무상 불필요한 프로그램 사용을 금지하고 정보시스템 관리자는 인터넷 연동구간의 침입차단시스템 등에서 관련 사이트 접속을 차단하도록 보안설정 하여야 한다. <개정 2022.12.23.>

4. 사용자는 웹브라우저를 통해 서명되지 않은(Unsigned) Active-X 등이 PC내에 불법 다운로드 되고 실행되지 않도록 보안설정을 하여야 한다.

5. 제1호부터 제4호까지의 보안대책과 관련하여 정보보안담당관은 사용자가 적용할 수 있는 보안기술을 지원하여야 한다.

② 정보시스템 관리자 또는 PC 등의 사용자는 시스템에 악성코드가 설치되거나 감염된 사실을 발견하였을 경우에 다음 각 호의 조치를 하여야 한다. <개정 2022.12.23.>

1. 악성코드 감염원인 규명 등을 위하여 파일은 임의삭제 등 감염 시스템 사용을 중지하고 전산망과의 접속을 분리한다.

2. 악성코드의 감염확산 방지를 위하여 정보보안담당관 또는 과학기술정보통신부 사이버안전센터에 관련 내용 및 보안조치 사항을 즉시 신고한다.

③ 정보보안담당관은 악성코드가 신종이거나 감염피해가 심각하다고 판단할 경우에는 관련사항을 국가사이버안전센터에 통보하여야 한다.

④ 보안담당관은 과학기술정보통신부장관 및 국가정보원장이 진흥원에 악성코드 감염사실을 확인하여 조치를 권고할 경우, 즉시 이행하여야 한다. 또한 악성코드의 감염 등 이상 징후가 감지될 경우에는 과학기술정보통신부 사이버안전센터에 즉시 신고하여야 한다.

제81조(위규자 처리) ① 정보보안 관련 규정 위반사항에 대한 위규자 처리는 위반사항의 정도에 따라 인사규정 제37조의12(보안준수 의무 불이행 징계처분)에 따른다.<개정 2022.12.23.>
② 정보보안 관련 법령에 대한 경미한 위반사항은 [별표1]에서 정하며, 정보보안담당관은 위규자에 대해 재발 방지대책이 포함된 경위서를 징구하고 재발방지 교육을 실시한다.<개정 2022.12.23.>
③ 정보보안 관련 위규사항이 중대한 경우 보안업무규칙 제9조에 따라 구성·운영되는 내부 보안심사위원회를 개최하여 위규자에 대한 징계위원회에 회부여부를 결정한다. 징계위원회에 회부하는 경우 인사규정 제37조의12(보안준수 의무 불이행 징계처분)에 따른다. <신설 2022.12.23.>

제5절 주요정보통신기반시설 보호

제82조(주요정보통신기반시설 지정·보호) ① 과학기술정보통신부장관은 「정보통신기반 보호법」에 따라 소관분야의 정보통신기반시설 중 중요성을 고려하여 주요정보통신기반시설의 지정할 수 있다.
② 보안담당관은 각종 전자적 침해행위로부터 보호하기 위하여 보호대책 수립하고 침해사고에 대비하여야 한다.<개정 2022.1.27>
③ 기타 주요정보통신기반시설 지정·보호 등에 관련된 사항은「과학기술정보통신부 소관 주요정보통신기반시설 보호지침」을 따른다.

제83조(취약점 분석・평가 결과물 관리) ① 보안담당관은「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.<개정 2022.1.27>
② 보안담당관은 제1항에 따른 취약점 분석・평가를 완료한 경우 취약점 분석・평가 결과물에 대하여 적절성을 검증하여야 한다. <개정 2022.1.27>
③ 보안담당관은 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.<개정 2022.1.27>
④ 보안담당관은 취약점 분석・평가의 효율적인 수행을 위하여 필요한 경우 과학기술정보통신부장관에게 평가 방향 및 중점사항, 평가 결과물의 적절성 검증, 취약점 분석・평가기관 보안점검 등의 지원을 요청할 수 있다.<개정 2022.1.27>

제4장 융합 보안

제1절 정보통신시설 및 기기 보호

제84조(정보통신시설 보호대책) ① 보안담당관은 다음 각 호의 어느 하나에 해당하는 정보통신시설 및 장소를「보안업무규칙」제49조에 따른 보호구역으로 지정・관리하여야 한다.
1. 암호실・정보통신실・전산실

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

② 보안담당관은 제1항에 따라 보호구역으로 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 긴급파기 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・운영 시 보안담당관은 해당 기관의 보안요구사항을 반영하여 보안대책을 수립한 후 이를 과학기술정통부장관과 협의하여 시행하여야 한다.

제85조(정보통신시설 출입관리) ① 보안담당관은 외부인이 정보통신시설을 방문할 경우 반드시 신원을 확인하고 보안교육 및 보안검색 후 출입을 허용하여야 한다.

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

③ 재외공관의 장은 재외공관의 정보통신시설에 대해 외국인의 출입이 꼭 필요하다고 판단하는 경우 공관 정보보안담당관 입회하에 출입하도록 허용할 수 있다. 이 경우 재외공관의 장은 출입한 외국인의 출입 목적・일시・장소・인원 정보를 5년 이상 기록・유지하여야 한다.

제86조(영상정보처리기기 보안) ① 보안담당관은 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・운용하고자 할 경우 운영자의 계정・비밀번호 설정 등 인증대책을 수립하고 특정 IP주소에서만 접속 허용 등 비(非)인가자 접근 통제대책을 수립・시행하여야 한다.

② 보안담당관은 영상정보처리기기를 통합・운용하는 시설(이하 “영상관제상황실”이라 한다)을 운영하고자 할 경우 영상관제상황실을「보안업무규칙」제49조에 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「국가 공공기관 영상정보

처리기기 도입ㆍ운영 가이드라인」 및 「안전한 정보통신 환경 구현을 위한 네트워크 구축 가이드라인」을 준수하여야 한다.

제87조(RFID 보안) ① 보안담당관은 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 「국가·공공기관의 무선랜 구축 및 RFID 보안가이드라인」을 준수하여야 한다.

제88조(디지털복합기 보안) ① 보안담당관은 디지털복합기(디지털복사기 등도 포함한다. 이하 "복합기"라 한다)를 설치·운용하고자 할 경우 복합기 내 저장매체가 있거나 장착이 가능한 경우 자료유출을 방지하기 위하여 자료 완전삭제 또는 디스크 암호화 기능이 탑재된 복합기를 도입하여야 한다.

② 복합기 관리 부서의 장은 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 관리 부서의 장은 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 관리 부서의 장은 소모품 교체 등 복합기 유지보수를 할 경우 분임정보보안담당관의 입회·감독 하에 실시하고 저장매체의 무단 교체 등을 예방하여야 한다.

⑤ 복합기 관리 부서의 장은 복합기를 통해 내부망과 기관 인터넷망간 접점이 발생하지 않도록 보안대책을 수립·시행하여야 한다.

⑥ 정보보안담당관은 저장매체가 장착되어 있는 복합기 운용과 관련한 보안대책의 적절성을 수시로 점검·보완하여야 한다.

⑦ 기타 복합기 보안과 관련한 사항은 국가정보원장이 배포한 「정보시스템 저장매체 불용처리 지침」을 준수하여야 한다.

제89조(재난 방지대책) ① 보안담당관은 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애

발생에 대비하여 정보시스템의 이중화, 백업관리 및 복구 등 종합적인 재난 방지대책을 수립·시행하여야 한다.

② 보안담당관은 재난 방지대책을 정기적으로 시험·검토하고 업무 연속성에 대한 영향평가를 실시하여야 한다.

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

④ 보안담당관은 제3항에 따른 백업시설을 구축·운영하고자 할 경우 정보통신실·통합데이터센터와 물리적으로 일정거리 이상 떨어진 안전한 장소에 설치하여야 하며 전력공급원 이중화 등 정보시스템의 가용성을 최대화할 수 있도록 하여야 한다.

제2절 전자파 보안

제90조(대도청 측정) ① 보안담당관은 다음 각 호의 어느 하나에 해당하는 시설·장소에 대하여 각 종 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. <개정 2022.1.27>

1. 기관 청사(신축, 이전 또는 증축, 개축, 대규모 수선 등)
2. 기관 장실, 회의실 등 중요업무 장소
3. 중요회의·회담·협상·행사 장소
4. 기타 대도청 측정이 필요하다고 판단되는 시설·장소·장비

② 보안담당관은 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 상급기관의 장이 관리하는 시설·장소
2. 하급기관의 장이 관리하는 시설·장소 중에서 관계 상급기관의 장이 국가안보 및 국익 보호를 위하여 필요하다고 판단하는 시설·장소

③ 제2항에 따라 자체 또는 불법감청설비탐지업자 등을 활용하여 측정을 실시한 보안담당관은 측정결과 취약요인이 발견된 경우 그 결과를 과학기술정보통신부장관을 거쳐 국가정보원장에게 통보하고 기술 지원 및 추가 측정을 요청할 수 있다.

④ 제2항에 따라 국가정보원장이 측정을 실시한 결과 취약요인이 발견된 경우 보안담당관은 개선대책을 수립·시행하여야 한다.

⑤ 보안담당관은 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.

제91조(무선통신망 보안) ① 보안담당관은 무선통신망(제43조에 따른 무선랜(WiFi)을 제외한다. 이하 본 조에서 같다)을 구축·운영하거나 이동통신망을 이용하여 관련 시스템을 구축·운용 시 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 보안담당관은 연간 전파측정 계획을 수립하여 연1회 전파측정을 실시하여야 한다.

③ 제1항에 따른 보안담당관은 과학기술정보통신부장관에게 제2항에 따른 연간 전파측정 계획서를 매년 1.25까지 제출하고 전파측정 실시 후 20일 이내에 [별지 제29호 서식]에 따른 전파측정 결과 보고서를 제출하여야 하며, 과학기술정보통신부장관은 국가정보원장에게 그 결과를 통보하여야 한다.

제92조(고출력 전자파 보안) ① 보안담당관은 소관 주요기반시설을 고출력 전자파(EMP)로부터 안전하게 보호하기 위한 예방·백업·복구 등 물리적·기술적 대책을 포함한 보호대책을 수립·시행하여야 한다.<개정 2022.1.27>

② 보안담당관은 제1항에 따른 보호대책을 수립하기 위하여 취약점 분석·평가를 실시하여야 하며 이를 위하여 담당자 지정 또는 전담반을 구성할 수 있다.<개정 2022.1.27>

③ 보안담당관은 제1항에 따른 보호대책을 수립할 경우 국가정보원장에게 기술 지원을 요청할 수 있다.<개정 2022.1.27>

제5장 훈련 및 평가

제1절 훈련 및 진단

제93조(사이버공격 대응훈련) 보안담당관은 기관의 정보통신망을 대상으로 매년 정기 또는 수시로 사이버공격 대응훈련을 실시하여야 한다. 이 경우 모의 해킹메일 대응훈련은 전 직원을 대상으로 연 2회 이상 실시하여야 한다.

제94조(정보통신망 보안진단) ① 보안담당관은「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.<개정 2022.1.27>

1. 사이버보안 강화를 위한 길라잡이(정보통신시스템 보안진단 및 대응방법)<개정 2022.1.27>
2. 홈페이지·네트워크·시스템·DBMS 취약점 점검매뉴얼<개정 2022.1.27>
3. 정보보안점검 체크리스트<개정 2022.1.27>

② 보안담당관은 정보통신망에 대한 보안취약점 점검 또는 종합 진단이 필요하다고 판단될 경우, 국가정보원장에게 보안진단을 요청할 수 있다.

제2절 정보보안 관리실태 평가

제95조(정보보안 관리실태 평가) 보안담당관은 국가정보원장이 「사이버안보 업무규정」 제13조, 「전자정부법」 제56조 및 같은 법 시행령 제69조·제70조, 「공공기록물 관리에 관한 법률 시행령」 제5조 등의 규정에 따라 진흥원의 국가 정보보안 정책 이행여부를 확인하기 위해 실시하는 정보보안 관리실태 평가에 협조하여야 한다.<개정 2022.1.27>

제96조(자체 평가) ① 보안담당관은 국가정보원장(또는 과학기술정보통신부장관)이 배포한 평가지표에 따라 자체 평가를 실시하여야 한다.

② 보안담당관은 자체 평가의 적절성을 입증하기 위하여 필요하다고 판단하는 경우 평가지표별 증빙자료를 국가정보원장(또는 과학기술정보통신부장관)에게 제출할 수 있다.

제97조(현장 실사) ① 국가정보원장(또는 과학기술정보통신부장관)은 진흥원이 실시한 자체 평가에 대한 객관성·공정성을 확보하기 위하여 진흥원을 방문하여 자체 평가결과를 검증(이하 "현장실사"라 한다)할 수 있다.

② 보안담당관은 자체 평가에 대한 증빙자료 제출, 담당자 면담 등 협조하여야 한다.

③ 국가정보원장(또는 과학기술정보통신부장관)은 현장 실사를 할 경우 다음 각 호에 해당하는 사항을 수행할 수 있다.

1. 사이버위기 대응능력 점검
2. 정보통신망 및 정보시스템 보안진단
3. PC 등 단말기·휴대용 저장매체 보안관리 실태 확인
4. 소속직원의 정보보안 기본수칙 숙지여부 확인

제98조(개선대책 강구) 보안담당관은 국가정보원장(또는 과학기술정보통신부장관)이 통보한 평가결과를 자체 정보보안 대책 등의 수립 시에 반영하고 취약요소를 개선·보완하여 정보보안 수준을 제고하여야 한다.

제6장 암호자재 및 암호알고리즘

제1절 기본사항

제99조(사용 원칙) ① 보안담당관은 비밀을 소통·보호하고자 할 경우 국가정보원장이 개발하거나 안전성을 확인한 암호자재를 사용하여야 한다. 또한 비밀이 아닌 중요자료를 보호하고자 할 경우에도 암호자재를 사용할 수 있다.

② 보안담당관은 제1항에 따라 암호자재를 사용하고자 할 경우 국가정보원장에게 암호자재 사용에 대한 승인 또는 암호자재 지원을 요청하여야 한다.

③ 보안담당관은 국가정보원장이 승인하지 아니한 암호자재나 외국에서 생산된 암호기능 탑재 시스템을 무단으로 사용하여서는 아니 된다.

제100조(암호자재 설치·운영) ① 보안담당관은 「보안업무규칙」 제49조에 따른 보호구역으로 지정된 장소에서 암호자재를 설치·운영하여야 한다.

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

제101조(운용관리 및 파기) 보안담당관은 암호자재를 운용할 경우「보안업무규칙」을 준수하여야 한다.

제2절 개발 및 제작

제102조(개발 및 제작) ① 암호자재의 개발 및 제작과 관련한 절차는「보안업무규정」제7조 및 국가정보원장이 배포한「국가보안기술 연구개발 지침」을 준수하여야 한다.

제3절 사용승인 및 지원요청

제103조(사용 승인) ① 보안담당관은 암호자재 제작업체로부터 암호자재를 도입·사용하고자 할 경우 다음 각 호의 사항을 포함한 문서를 국가정보원장에게 제출하고 사용 승인을 받아야 한다.

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

② 암호자재 사용 승인을 받은 보안담당관은 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.

제104조(지원 요청) ① 보안담당관은 국가정보원장이 제작·지원하는 암호자재가 필요할 경우 다음 각 호의 사항을 포함한 문서를 제출하고 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 국가정보원장이 제작·지원하는 암호자재를 매년 반복하여 지원받는 보안담당관은 [별지 제8호서식]에 따른 암호자재 신청서를 매년 1.25까지 국가정보원장에게 제출하여야 한다. 이 경우 제1항의 절차를 생략할 수 있다.

제105조(목적 외 사용금지) 보안담당관은 제103조 및 제104조에 따라 암호자재를 사용할 경우 국가

정보원장이 사용 승인 또는 지원한 목적 이외 교육·시험 등 다른 목적으로 사용하여서는 아니 된다. 다만, 국가정보원장이 필요하다고 인정하는 경우에는 그러하지 아니할 수 있다.

제4절 암호알고리즘

제106조(개발 및 지원요청) ① 보안담당관은 비밀이 아닌 업무자료를 암호화하여 소통·보호하고자할 경우 국가정보원장이 개발하거나 안전성을 확인한 암호알고리즘 또는 검증필 암호모듈을 사용하여야 한다. 다만, 필요한 경우 국가정보원장의 승인 하에 자체적으로 개발·사용할 수 있다.
<개정 2022.1.27>

② 보안담당관은 암호알고리즘이 필요한 경우 다음 각 호의 사항을 포함한 문서를 국가정보원장에게 제출하고 지원을 요청할 수 있다.

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

③ 보안담당관은 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 보안담당관은 이를 개선 조치하여야 한다.

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

제107조(적용 및 운용) 보안담당관은 제106조에 따라 국가정보원장으로부터 지원받거나 자체 개발한 암호알고리즘을 정보통신시스템 등에 적용·운용하고자 할 경우 적절한 보안대책을 수립·시행하고 운용 시험을 통한 정상 동작여부 등을 확인하여야 한다.

제108조(반납 및 파기) 보안담당관은 제106조에 따라 국가정보원장으로부터 지원받거나 자체 개발한 암호알고리즘의 실효성이 상실되거나 유효기간이 만료된 경우 지원받은 암호알고리즘은 국가정보원장에게 반납하고 자체 개발한 암호알고리즘은 보안담당관 책임 하에 파기(소자)하고 그 결과를 국가정보원장에게 통보하여야 한다.

제7장 사이버위협 탐지 및 대응

제1절 보안관제

제109조(보안관제센터 설치・운영) ① 보안담당관은 보안관제센터 운영시 국가보안관제체계와 연계 운영하여야 한다. 이 경우 연계 방법은 국가보안관제체계를 운영하는 국가정보원장과 사전 협의하여 정한다.<개정 2022.1.27>

② 보안담당관과 국가정보원장은 보안관제에 필요하다고 판단하는 경우 상호간 기술・인력・장비 등의 지원을 요청할 수 있다.<개정 2022.1.27>

③ 보안담당관은 야간시간대 근무자 관리 등을 위하여 필요하다고 판단하는 경우 관계 기관의 장과 협의하여 근무자 일일 당직보고를 실시할 수 있다.<개정 2022.1.27>

제110조(보안관제 인원) ① 보안담당관은 보안관제센터 운영시 보안관제업무를 24시간 중단 없이 수행하여야하며 이를 담당할 전문 또는 전담인력을 배치하고 교대근무 체계를 운영하여야 한다. 다만, 단위보안관제센터의 경우 보안관제 대상기관의 범위 및 중요성, 보안관제센터의 규모 등을 고려하여 그러하지 아니할 수 있다.<개정 2022.1.27>

②「국가사이버안전관리규정」제10조의2제4항에 따라 보안관제전문업체의 인원을 활용하고자 하는 기관의 장은 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. 보안관제업무의 책임 있는 수행 및 보안관리 등을 위하여 적정한 수의 공무원 또는 정규직원 상시 배치
3. 업체 인원에 대하여 제27조(용역업체 보안) 및 제31조(누출금지정보 유출시 조치) 준용
4. 업체 인원을 대상으로 매월 1회 이상 탐지규칙정보 관리 등에 관한 보안교육 및 점검 실시

제111조(탐지규칙정보 개발 및 배포) ① 보안담당관은 보안관제센터 운영시 국가정보원장과 사이버공격을 탐지할 수 있는 기술정보(이하 “탐지규칙정보”라 한다)를 개발하여 보안관제업무에 활용할 수 있다.<개정 2022.1.27>

② 보안담당관은 보안관제센터 운영시 제1항에 따른 탐지규칙정보를「공공기관의 정보공개에 관한 법률」제9조제1항에 따른 비공개 대상 정보 및「국가정보자료규정」제2조제1호에 따른 국가정보자료로서 취급・관리하여야 한다.<개정 2022.1.27>

③ 탐지규칙정보를 배포받은 기관의 장은 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

④ 탐지규칙정보를 배포받은 기관의 장은 탐지규칙정보가 유출된 경우 즉시 그 사실을 국가정보원장에게 통보하여야 한다.

제112조(공격정보 탐지・수집) ① 보안담당관은 보안관제센터 운영시 보안관제 대상기관에 대한 사이버공격에 관한 정보를 탐지・수집하여야 한다.<개정 2022.1.27>

② 보안담당관은 보안관제센터 운영시 제1항의 업무를 수행하기 위하여 보안관제 대상기관의 장과 협의하여 사이버공격에 관한 정보를 실시간 수집하는 장비를 보안관제 대상기관의 정보통신망

에 설치·운용하거나 탐지규칙정보를 제공하여 관련 정보를 실시간 수집할 수 있다.<개정 2022.1.27>

③ 제109조제1항에 따라 보안담당관은 보안관제센터 운영시 탐지·수집한 사이버공격에 관한 정보 중 안보위해(危害) 공격에 관한 정보는 보안관제 대상기관의 장과 국가정보원장에게 실시간 제공하여야 하고 기타 사이버공격에 관한 정보는 보안관제 대상기관의 장에게 실시간 제공하여야 한다.<개정 2022.1.27>

④ 제109조제3항에 따라 보안담당관은 보안관제센터 운영시 「전자정부법 시행령」제69조에 따른 보안조치에 필요하다고 판단하는 경우 안보위해(危害) 공격에 관한 정보를 국가정보원장에게 실시간 제공할 수 있다.<개정 2022.1.27>

⑤ 보안담당관과 국가정보원장은 사이버공격에 관한 정보를 탐지·수집하기 위하여 불가피한 경우 다음 각 호에 해당하는 정보를 처리할 수 있다.<개정 2022.1.27>

1. 공격 주체 및 피해자를 식별하기 위한 IP주소 및 MAC주소, 전자우편 주소, 정보통신서비스 이용자 계정 정보, 피해자의 성명 및 연락처
2. 그 밖에 사이버공격의 방법 및 피해 확인에 필요한 정보<개정 2022.1.27>
3. 사이버공격으로 인하여 발생한 패킷<신설 2022.1.27>

제113조(초동 조치) ① 보안담당관은 사이버공격으로 인한 피해 최소화 및 확산 방지를 위하여 다음 각 호의 사항을 포함한 조치를 취하여야 한다.<개정 2022.1.27>

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 보전

② 보안담당관과 국가정보원장은 사이버공격으로 인한 피해를 최소화 하기 위하여 필요한 경우 보안관제 대상기관의 장에게 피해 시스템과 사용자에 관한 정보 제공을 요청할 수 있다.<개정 2022.1.27>

제114조(조치결과 통보) ① 제112조제3항에 따라 사이버공격에 관한 정보를 제공받은 보안관제 대상기관의 장은 제공받은 날로부터 5일 이내에 대응조치 결과를 원장에게 통보하여야 한다.<개정 2022.1.27>

② 보안담당관은 보안관제센터 운영시 국가정보원장이 별도로 요청한 안보위해(危害) 공격을 초동 조치한 경우 관련내용을 즉시 국가정보원장과 장관에게 통보하여야 한다. 또한 단위 보안관제센터를 운영하는 기관의 장은 관계 부문 보안관제센터를 운영하는 기관의 장에게도 통보하여야 한다. <개정 2022.1.27>

제115조(운영현황 통보) ① 제109조제1항에 따라 보안담당관은 보안관제센터 운영시 [별지 제12호 서식]에 따른 보안관제센터 운영현황을 작성하여 매년 1.25까지 국가정보원장에게 통보하여야 한다.<개정 2022.1.27>

② 국가정보원장은 국가보안관제체계의 운영을 위하여 필요하다고 판단하는 경우 제1항의 따른 운영현황과 관련된 추가 자료를 요청할 수 있다.

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

제116조(직원 교육) ① 보안담당관은 보안관제센터 운영시 보안관제업무 담당직원에 대한 교육 계획을 수립·시행하여야 한다. <개정 2022.1.27>

② 보안담당관은 보안관제센터 운영시 보안관제업무 담당직원이 매년 20시간 이상 보안관제 관련 교육을 이수하도록 하여야 한다.<개정 2022.1.27>

제2절 사고 대응

제117조(사이버공격으로 인한 사고) ①「사이버안보 업무규정」제16조 제1항에 따라 사고조사를 실시할 경우 국가정보원장은 안보위해(危害) 공격으로 인한 사고에 대하여 조사를 실시하며, 보안담당관은 안보위해(危害) 공격을 제외한 사이버공격으로 인한 사고에 대하여 조사를 실시한다. <개정 2022.1.27>

② 제1항에 따른 보안담당관은 사이버공격으로 인한 사고의 원인 분석 및 재발 방지를 위하여 피해 부서의 장에게 다음 각 호에 해당하는 자료 제출을 요청할 수 있다. 사이버공격으로 인하여「보안업무규정」제38조 및 제45조,「보안업무규정 시행규칙」제65조의2, 진흥원「보안업무규칙」에 따른 보안사고가 발생한 경우에도 같다.<개정 2022.1.27>

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 하며 보안담당관은 제출받은 자료를 사고원인 분석, 공격자 의도 파악, 피해영향 평가 등 사이버공격에 대한 예방 및 대응과 관련한 목적으로만 사용하여야 한다.

④ 피해 부서의 장은 사고 원인을 규명할 때까지 피해 시스템에 대한 증거를 보전하고 임의로 관련 자료를 삭제하거나 포맷하여서는 아니 된다.<개정 2022.1.27>

⑤ 공공 전용(專用) 민간클라우드에서 사고가 발생한 경우 보안담당관은 조사반을 구성하여 클라우드컴퓨팅서비스 제공자에 대하여 계약의 범위 내에서 자료의 보전 및 제출 요구, 현장 조사 등 필요한 조치를 취하여야 한다.<개정 2022.1.27>

제118조(정보통신보안 규정 위반 및 자료유출 사고) ① 보안담당관은 국가정보원장으로부터「보안업무규정 시행규칙」[별표 2]에 따른 정보통신보안 규정 위반사항에 대한 사실을 통보받은 경우 동(同)규정 시행규칙 제66조제3항에 따라 즉시 필요한 조치를 취하고 위규자, 위규 내용 및 조치 결과를 과학기술정보통신부장관 및 국가정보원장에게 통보하여야 한다.

② 보안담당관은 비밀·대외비 등 국가 기밀에 속하는 업무자료가 유출되거나 비공개 업무자료가 유출된 사고 중「국가정보원법」제4조 제1항 제1호 나목부터 마목까지와 관련된 사안일 경우 즉시 과학기술정보통신부장관과 국가정보원장에게 통보하여 합동 조사를 실시하여야 한다. <개정 2022.1.27>

③ 소속직원의 과실로 인하여 개인 소유의 정보통신기기 및 이동통신단말기, 상용 정보통신서비스에서

제2항에 따른 유출사고가 발생한 경우 조사 기관의 장은 보안담당관을 통해 해당 직원에게 저장자료・이용내역 등의 자료 제출을 요청할 수 있다.
④ 소속직원은 제3항에 따른 요청이 위법하다고 판단하는 경우 그 사유를 소명하고 자료 제출을 거부할 수 있다.
⑤ 보안담당관은 제1항 및 제2항에 따른 조사를 통해 유출이 확인된 자료에 대하여 관계부서의 장과 합동으로 국가안보 및 국익, 정부정책에 미치는 영향을 평가하여 필요한 조치를 취하여야 한다. <개정 2022.1.27>

제119조(재발방지 조치) ① 보안담당관은 제117조 및 제118조에 따른 조사 결과 및 재발방지를 위한 보안조치 사항을 해당 부서의 장에게 통보하여야 한다.<개정 2022.1.27>
② 제1항에 따라 조사 결과를 통보받은 해당 부서의 장은 관계 법규에 따른 관련자 징계, 개선대책 수립・시행 등 필요한 조치를 취하여야 한다.<개정 2022.1.27>

제120조(정보보안 사고조사) ① 보안담당관은 [별표 2]의 정보보안 사고가 발생한 때에는 즉시 피해 확산 방지를 위해 다음 각 호의 사항을 조치하여야 한다. 이 경우, 사고원인 규명시까지 피해 시스템에 대한 증거를 보전하고 임의로 관련 자료를 삭제하거나 포맷하여서는 아니 된다.

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

② 보안담당관은 사고조사 결과 피해가 심각하다고 판단되는 경우 과학기술정보통신부장관과 협의하여 합동조사 및 복구지원팀을 구성·운영할 수 있다.<개정 2022.1.27>
③ 보안담당관은 규정에 의한 관련자 징계, 재발방지를 위한 보안대책의 수립·시행 등 사고조사 결과에 따라 필요한 조치를 하여야 한다.<개정 2022.1.27>

제121조(징계조치) 원장은 다음 각 호의 정보보안 사항을 위반한 소속직원에 대해 진흥원 자체 인사 및 복무규정에 따라 처분을 요구할 수 있다.

1. 제9조에 따른 정보보안 감사 등 결과 정보보안업무 규정을 위반한 자
2. 제120조에 따른 사고조사 결과 [별표 2]의 보안사고 유형에 해당한 자

제8장 정보 협력

제122조(정보협조 요청) 보안담당관은 국가정보원장이 국제 및 국가배후 해킹조직 등 사이버안보 정보의 수집・작성 및「국가정보원법」제5조제2항에 따른 조사를 위하여 보안담당관에게 제117조 제1항 각 호의 자료 제출 및 관련 지원을 요청 할 경우 해당 자료를 제출하거나 필요한 지원을 할 수 있다. 다만,「형사소송법」,「군사법원법」또는「통신비밀보호법」에 따른 절차는 해당 법률이 정하는 바에 따른다.<개정 2022.1.27>

제123조(기관간 정보공유 협력) 보안담당관은 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

제124조(정보공유시스템의 정보 관리) 정보공유시스템을 이용하는 경우 보안담당관은 정보공유시스템에 등록된 정보를「공공기관의 정보공개에 관한 법률」제9조제1항에 따른 비공개 대상 정보 및「국가정보자료규정」제2조제1호에 따른 국가정보자료로서 취급・관리하여야 한다.

제9장 보 칙

제125조(다른 법령과의 관계) 이 지침에 명시되지 않은 사항은 다음 각 호의 관련규정 및 지침에 따른다.

1.「국가정보원법」
2.「정보 및 보안업무 기획・조정규정」
3.「보안업무규정」 및 시행규칙
4.「전자정부법」과 동법 시행령
5.「정보통신기반보호법」과 동법 시행령
6.「공공기록물 관리에 관한 법률 시행령」
7.「국가 사이버안전 관리규정」
8.「국가위기관리 기본지침」
9.「국가 정보보안 기본지침」
10. 그 밖의 관계 법규

부 칙<2014. 1. 24.>

이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

부 칙<2015. 5. 13.>

이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

부 칙<2015. 7. 14.>

이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

부 칙<2017. 4. 13.>

이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

부 칙<2018. 12. 28.>

이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

부 칙<2020. 1. 31.>

이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

부 칙<2021. 2. 25.>

이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

부 칙<2022. 1. 27.>

이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

부 칙<2022. 12. 23.>

이 지침은 경영기획본부장의 승인을 받은 날부터 시행한다.

별 표

【별표 1】 <개정 2021.2.25>

정보보안 규정의 위반사항

내 용	세 부 내 용
1. 정보통신망 및 정보시스템(연구용 시스템 포함) 운영	가. 정보시스템 외부 원격 접속 허용 나. 정보시스템 내 저장장치 임의 분해 또는 유출 다. 정보시스템 접근기록 및 작업기록 임의 삭제 또는 유출 라. 정보시스템 관리대장, 관리자 계정 등 중요정보 유출 마. 정보시스템 관리자 접속용 단말 인터넷 접속 등 보안관리 미흡 바. 정보시스템 취약포트 및 불필요 포트 미차단 사. 승인 없이 업무망, 인터넷망 간 혼용 접속 허용 아. 고유식별번호, 비밀번호 등 중요정보 암호화 미적용 자. 정보시스템 관리자 접근제어 미설정 차. 보안지원이 중단된 운영체제 사용 카. 시스템 취약점 점검 및 웹 취약점 점검 결과에 따른 취약점 미조치
2. 용역사업 관리	가. 용역직원 대상 보안교육 미실시(사업 착수 후 1개월 이내) 나. 승인 없이 용역직원에게 대외비 등 비공개 정보 누설 또는 유출 다. 용역직원에게 제공한 자료에 대한 인수인계대장 미작성 라. 전산장비 반출입 내역 미작성 및 장비 무단 반출·입 마. 산출물 회수, 자료삭제 확인, 확약서 징구 등 산출물 회수관리 미흡 바. 용역직원의 비인가 휴대용 저장매체 사용 허용 사. 용역직원의 인터넷 허용 및 우회 정보통신망 사용관련 미차단 아. 용역직원 사용 전산망과 기관 전산망 혼용 사용 자. 비인가 PC·노트북 등 정보통신망에 연결 차. 정보시스템 취급 용역직원에게 관리자 권한의 계정 부여
3. PC 등 단말기 보안관리	가. 매월 사이버보안진단의 날 기준 내PC지키미 미수행 나. 업무PC에 개인정보가 포함된 민감 자료 저장 및 유출 다. 인터넷망 PC에서 업무자료 작성 및 저장 라. 인터넷PC에 비인가 프로그램 설치 및 사용 마. 인터넷망PC에 VPN SW, 테더링, 블루투스 등 정보통신망 우회 사용 바. 비인가 휴대용 저장매체(USB, CD, 기타 휴대용 저장매체 등) 사용 사. 등록된 휴대용 저장매체(보안USB, 보안SSD 등) 분실·대여·미소지 아. 매체제어, 망간자료전송, DLP 등 정보보호 솔루션 고의적 우회 시도 및 사용
4. 기타 훈련 및 보안점검	가. 해킹메일 대응 훈련시 메일 열람 후 미신고 나. 해킹메일 대응 훈련시 메일 전달 및 수신자 조작 등 고의적 방해 행위

【별표 2】

정보보안 사고 유형

조	내 용	항	세 부 내 용
1	전자정보 (전자문서 및 전자기록물)	(1) (2) (3) (4)	비밀의 유출 주전산기.대용량 전자기록(DB) 손괴 전자정보의 위조.변조.훼손 및 유출 PC 등 단말기內 비밀의 평문 보관 및 유통
2	정보통신시스템 및 정보통신실	(1) (2) (3) (4) (5) (6) (7)	정보통신망에 대한 해킹.악성코드의 유포 비밀이 저장된 PC, 휴대용 저장매체 등 분실 중요 정보통신시스템 및 정보통신실 파괴 고의적인 중요 정보시스템 기능 장애 및 정지 상용메일, PC·스마트폰 메신저 등을 통한 비밀 등 중요자료 무단 소통 비밀 등 중요자료의 무단 반출 정보통신기기를 통한 비밀 등 중요자료 무단 소통
3	암호장비	(1) (2) (3) (4) (5) (6)	암호장비 분실 및 피탈 암호장비 파손 및 임의파기 암호장비 복제.복사 비인가 암호장비 사용 암호장비 비닉체계 특성 및 제원 노출 암호장비 키 운용체계 노출
4	보안자재	(1) (2) (3) (4)	암호자재의 분실 및 누설 암호자재의 파손 및 임의 파기 암호자재의 임의제작 사용 세부 암호체계 노출

[별표 3] <개정 2022.1.27., 2022.12.23.>

IT보안제품(정보보호시스템, 네트워크 장비 등)의 도입 요건

제품군	제품유형	사전인증 요건
침입차단 제품군	침입차단시스템(FW)	CC인증 또는 보안기능 확인서
	침입차단시스템(FW+VPN)	CC인증 또는 보안기능 확인서, +암호모듈검증제도
	웹 방화벽(WAF)	CC인증 또는 보안기능 확인서
	DDOS 대응장비	CC인증·성능평가·보안기능 확인서 중 어느 하나
	인터넷전화 보안제품	CC인증 또는 보안기능 확인서
	침입차단제품군 기타 (신기술·신종제품)	CC인증·보안기능 확인서 중 어느 하나 (未발급 제품은 도입 후, 검증신청)
침입방지 제품군	침입방지 시스템(IPS, IDS)	CC인증 또는 보안기능 확인서
	침입방지시스템(IPS+VPN)	CC인증 또는 보안기능 확인서, + 암호모듈검증제도
	무선침입방지제품(WIPS)	CC인증 또는 보안기능 확인서
	침입방지제품군 기타 (신기술·신종제품)	CC인증·보안기능 확인서 중 어느 하나 (未발급 제품은 도입 후, 검증신청)
구간보안 제품군	가상사설망(VPN)	CC인증 또는 보안기능 확인서 +검증필 암호모듈
	네트워크 접근통제제품(NAC)	CC인증 또는 보안기능 확인서
	망간 자료전송제품	보안기능 확인서
	무선랜 인증제품	CC인증 또는 보안기능 확인서
	구간암호화제품	검증필 암호모듈
	구간보안제품군 기타 (신기술·신종제품)	CC인증·보안기능 확인서 중 어느 하나 (未발급 제품은 도입 후, 검증신청)
전송자료 보안 제품군	스팸메일 차단시스템	CC인증 또는 보안기능 확인서
	네트워크 자료유출방지제품(NDLP)	보안기능 확인서
	소프트웨어 기반 보안USB제품	보안기능 확인서+검증필 암호모듈탑재
	호스트 자료유출방지제품(HDLP)	보안기능 확인서+검증필 암호모듈탑재
	메일암호화제품	검증필 암호모듈 (보안기능 확인서+검증필 암호모듈 탑재 권고)

	전송자료보안제품군기타 (신기술·신종제품)	CC인증·보안기능 확인서 중 어느 하나 (未발급 제품은 도입 후, 검증신청)
보안관리 제품군	스마트카드(COS 포함)	CC인증 또는 보안기능 확인서
	통합보안 관리제품 (ESM, 통합로그관리 등)	CC인증 또는 보안기능 확인서
	소스코드 보안약점 분석도구	CC인증·성능평가·보안기능 확인서 중 어느 하나
	패치관리시스템	CC인증 또는 보안기능 확인서
	DB 접근통제 제품	CC인증 또는 보안기능 확인서
	통합인증제품(SSO)	CC인증 또는 보안기능 확인서+검증필 암호모듈
	보안관리제품군 기타 (신기술·신종제품)	CC인증·보안기능 확인서 중 어느 하나 (未발급 제품은 도입 후, 검증신청)
가상화 제품군	가상화 관리제품	보안기능 확인서
	가상화제품군 기타 (신기술·신종제품)	CC인증·보안기능 확인서 중 어느 하나 (未발급 제품은 도입 후, 검증신청)
엔드포인트 보안제품군	디지털 복합기	CC인증(별도 검증신청 불요)
	안티바이러스 제품 (WINDOWS)	CC인증·성능평가·보안기능 확인서 중 어느 하나
	안티바이러스 제품 (LINUX, 모바일)	성능평가
	스마트폰 보안관리제품 (MDM,EMM 등)	CC인증 또는 보안기능 확인서
	운영체제(서버) 접근통제 제품	CC인증 또는 보안기능 확인서
	문서암호화제품(DRM)	CC인증 또는 보안기능 확인서+검증필 암호모듈
	DB 암호화제품	CC인증 또는 보안기능 확인서+검증필 암호모듈
	엔드포인트 보안제품군기타 (신기술·신종제품)	CC인증·보안기능 확인서 중 어느 하나 (未발급 제품은 도입 후, 검증신청)
네트워크 장비	스위치(L3,L4, L7 등)	보안기능 확인서
	SDN컨트롤러	보안기능 확인서
	SDN스위치	보안기능 확인서
	L2 보안시스템	보안기능 확인서
	네트워크 장비 기타 (신기술·신종제품)	보안기능 확인서

[별표 4] <개정 2022.12.23.>

검증필 암호모듈 도입기준

제품 유형	도입 요건	비 고
메일 암호화제품	검증필 암호모듈 탑재	
구간 암호화제품		
하드웨어 보안토큰		
디스크·파일 암호화제품		
기타 암호화제품		
DB암호화	검증필 암호모듈 탑재 및 보안적합성 검증제도 참고	상세 도입기준은 [별표3] IT보안제품 도입요건 참고
통합인증(SSO)		
문서 암호화제품(DRM 등)		
가상사설망(VPN)		
소프트웨어기반 보안USB		
호스트자료 유출방지		

* 최신 도입요건은 국가정보원 홈페이지(암호모듈 검증)를 참조

[별표 5] <개정 2022.12.23.>

보안적합성 검증 신청 시 제출물

1. 최초검증 신청 시 제출물

제출물	정보보호시스템		작성 주체
	상용 제품	자체(용역) 개발	
[별지 제11호 서식]에 따른 보안적합성 검증 신청서	○	○	신청기관
[별지 제10호 서식]에 따른 IT보안제품 도입확인서(현황)	○	○	
기술제안요청서 사본	○	○	
보안기능 점검표	○	○	
운용점검사항	○	○	
CC인증서 사본	○ (인증서 보유시)		업체
보안기능 운용 설명서	○	○	
기본 및 상세 설계서		○	
개발완료 보고서		○	

2. 재검증 신청시 제출물

제출물	정보보호시스템		작성 주체
	상용 제품	자체(용역) 개발	
[별지 제11호 서식]에 따른 보안적합성 검증 신청서	○	○	신청기관
[별지 제10호 서식]에 따른 IT보안제품 도입확인서(현황)	○	○	
보안기능 점검표	○	○	
운용점검사항	○	○	
변경내용 분석서	○	○	업체

별 지 서 식

【 별지 제1호 서식 】

정보보안업무 세부 추진계획

< 작성 요령 >

1. 활동목표

2. 기본방침

3. 세부 추진계획

분야별	사 업 명	세 부 추 진 계 획	주관.관련부서	비 고

* 국가정보원 보안성 검토 대상여부 표기

4. 전년도 보안감사·지도방문시 도출내용과 조치내역

도출내용	조 치 내 역	담당부서

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

【별지 제2호 서식】

정보보안업무 심사분석

1. 총 평

2. 주요성과 및 추진사항

3. 세부 사업별 실적분석

추 진 계 획	추 진 실 적	문 제 점	개 선 대 책

* 추진실적은 목표량과 대비하여 성과 달성도를 계량화

4. 부진(미진)사업

부진사업	원인 및 이유	익년도 추진계획

5. 애로 및 건의사항

6. 첨부(정보통신망 및 정보보호시스템 운용현황 등)

【 별지 제3호 서식 】<개정2022.12.23>

정보시스템 관리대장

연번	소속	관리자	관리 책임자	종류 (서버·PC 등)	제조사	모델명	관리번호	도입일자	비고

【 별지 제4호 서식 】

암호실 및 암호취급자 현황

구분	암 호 실				암 호 취 급 자				비고
부서	인가	운용	과부족	변동 내용	인가	운용	과부족	변동 내용	
총계									

【 별지 제5호 서식 】

암호실 출입자 기록부

출입일시	소속	직책	직급/ 성명	용무	서명	인가자인	비고

【 별지 제6호 서식 】

서 약 서

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

1. 본인은 암호자재와 관련된 소관업무가 국가기밀 사항임을 인정하고 제반 보안 관계규정 및 지침을 성실히 준수한다.
2. 나는 이 기밀을 누설함이 이적행위가 됨을 명심하고 재직 중은 물론 퇴직 후에도 알게 된 모든 기밀사항을 일절 타인에게 누설하지 아니한다.
3. 나는 기밀을 누설한 때에는 아래의 관계법규에 따라 엄중한 처벌을 받을 것을 서약한다.

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)

년 월 일

서약자	소속	직급 직위	주민등록번호(앞자리) 성 명	인
서 약 집행자	소속	직급 직위	성 명	인

【 별지 제7호 서식 】

암호자재 운용관리 현황

기관명 :　　년　　월　　일 현재

자재명	기관번호	일련번호	제작년월	설치장소	상대국소	설치일자	비고

【 별지 제8호 서식 】

암호자재 신청서

자재명	수령 지역	실수령 기관	부수	산출내역	보유	과부족	비고

※ 작성 요령

- 수령지역 : 서울청사, 과천청사, 세종청사, 대전청사, 지자체별
- 산출내역 : 세부 운용부서 및 부수
- 보유 : 현용 자재기준 산출
- 과부족 : 소요자재 부수-현재 보유자재 부수
- 비고 : 조직 신편·증편·통합 등 참고사항 기재

【 별지 제9호 서식 】

지편자재 사용기록부

자재번호	관리번호	년월일	전문 액표			난수 사용				소자 년월일	소자자	비고
			암호전문 일련번호	수·발신 구분	암호전문 조수	부터		까지				
						쪽	행	쪽	행			

【 별지 제10호 서식 】<개정 2022.12.23.>

IT보안제품 도입확인서·보안적합성 검증 신청서

사업 추진기관		설치기관 편성그룹	
제품 설치기관		담당관	
담당관 이메일		담당관 전화번호	
사업명		계약일	
		도입일	
보안성 검토		적용 도입기준	

연번	개발업체				도입제품			사전인증					도입수량	적합성 검증 신청
	업체명	소재지 (국적)	담당자	담당자 휴대폰	제품유형	제품명	해시값	사전인증 유형	인증완료 여부	발급 (인증) 번호	발급 (인증)일	암호검증 번호		
						L3 스위치		국내CC 인증				CM-00-000.0		

【 별지 제11호 서식 】 <개정 2022.1.27>

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 (□ 반영·개선 □ 반영불가)		
신청 제품	제품명	※ 신청 제품이 2種 이상인 경우, 별도 신청	S/W(펌웨어) 버전	
	제품 유형		도입 수량	대
	사전 인증 대상 여부	□ CC인증 대상 □ 검증필 암호모듈 탑재 □ 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	

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

【 별지 제12호 서식 】

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	

<table>
<tr><th colspan="6">보안장비 현황</th></tr>
<tr><td>F/W</td><td colspan="2">* 제품명 및 사용대수</td><td>IDS/IPS</td><td colspan="2"></td></tr>
<tr><td>ESM</td><td colspan="2"></td><td>WEB F/W</td><td colspan="2"></td></tr>
<tr><td>라우터</td><td colspan="2"></td><td>그 밖의 장비</td><td colspan="2">예) NMS 1대
* 네트워크 구성도 사본 제출</td></tr>
<tr><th colspan="6">보안관제 연동기관 현황</th></tr>
<tr><td colspan="6">* 대상기관 수, 기관명, 대상목표(인터넷 또는 내부망, 홈페이지 등)</td></tr>
<tr><th colspan="6">연동기관 IP할당 현황</th></tr>
<tr><td rowspan="3">1</td><td>연동기관</td><td></td><td rowspan="3">IP
관리자</td><td>성 명</td><td></td></tr>
<tr><td>공인IP</td><td></td><td>연락처</td><td>전화: HP:</td></tr>
<tr><td>사설IP</td><td></td><td>이메일</td><td></td></tr>
<tr><td>2</td><td></td><td colspan="4"></td></tr>
<tr><td>3</td><td></td><td colspan="4"></td></tr>
<tr><td>4</td><td></td><td colspan="4"></td></tr>
<tr><td>5</td><td></td><td colspan="4"></td></tr>
<tr><td>6</td><td></td><td colspan="4"></td></tr>
<tr><th colspan="6">국가사이버안전센터 탐지규칙 재배포 현황</th></tr>
<tr><th colspan="2">기관명</th><th>배포방법</th><th>기관명</th><th colspan="2">배포방법</th></tr>
<tr><td colspan="2"></td><td></td><td></td><td colspan="2"></td></tr>
</table>

【별지 제13호 서식】 <삭제 2022.12.23.>

【 별지 제14호 서식 】

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 비밀통신을 수행하도록 제품 변경 *** 필요시 화면 캡쳐**

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: test1.1.img — 97BA3B7A1B325E4E8A517CDDB01AFFD3 변경후: test1.2.img — DCE24E537D2EB6E28E5BADBD1CEC0898 *** 필요시 화면 캡쳐**
사용자 인터페이스(UI) 변경 유무	로그인 기능 변경을 위해 내부 코드가 변경되었으며 제품의 사용자 인터페이스(UI) 변경은 없음 *** 필요시 화면 캡쳐**

라. 변경부분에 대한 자체 시험결과

변경된 기능	시험 내용	시험 결과
로그인	관리자 로그인시 비밀통신 수행여부 확인	정상동작 확인 *** 필요시 화면 캡쳐**

【별지 제15호 서식】

보안정책 예외처리 신청서

담당자	팀장

신 청 일		**부서**	
신 청 자		**연락처(내선)**	
사용기간	기간 : 년 월 일 ~ 월 일(최대 당해연도 12월 31일까지)		
적용희망일시			
신청구분	망분리 관련 예외처리	☑ 인터넷망 문서편집 이용 ☐ 인터넷망 차단 웹사이트 접근허용 ☐ 인터넷망 보안USB 매체 읽기허용 ☐ 인터넷망 보안USB 매체 쓰기허용 ☐ 인터넷망 파일 자동 삭제 확장자 예외 ☐ 망간자료전송 파일 확장자 허용 (☐ 업무망→인터넷망 ☐ 인터넷망→업무망)	
	기타 예외처리	☐ CD/DVD 매체 읽기허용(☐ 업무망 ☐ 인터넷망) ☐ CD/DVD 매체 쓰기허용(☐ 업무망 ☐ 인터넷망)	
PC IP주소	. . . (예, 10 . 34 . xxx. xxx)		
소프트웨어명			
확장자명	☐ 망간자료전송 파일 확장자명 ( )		
	☐ 인터넷망 파일 자동삭제 예외 확장자명 ( )		
웹사이트 주소			
신청사유			

상기 사유와 같이 정보보안 정책적용의 예외처리를 신청합니다. 신청자 본인은 상기 보안 정책 예외처리 신청에 대해 내부자료 유출 및 악성코드 감염 등 보안 위규사항이 발생되지 않도록 철저히 관리하겠으며, 내부 자료의 유출 및 악성코드 감염 등 중대한 보안 위규 사항 발생 시 보안상의 책임과 관계법규(지침)에 의한 조치에 따를 것을 서약합니다.

20 년 월 일

【 별지 제16호 서식 】

팀 노트북 보안점검 현황

o 점검 대수(　　대), 점검 일자(　~　)

연번	관리담당		사용 목적	자산 출처	보안 설정				
	부서	성명			주요자료 삭제	CMOS PW	로그인 PW	화면보호 기설정	최신백신 설치

【별지 제17호 서식】

계정발급(삭제) 신청서

담당자	팀장

o 계정 신청자

일 자	
구 분	신규 ( ), 추가 ( ), 삭제 ( ), 기타 ( )
	서버( ), 네트워크( ), 보안장비( ), 데이터베이스( ), 응용프로그램( )
사 유	
팀 명	
사용자 ID	
사용자 이름	
사용자 그룹	

o 접근 권한

지정 그룹	
접근 가능 권한	
비 고	

【별지 제18호 서식】

관리자계정(비밀번호) 관리대장

담당자	팀장

No.	시스템명	분류	위치	ID	Password	관리자(성명)

【별지 제19호 서식】

웹방화벽 정책등록 신청서

담당자	팀장

신 청 일			연락처(내선번호)		
부 서			적용희망일시		
신청자(보안담당자)			등록 사유		
출발지	목적지		정책등록 요청내용	적용일	종료일
IP	IP/URI	Port			

【별지 제20호 서식】

네임서버 도메인 등록(변경) 신청서

담당자	팀장

신청부서			
신 청 일			
신 청 자			
연락처(내선번호)			
적용희망일시			
요 청 내 용 **(정책변경 사유)**			
네임서버	**등록대상 도메인명**	**등록대상 서버 IP**	**비고**

【별지 제21호 서식】

망연계 및 방화벽 정책등록 신청서

담당자	팀장

신 청 일	
부 서	
신 청 자	
연락처(내선번호)	
적용희망일시	
등록 사유	

출발지		**목적지**		**서비스명**	**적용일**	**종료일**
IP	**Port**	**IP**	**Port**			

【별지 제22호 서식】

VPN OTP 발송방법 변경신청서

신청자

신청 개요	
신청일	OOOO년 OO월 OO일
부서명	OOOO 팀
성명	O O O
연락처(내선번호)	5571
신청자 ID	
신청사유	국외 출장으로 휴대폰 메시지 수신 불가, 출장지 해당기관의 보안정책상 휴대폰 사용 불가 등

변경 신청사항				
선택	**변경 전(前)**	**변경 후(後)**	**적용 기간**	**OTP 전송 연락처**
■	휴대폰	이메일	2013.07.27 ~ 2013.08.30	abc@kisa.or.kr
□	이메일	휴대폰	2013.08.01 ~ 계속	010-****-****

【별지 제23호 서식】

신규 IP주소 할당 신청서(용역업체용)

담당자	팀장

신 청 일	
부 서	
신 청 자	
연락처(내선번호)	
용역사업 명	

사용자 명	MAC 주소	PC명	소속사명	시작일	종료일
홍길동	00-E0-91-20-D7-73	KISA01	SPlus	2013.06.03	2013.12.27

【별지 제24호 서식】

사용자계정 관리대장

No.	소속	성명	시스템명	계 정	접근권한	처리내용 (등록, 수정, 삭제)	처리일자	확인

【별지 제25호 서식】

인수자료 관리대장

No.	인수자료 목록	인수일자	구분	담당자	용역업체 담당자
		. . .	문서		
			파일		

【별지 제26호 서식】

보안USB관리시스템 Agent 삭제요청서

사용자	팀장

사용자					
사용자	**사번**	**IP주소**	**내선번호**	**기간**	**요청사유**
홍길동	K00000	172.16.00.000	5118	2013. 00. 00 ~ 2013. 00. 00	ex) 용역업무 종료에 따른 장비 반출, 국외출장, 퇴사 등

※ 보안USB관리시스템 Agent 삭제는 국외출장 및 사업종료에 따른 장비반출, 퇴사 등 특수한 경우에 한함

【별지 제27호 서식】

휴대용 저장매체 승인 요청서(일반용)

보안담당자	팀장

신청자(보안담당자)	
신청일	OOOO년 OO월 OO일
부서명	OOOO 팀
성명	O O O
연락처(내선번호)	5571

사용자						
사용자	**내선번호**	**제품명**	**종류**	**용량**	**사용기간**	**용도**
홍길동	5555	LGK-16G	USB	16G	13.7월 ~ 13.12월	외부 출장
박부장	6654	갤럭시2	휴대폰	8G	영구	개인 업무용

【별지 제28호 서식】

보안USB (재)발급 신청서

담당자	팀장

접수	보안담당

신청자(보안담당자)	
신청일	년 월 일
사용기간	년 월 일 ~ 월 일(최대 당해연도 12월 31일까지)
부서명	
성명	
연락처(내선번호)	

사용자					
사용자	**직급**	**사번**	**내선번호**	**보조기억매체**	**신청사유**

【 별지 제29호 서식 】

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 제30호 서식 】 <개정 2021.2.25>

정보시스템 반출·입 대장

<관리책임자 : ＯＯＯ *서명* >

※ 보안조치 : ①CMOS PW설정, ②윈도 PW설정, ③화면보호기 설정, ④최신백신, ⑤자료완전삭제

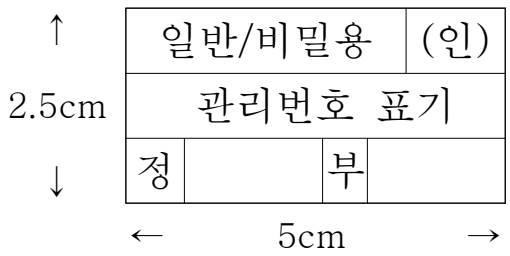
장비명	관리번호 (시리얼번호)	사용자	반출입 사유	반출입 일시 (입·출 구분)	보안조치	확인
디지털 복합기	OO-OO-OO	공용	고장	'19.00.00 00:00(출)	⑤	*OOO* *서명*
PC	OO-OO-OO	OOO	인터넷자료열람	'19.00.00 00:00(입)	①,②, ③,④	OOO 서명
모뎀	OO-OO-OO	OOO	상용인터넷 연결용	'19.00.00 00:00(입)	-	OOO 서명
프린터	OO-OO-OO	공용	고장	'19.00.00 00:00(출)	-	OOO 서명
노트북	s111-001-113 (5004829800055)	5급 홍길○	세미나 발표	2011.12.3 13:00 (출)	⑤	OOO 서명
USB	총무-일반-01 (610-RUCW-61659)	5급 홍길○	국회 제출	2011.10.1 11:00(출)	⑤	OOO 서명
CD	총무-일반-03 (4589-KK-4585)	5급 유관○	법무부 회의참석	2011.10.7 09:40 (출)	⑤	OOO 서명

* 정보시스템이란?

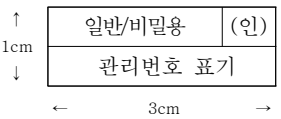
운용을 위해 도입한 PC, 노트북, 프린터, 디지털복합기, 통신기기, 휴대용저장매체 등을 말함

【 별지 제31호 서식 】

휴대용 저장매체 라벨



< 디스켓, 이동형 HDD 서식 >



< USB·CD 등 서식 >

가. 同서식을 만들어 휴대용 저장매체 중앙의 적절한 위치에 부착

나. 첫 번째 줄에는 일반/비밀용은 보안담당관의 직인을 날인하고 공인인증서용은 매체관리책임자의 직인을 날인

다. 두번째 줄에는 휴대용 저장매체 관리번호 표기

라. 세 번째 줄의 '정'란에 매체관리책임자·'부'란에 취급자 표기
(USB메모리 및 CD의 경우 생략 가능)

마. 휴대용 저장매체의 크기를 고려하여 서식·글자 크기 조정 가능

<별지 제31호 서식 예시>

일반용	(인)		
총무과-일반-01			
정	이순○	부	홍길○

대외비용	(인)		
총무과-대외비-01			
정	이순○	부	홍길○

일반용	(인)
총무과-일반-01	

Ⅱ급비밀용	(인)
총무과-Ⅱ급-01	

【 별지 제32호 서식 】

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					
2					
3					
4					
5					
6					
7					
8					
9					
10					

확인일자 : 년 월 일

요 청 자 : 소속・직책 성명 : (인)

확 인 자 : 정보보안안담당관 성명 : (인)

【 별지 제33호 서식 】

휴대용 저장매체 등록 신청서

등록구분	☑ 신규	☐ 변경 (사유 :)	
매체구분	☑ 보안USB	☐ 외장형 하드디스크	
등록요청 부서	**소속**	**직위(직급)**	**관리담당자(정보보안실무자)**
신청매체 정보	*※ 일반용 USB에 대외비 문서 저장은 금하며, 자료전송 목적으로 사용 시에는 정보보안운영팀에서 대여용 USB를 대여하여 사용* *※ 비밀용 USB의 경우 **비밀관리기록부**에 매체정보를 등재하여 관리하여야 함* *※ **외장형 하드디스크에는 대외비 및 업무자료 저장 금지 (자료전송의 목적으로만 사용)***		
신청사유			

상기와 같이 보안USB의 시스템 등록을 신청합니다. 신청자 본인은 보안USB를 통한 내부 자료의 유출이 발생하지 않도록 **주기적인 매체현황 파악 및 월별 휴대용 저장매체 점검대장 작성** 등을 통해 철저히 관리하겠으며, 내부 자료의 외부 유출 시 보안책임서약내용에 따라 모든 책임을 지겠습니다.

20 년 월 일

부서 정보보안실무자 직위(직급)		**성명**	
정보보안담당관(직급)		**성명**	

※ 필수숙지사항

1. 신청자는 보안책임서약서 내용을 확인한 후 신청서를 작성
2. 매체는 **부서단위로 신청하여 관리**하여야 하며, 담당자 및 책임자(부서장)의 직위·성명을 입력하고 전자결재를 통해 정보보안운영팀에 공문 송부
3. 부서별로 사용매체를 최소화하여야 하며, 진흥원 정보보안 기본지침에 의거하여 매체등록을 허용하지 않을 수 있으므로 담당자에 사전협의 요망
4. 외장형 하드디스크는 **꼭 필요한 업무 이외의 등록신청을 자제하여야 하며, 락(Lock) 기능**이 있는 제품을 구매하여야 함
5. 등록 승인된 저장매체는 **휴대용 저장매체 점검대장**(매월 1회 점검)으로 관리하여 정보보안담당관에게 반기별로 자료제출 요청 시 제출하여야 하며, **미 제출 시 해당 매체 사용중지 조치**
6. **인사이동으로 인한 저장매체 관리담당자 변경 시, 반드시 매체 현황 및 휴대용 저장매체 점검대장을 인수인계 하여야 하며, 인수인계 미흡으로 인한 매체 분실 시 보안책임을 물을 수 있음**

【 별지 제34호 서식 】

보안 서약서(용역사업)

본인은 년 월 일부로 “ ”관련 용역사업(업무)을 수행함에 있어 다음사항을 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 일체 누설하거나 공개하지 아니한다.
3. 본인이 이 기밀을 누설하거나 관계규정을 위반한 때에는 관련법령 및 계약에 따라 어떠한 처벌 및 불이익도 감수한다.
4. 본인은 하도급업체를 통한 사업수행 시 하도급업체로 인해 발생하는 위반사항에 대하여 모든 책임을 부담한다.

년 월 일

서 약 자 (업체 대표)	업 체 명 : 직 위 : 성 명 : 생년월일 :	(서명)
서약집행자 (용역사업 담당)	업 체 명 : 직 위 : 성 명 : 생년월일 :	(서명)

【 별지 제35호 서식 】

일일 용역사업 보안점검 리스트

순번	점검항목
1	용역업체 사용 전산망과 기관 전산망의 분리 여부(VLAN 분리 포함)
2	용역업체 직원 PC의 내부 정보시스템 접근 통제 여부
3	P2P, 웹하드, 메신저 등 불필요한 인터넷 접속 차단 여부
4	용역업체 직원에 주요 계정 비밀번호 제공 여부
5	용역업체 직원에 비밀번호 부여시 관련사항 별도 기록 여부
6	용역업체 직원에 시스템 관리자 계정 단독 접근 여부
7	노트북PC 등 휴대형 정보시스템을 시스템 관리용 PC로 활용 여부
8	용역업체 직원 등에 의한 기관 외부에서의 원격 접속·작업 여부
9	용역업체 정보시스템 접근시 작업이력 로깅 기능 사용 여부
10	용역업체 PC 및 휴대형 저장매체에 정보시스템 '계정명/비밀번호' 저장 여부
11	용역업체 PC에 설치된 운영체제 및 응용프로그램 최신상태 유지 여부
12	용역업체 PC 백신 프로그램 자동 업데이트 및 실시간 감시기능 사용 여부
13	용역업체 PC USB·CD-RW·무선랜 등 매체 통제 여부
14	용역업체 PC 비밀번호 및 화면보호기 설정 여부
15	용역업체 직원의 비인가 정보통신장비(노트북 등) 휴대·반입 여부

부 록

【부록 1】

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・조치절차가 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?	

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 확인하고 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】

정보시스템 저장매체·자료별 삭제방법

저장자료 / 저장매체	공개자료	민감자료 (개인정보 등)	비밀자료 (대외비 포함)
플로피디스크	㉮	㉮	㉮
광디스크 (CD.DVD 등)	㉮	㉮	㉮
자기 테이프	㉮.㉯중 택일	㉮.㉯중 택일	㉮
SSD·USB등 반도체메모리 (EEPROM 등)	㉮	㉮	㉮
하드디스크	㉱	㉮.㉯.㉰중 택일	㉮.㉯중 택일

㉮ **완전파괴(소각·파쇄·용해)** : 파쇄시에는 파쇄조각의 크기가 0.8mm 이하가 되도록 조치

㉯ **전용 소자장비 이용 저장자료 삭제** : 저장매체의 보자력보다 큰 자기력으로 삭제

㉰ **완전포맷 3회 수행** : 저장매체 전체를 '난수'·'0'·'1'로 각각 중복 저장하는 방식으로 삭제

㉱ **완전포맷 1회 수행** : 저장매체 전체를 '난수'로 중복 저장하는 방식으로 삭제

※ **(SSD의 경우)** 완전파괴가 원칙이나 디스크 암호화 기술을 적용하여 SSD를 암호화 할 경우 암호키를 폐기하고 소프트웨어 제품으로 완전포맷 후 활용가능. 다만, 비밀자료를 생산·저장·보관 등을 수행한 경우에는 완전파괴 함

【부록 3】

직원 PC 및 스마트폰 보안수칙

< 단말기 보안 규정 >

※ 단말기 사용자는 PC・노트북 등 단말기 사용과 관련한 일체의 보안관리 책임

1. **장비**(CMOS)·**자료**(문서자료 암호화)·**사용자**(로그온)별 비밀번호 주기적 변경
2. PC 등의 10분 이상 작업 중단시 비밀번호 등이 적용된 **화면보호** 조치
3. 단말기 최신 **백신** 운용・점검 및 운영체제・응응프로그램 최신 **보안패치** 유지
4. 업무상 **불필요한 응용프로그램** 설치 금지 및 **공유폴더 삭제**
5. 단말기 교체・반납・폐기 시 정보보안담당관과 협의, 하드디스크 수록 자료 유출・훼손 방지
6. 단말기 외부 **반・출입시** 최신 백신 등을 활용 해킹프로그램 **감염 점검**
7. 개인소유 단말기 **무단 반입 사용 금지**
8. 메신저・P2P・웹하드 등 **업무 무관 프로그램・비인가 장치 설치 금지**
9. 인터넷 PC에 문서편집기 사용금지 및 음란・도박 등 업무 무관 사이트 접근 차단

< 스마트폰 보안수칙 >

1. 의심스러운 애플리케이션은 다운로드 금지
2. 신뢰할 수 없는 사이트는 방문 금지
3. 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제
4. 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경
5. 블루투스・WIFI 등 무선 네트워크 기능은 사용시에만 활성화
6. 이상증상이 지속될 경우 악성코드 감염여부 확인
7. 중요회의시 스마트폰 휴대금지 또는 전원 차단
8. 백신 프로그램을 설치하고 정기적으로 바이러스 검사
9. 루팅 등을 통한 스마트폰 플랫폼의 구조 임의 변경 금지
10. 운영체제 및 백신 프로그램을 항상 최신버전으로 업데이트