서울특별시 서대문구 보안업무 처리 규정

전부개정규정을 이에 발령한다.

서울특별시 서대문구청장

2016년 2월 24일

서울특별시 서대문구 훈령 제163호

서울특별시 서대문구 보안업무 처리 규정 전부개정

서울특별시 서대문구 보안업무 처리 규정 전부를 다음과 같이 개정한다.

서울특별시 서대문구 보안업무 처리 규정

제1장 총칙

제1조(목적) 이 규정은 「보안업무규정」,「보안업무규정 시행규칙」, 「보안업무규정 시행세칙」,「서울특별시 보안업무 처리규칙」,「국가 공간정보 기본법」, 「국가공간정보 기본법 시행령」, 「서울특별시 정보통신 보안업무규정」에 따라 서울특별시 서대문구 본청, 보건소, 자연사박물관, 동 및 구의회사무국에서 적용·시행해야 할 보안업무 전반에 관한 사항을 규정함을 목적으로 한다.

제2조(정의) 이 규정에서 사용하는 용어의 뜻은 다음과 같다.

1. "비밀"이란 그 내용이 누설될 경우 국가안전보장에 해를 끼칠 우려가 있는 국가 기밀로서 「보안업무규정」(이하 "규정"이라 한다)에 비밀로 분류된 것을 말한다.
2. "대외비"란 비밀 외에 직무수행상 특별히 보호가 필요한 사항으로 비밀에 준하여 보관한다.
3. "보안사고"란 비밀이나 보안자재의 누설, 분실, 오인소각, 국가중요시설 및 장비의 파괴, 보호구역 내의 불법침입, 전산망의 무단침입 등의 사고를 말한다.

제3조(보안심사위원회의 설치) 서울특별시 서대문구(이하 “구”라 한다)의 보안업무를 효율적으로 수행하기 위하여 서울특별시 서대문구 보안심사위원회(이하 "위원회"라 한다)를 둔다.

제4조(위원회의 구성 등) ① 위원회의 위원장은 부구청장이 되고, 부위원장은 주민자치 관련 국장이 되며, 위원은 경제재정, 복지문화, 환경도시, 안전건설교통 관련 국장과 전산정보업무 관련 소관 과장이 된다.

② 위원장은 위원회를 대표하고, 위원회의 업무를 총괄한다.

③ 위원장이 부득이한 사유로 직무를 수행할 수 없을 때에는 부위원장이 그 직무를 대행한다.

④ 위원회에 위원회의 사무를 처리할 간사 1명을 두되, 간사는 보안업무 관련 소관 과장이 된다.

제5조(위원회 등의 임무) 위원회는 다음 각 호의 사항을 심의·의결한다.

1. 자체보안업무 향상을 위한 연구발전에 관한 사항
2. 보안업무 관련 내규의 제정 및 개정에 관한 사항
3. 신원특이자의 인사관리에 관한 사항
4. 경미한 보안위반자의 심사 처리에 관한 사항
5. 비밀취급인가에 관한 사항
6. 그 밖에 보안업무 수행에 따른 대책 및 수립에 관한 사항

제6조(의안의 제출 및 회의) ① 구 본청 및 보건소, 자연사박물관, 동, 구의회 사무국(이하 “소속기관”이라 한다)의 장이 소관업무에 대한 의안을 발의하고자 할 때에는 간사를 경유하여 발의한다.

② 위원회 개최 등 위원장이 회의를 소집하는 경우, 간사는 개최일자 통보 등 위원회 운영에 필요한 세부사항을 수행한다.

③ 위원회 등의 심의 사항은 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 의결한다.

④ 위원장은 필요하다고 인정할 때에는 관계 직원을 출석시켜 의견을 들을 수 있다.

⑤ 간사는 위원회 개최 시 회의록을 작성하여 2년간 유지하여야 한다. 이때 회의록은 서면 또는 녹음하여 전자파일, 테이프 등으로 보관할 수 있다.

⑥ 위원회 등의 심의 방법은 회의제를 원칙으로 하되, 필요시 서면으로 할 수 있다.

제2장 비밀의 보호

제7조(보안담당관의 지정) ① 규정 제43조에 따라 주민자치 소관 국장은 구 전체 보안담당관(이하 “보안담당관”이라 한다)이 된다. 다만, 정보통신 및 공간정보 보안담당관은 전산정보업무 관련 소관 과장이 된다.

② 보안담당관이 공석 중인 경우에는 당해 보안담당관의 직근 상급자가 그 직무를 대행한다.

제8조(분임보안담당관의 지정 등) ① 다음 각 호에 해당하는 자가 분임 보안담당관이 된다.

1. 구 본청 : 각 담당관 및 국장
2. 보건소 : 보건소장
3. 자연사박물관 : 박물관장
4. 동 : 동장
5. 구의회사무국 : 사무국장

② 보안담당관은 분임보안담당관으로 하여금 「보안업무규정 시행규칙」(이하 “시행규칙”이라 한다) 제68조에 따른 업무의 일부를 수행하게 할 수 있다.

③ 분임보안담당관은 소속부서의 보안업무를 지도·감독하여야 한다.

제9조(보안담당관의 업무관계) ① 보안담당관은 시행규칙 제68조의 업무를 수행하고, 구 본청 및 소속기관의 보안업무를 총괄 지도・감독한다.

② 보안담당관은 매년 구 전체 보안업무 실시계획을 수립하여 서울특별시(이하 “시”라 한다) 전체 보안담당관에게 제출하여야 한다.

제10조(보안담당관 인계인수) 보안담당관이 교체되어 인계인수할 때에는 구청장의 입회하에 다음 각 호의 사항을 인계·인수하여야 한다.

1. 자체보안업무 내규
2. 비밀취급 인가자 현황
3. 비밀소유현황
4. 비밀보관단위 및 비밀보관책임자

5. 암호자재 관리 현황
6. 당면과제(인원, 문서, 자재, 시설 등 문제점)
7. 보안업무 관련 진행사항
8. 그 밖에 참고사항

제11조(비밀보관책임자) ① 다음 각 호에 해당하는 사람은 따로 발령함이 없이 규정 제20조에 따라 Ⅱ급 및 Ⅲ급 비밀보관책임자가 된다.
1. 구 본청, 보건소 : 각 담당관 및 과장
2. 자연사박물관 : 박물관장
3. 동 : 동장
4. 구의회사무국 : 사무국장
② 제1항의 비밀보관책임자는 그 차하위 직위에 있는 사람을 부책임자로 지정할 수 있다.
③ 보관 부책임자는 비밀보관 정책임자가 유고시 그 직무를 대행한다.

제12조(보안교육) 보안담당관은 소속직원에 대한 보안교육 책임을 지며, 시행규칙 제69조제1항 각 호에 정한 자에게는 사전에 충분한 교육과 보안조치를 실행하여야 한다.

제13조(비밀취급 인가권자) ① 규정 제9조제2항제3호에 따라 구청장은 소속 공무원과 직원에 대하여 Ⅱ급 및 Ⅲ급 비밀취급을 인가한다.
② 제1항에서 Ⅱ급 이하의 비밀취급인가권 직위에 보직된 자는 별도 비밀취급인가 절차 없이 임용과 동시에 비밀취급을 인가한 것으로 보고, 위임 받은 비밀취급인가권은 이를 다시 재위임할 수 없다.

제14조(자체보안내규 수립·시행) 제13조에 따라 비밀취급 인가권자인 구청장은 규정·시행규칙 및 시행세칙의 범위에서 자체 보안내규를 수립·시행하여야 한다.

제15조(비밀의 인가 및 취급의 한계) ① 제13조에 따른 비밀취급인가는 위임받은 인가등급에 한정하고 또한 업무수행에 필요한 최소한의 인원에 한정하

여 인가하여야 한다.

② 비밀취급인가를 받은 자가 취급할 수 있는 비밀의 한계는 담당업무 범위에 한정되며 인가 받은 비밀등급보다 상위등급의 비밀 또는 담당업무 이외의 비밀에 대해서는 취급할 수 없다.

제16조(비밀취급인가 사무) 비밀취급인가 사무는 비밀취급인가 총괄 부서에서 구 소속 공무원과 업무상 조정감독을 받는 민간인을 총괄 취급한다.

제17조(특별인가) ① 다음 각 호에 정한 자는 별도 비밀취급인가 절차없이 Ⅱ급 비밀의 취급권이 인가된 것으로 보며, 비밀취급이 불필요한 직위로 임용되는 때에는 해제된 것으로 본다.

1. 부구청장
2. 각 국장, 보건소장, 구의회사무국장
3. 각 담당관·과장·동장
4. 각 담당관·과·동 주무팀장 및 보안업무 담당자
5. 비밀을 취급하는 업무(기록물관리, 주민등록, 민방위, 감염병관리 업무 등)를 담당하는 자
6. 업무의 특성상 비밀을 취급하는 부서(전산정보과 등)로 임용되는 자

② 제1항에 따라 특별인가 및 해제된 자에 대하여는 각 담당관·과·동·사업소별로 제20조에 따른 비밀취급인가대장에 기록·유지하여야 한다.

③ 제1항의 해당자 중 신원특이자는 위원회에서 인가여부를 결정하고 불가로 결정된 자는 즉시 인사조치를 하여야 한다.

제18조(민간인에 대한 비밀취급인가) ① 구청장은 시행규칙 제13조에 따라 업무상 조정·감독을 받는 민간인에 대한 비밀취급인가 시에는 사전에 국가정보원장과 협의 보안대책을 강구하여야 한다.

② 제1항의 경우 해당 민간인 신원조사는 소관에 따라 분임보안담당관이 요청하며, 분임보안담당관이 그 신원조사회보서(시행규칙 별지 제23호서식)를 받은 때에는 관계 서류를 첨부하여 이를 보안담당관에게 제출하여야 한다.

③ 제2항의 분임보안담당관은 해당 민간인의 보안에 관한 교육 및 지도·감독을 하여야 한다.

제19조(서약 및 교육) ① 비밀취급을 인가할 때에는 임용권자 또는 보안담당관이 시행규칙 제14조에 따른 서약을 받고 기초 보안교육을 실시하여야 한다. 다만, 제17조에 따라 특별인가를 받은 자는 시행규칙 제5조 별지 제5호서식의 서약서를 보안담당관에게 제출하여야 한다.

② 공무원이 퇴직 시에는 근무 중 지득한 기밀의 누설방지를 위한 보안교육을 실시한 후 별지 제1호서식에 따른 서약을 받아 관리하여야 한다. 이 경우 서약집행은 구청장이나 보안담당관 또는 각 담당관·과장급이상 직근 상급자가 된다.

제20조(비밀취급인가대장) 비밀보관책임자는 별지 제2호서식에 따른 비밀취급인가대장(누년 일련번호와 연도별)을 작성·비치하고 인가 및 해제사유를 기록·유지한다.

제3장 인원보안

제21조(신원조사 책임) 규정 제33조에 따른 신원조사는 임용 전에 실시하고 회보 사항을 신중히 검토하여야 한다.

제22조(신원조사 회보서) ① 신원조사회보서는 공무원 인사기록 및 「서울특별시 서대문구 지방공무원 인사규칙」에서 정하는 바에 따라 관리한다.

② 제1항의 인사기록을 보유하지 아니할 경우에는 신원조사회보서 사본을 비치하여야 한다.

③ 소속 공무원이 타 기관으로 전출할 때에는 신원조사회보서 또는 그 사본을 전출기관에 이송하여야 한다.

제23조(신원대장) ① 구청장은 소속 직원의 현재원을 중심으로 별지 제3호서식에 따른 신원대장을 기록·유지하여야 한다.

② 제1항의 신원대장은 연도별로 국·과별 또는 직급별로 하여야 한다.

제24조(신원특이자 관리) 구청장은 신원조사회보서에 신원특이내용이 있는 자는 보직결정 등 보안상 적성을 판단하는 자료로 활용할 수 있도록 관리한

다.

제25조(외국인 공직임용 관련 보안대책) ① 업무상 자문 및 기타의 목적을 위하여 외국인과 고용계약을 체결할 경우에는 임용 30일 전에 국가정보원에 신원조사를 의뢰하여야 하며, 신원특이자는 위원회의 심의를 거쳐 임용여부를 결정하여야 한다.
② 고용계약 체결 시에는 근무 중 알게 된 기밀사항을 계약시간 중이나 계약만료 후에 누설할 경우의 손해배상책임과 피고용인 업무의 한계 설정 등 보안 유의사항을 명시하여 계약서를 작성하고 서약을 집행하여야 한다.
③ 공직에 임용된 외국인에 대해서는 보안교육을 포함한 공직자로서의 기본자세 및 보안준수 등 의무사항에 대한 기본교육을 실시하여야 한다.
④ 국가 중요정책 등 민감한 내용을 다루는 회의에 외국인 공직자를 참석시킬 필요가 있을 경우에는 위원회에서 사전 보안성 검토를 실시하여야 하며, 회의종료 후 외국인 공직자에게 배포한 관련자료를 회수 하여야 한다.
⑤ 재직 중인 외국인이 퇴직할 경우에는 제19조제2항을 준용한다.

제26조(무기계약직, 임시직, 단순고용직 채용) ① 무기계약직, 임시직, 단순고용직을 채용하고자 할 때에는 보안담당관의 사전 협의를 거쳐야 한다.
② 임시직이나 단순고용직으로 채용되는 사람 중 중요시설·지역의 통제·출입 및 중요 문서·자재의 취급자로서 소속 부서장이 보안상 필요로 하는 자 외에는 신원조사를 생략한다.
③ 무기계약직으로 채용되는 자는 「서울특별시 서대문구 공무직 등 관리 규정」제9조에 따라 신원조사를 의뢰하여야 하며, 신원조사회보서 결과 부적격자로 판명될 경우 채용해서는 아니 된다.

제27조(무기계약직, 임시직, 단순고용직 보안조치) ① 무기계약직, 임시직, 단순고용직에게는 보안상 책임 있는 임무를 부여하여서는 아니 된다.
② 부득이 비밀취급을 인가하고자 할 때에는 위원회 또는 자체 심의기구의 의결을 거쳐야 한다.
③ 무기계약직, 임시직, 단순고용직 중 사무업무(행정문서 작성, 행정보조, 문서수발)와 사무실을 수시 출입하는 업무(청사 청소 등)를 부여하고자 할

때는 소속 부서장은 별지 제4호서식의 서약서를 받아야 한다.
④ 무기계약직, 임시직 또는 단순고용직으로 인하여 야기되는 보안책임은 소속 부서장이 진다.

제28조(공무국외여행공무원 보안조치) 공무국외여행공무원 보안교육은 소속기관 또는 국외여행 추천기관의 보안담당관 또는 분임보안담당관이 행한다.

제4장 문서보안

제29조(비밀세부분류지침) 구청장은 국가정보원장이 작성 배부한 비밀세부분류지침을 구 본청 및 소속기관에 시달하고, 이 지침이 변경이 있을 때에는 구 본청 및 소속기관에 변경 시달한다.

제30조(비밀의 분류) ① 비밀의 분류는 비밀세부분류지침에 의하되 규정 제11조 및 제12조에 따라 비밀분류 3대원칙(과대·과소분류 금지, 독립분류, 섭외비밀의 존중)에 따라 분류하여야 한다. 다만, 위 지침에 포함되지 아니한 사항은 해당 비밀보관책임자가 보안담당관과 협의하여 정한다.
② 비밀문서는 동일한 사본이라도 건마다 별개의 관리번호를 부여하여야 하며 필요시에는 수정 기안할 수 있다.
③ 협조권자 및 최종결재권자는 결재과정에서 분류지침 및 분류 3대 원칙에 의하여 비밀분류사항을 검토 조정하여야 하며 분류조정 하였을 때에는 기안용지 결재자란에 분류조정사항을 기록하여 조정에 따른 보안 조치를 마련하여야 한다.
④ 분류착오로 인한 보안사고에 대해서는 기안자, 중간보고자 및 최종 결재권자가 연대책임을 진다.
⑤ 비밀을 결재·공람하기 위하여 그 요지를 기재한 요약서도 해당 등급으로 분류하여야 한다. 다만, 이 경우의 예고문, 사본번호 및 관리번호는 부여하지 아니하되 반드시 비밀에 첨부되어야 한다.

제31조(비밀소유현황 조사 보고) 구청장은 비밀소유현황조사서(시행규칙 별지 제18호서식)를 6월 말과 12월 말을 기준 작성하여 조사 기준일 다음 달 10

일까지 시 보안담당관에게 제출하여야 한다.

제32조(불필요한 비밀의 정리방법) 규정 제15조제2항제3호에 따라 소유 비밀을 파기하고자 할 때에는 목록을 작성하여 보안담당관을 경유, 구청장의 승인을 받아 파기 조치한다.

제33조(비밀의 수발) ① 문서 주관과에서는 비밀문서 접수부와 발송부 (시행규칙 별지 제14호서식)를 각각 비치하고 그 수발 사항을 기록하여야 하며, 접수문서는 그 문서의 주관과에 직접 인계하고 발송문서는 그 문서의 수신기관으로 발송한다.

② 비밀문서의 수발사무는 일반문서 수발 부서에서 담당하며, Ⅱ급 비밀취급이 인가된 공무원이 담당하여야 한다.

제34조(비밀의 기록관리) ① 비밀의 작성과 등급변경, 파기, 이송 및 수발에 관한 일체의 관리사항을 비밀관리기록부(시행규칙 별지 제13호서식)에 기록·유지하여야 한다.

② 비밀을 재분류 또는 이송하였을 때에는 비밀관리기록부 상의 비밀등급, 형태, 건명, 사본번호만을 2개의 적선으로 삭선하여 삭제부분을 해독할 수 있도록 하고, 그 사유를 재분류란에 기록하여야 한다.

제35조(비밀관리기록부의 갱신) ① 비밀관리기록부는 다음 각 호에 해당하는 경우에는 이를 갱신할 수 있다.

1. 비밀관리기록부의 훼손으로 인하여 그 내용을 알아보기가 어려운 경우
2. 서식의 개정 및 그 밖의 사유로 비밀관리기록부를 정리할 필요가 있는 경우

② 비밀보관책임자는 비밀관리기록부를 갱신하고자 하는 경우에는 미리 보안담당관의 승인을 받아 구 비밀관리기록부의 최종기재란 밑에 주선으로 마감하고, 다음과 같이 신 비밀관리기록부로 이기한 내용을 기재하여야 한다.

신 비밀관리기록부에 이기함.

급 비밀 건

년 월 일

이 기 자 직급 성명 (인)

보관책임자 직급 성명 (인)

보안담당관 직급 성명 (인)

③ 신 비밀관리기록부는 구 비밀관리기록부에서 비밀을 이기한 다음에, 제2항의 내용과 같은 이기사항을 기재한다. 이 경우 이기 사항 중 “신 비밀관리기록부에 이기 함”을 “구 비밀관리기록부에서 이기함”으로 한다.

제36조(대외비문서 관리) ① 규정 제4조에서 규정한 비밀 이외의 사항으로서 직무 수행상 특별히 보호가 필요한 사항은 시행규칙 제16조제3항에 따라 대외비로 분류하고 제4항에 따른 표시를 하여야 한다.

② 대외비문서의 수발은 제33조를 준용하여 수발하며 일반문서와 혼합보관할 수 없으며 비밀보관함 또는 이에 준하는 용기에 별도 보관하여야 한다.

③ 대외비문서는 비밀보관책임자가 집중 관리하여야 한다.

④ 대외비문서는 시행규칙 제40조 및 제42조와 제43조제1항에 준하여 관리번호 및 사본번호의 기재와 대외비 문서 원본 말미에 배포선을 작성 첨부하여야 한다.

⑤ 대외비문서에도 시행규칙 제18조제1항부터 제6항까지의 규정을 준하여 예고문을 기재하여야 한다.

⑥ 대외비 보관책임자는 대외비관리기록부를 비치하고 건마다 별개의 관리번호를 부여하여야 한다. 다만, 15일 이내 주기적으로 생산되는 문서는 문서철에 관리 번호를 부여하고 표지내부에 색인목록을 첨부하여 1건으로 합철 관리할 수 있다.

⑦ 대외비 보관책임자가 교체되었을 때에는 비밀문서에 준하여 인계·인수를 실시하여야 하며, 보안담당관이 확인하여야 한다.

제37조(접수증의 관리) ① 시행규칙 제32조에 따라 문서수발 계통을 통하여 발송된 비밀문서의 접수증은 문서접수 담당자가 접수한 즉시 비밀의 발송기관에 반송하여야 하며, 비밀발송부서에서 접수증을 받아 보관한다.

② 비밀접수증은 접수증철을 비치하고 연도별로 구분하여 일련번호를 부여

한다. 다만, 접수증의 수가 적어 연도별로 구분할 필요가 없을 때에는 계속 일련번호를 부여하여 관리할 수 있다.

제38조(비밀의 대출 및 열람) 비밀의 대출 및 열람은 시행규칙 제45조에 따라야 하며, 비밀이 자재인 경우에는 따로 시행규칙 별지16호서식의 비밀열람기록전을 비치하고 기록·유지하여야 한다.

제39조(연습관계부책) ① 을지연습 등 연습관계 비밀을 취급하기 위하여 별도의 비밀관리기록부, 비밀수발대장 및 그 밖의 대장을 비치 사용할 수 있다.
② 제1항에 따른 비밀관리기록부, 비밀수발대장, 그 밖의 장부는 이 규정에서 정하는 바에 따라 취급한다. 다만 비밀접수증과 열람기록전 제도는 제외한다.

제40조(비밀의 반출) 규정 제27조에 따른 비밀을 반출하고자 할 때에는 시행규칙 제48조에 따라야 한다. 다만, 구청장의 승인을 보안담당관의 승인으로 갈음할 수 있다.

제41조(비밀보관책임자의 교체) ① 비밀보관책임자 교체 시의 인계·인수는 시행규칙 제36조제1항에 따른다.
② 인계인수 요령은 시행규칙 제36조제2항에 따라 비밀관리기록부 중앙여백에 예시와 같이 실시한다.

다음과 같이 정히 인계인수함.

급 건

년 월 일

인	계	자	직명	성명 (인)
인	수	자	직명	성명 (인)
확인자(보안담당관)			직명	성명 (인)

제42조(보관용기) 비밀의 보관용기(금고 또는 이중캐비넷)는 각 부서의 비밀보관책임자 단위로 비치하고 열쇠는 반드시 이중으로 장치를 하여야 하며, 보

관용기 외부에는 어떠한 이유를 막론하고 비밀의 보관을 알리는 표시를 하여서는 아니 된다.

제43조(발간업체의 지정) 비밀 또는 대외비문서의 발간은 자체시설을 이용함을 원칙으로 한다. 다만, 민간시설을 이용할 때에는 비밀취급을 인가 받은 발간업체를 이용하여야 한다.

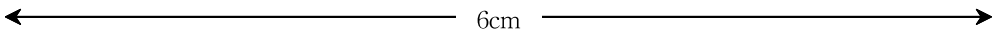
제44조(작업일지의 비치) 자체시설 및 민간시설을 이용 비밀을 발간할 때에는 비밀 입력·출력 및 작업대장(별지 제5호서식)에 그 내용을 기록·유지하여야 한다.

제45조(비밀·대외비 문서의 발간통제 및 승인) ① 민간시설을 이용하여 비밀·대외비 문서를 인쇄·발간 또는 제작하거나 복제·복사 하고자 할 때에는 사전에 별지 제6호서식의 비밀(대외비)문서 발간신청서를 보안담당관에게 제출하여야 한다.

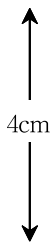
② 보안담당관이 제1항에서 정한 승인 시 사전 검토사항은 다음과 같다.

1. 외주 발간의 타당성
2. 비밀 발간량의 적합성
3. 민간시설 보안대책의 타당성
4. 입회자 지정의 적합성
5. 그 밖에 보안 관리상 저촉 여부

③ 보안담당관은 제1항의 신청서를 접수 후 발간의 필요성이 있다고 인정될 때에는 다음과 같은 비밀발간승인을 비밀문서의 원본 첫면 여백에 날인하고 별지 제7호서식의 비밀(대외비)문서 통제대장에 기록 유지하고 별지 제8호서식의 비밀문서 조달의뢰확인서를 발급한다.



( )급 비밀발간승인			
업 체			
부 수		인가근거	
통제관		통제일시	



④ 회계절차에 따라 계약자가 선정되면 주무과 담당자 또는 입회자가 직접 원고를 발간업체에 수교(직접 건네줌)한다.
⑤ 비밀 발간 시 입회 감독자는 모든 작업과정에 입회하여 요구부수와 발행 수량을 확인하고 원지, 파지, 잔여부수 및 기타 폐지 등은 세절 또는 소각하고 납품 시까지 입회하여야 한다.

제46조(비밀문서의 처리) ① 비밀문서 파기 시는 세절 또는 소각 등의 방법으로 원형을 알아 볼 수 없도록 완전히 파기한다.
② 비밀용기는 비밀보관책임자가 별도 비치하고 보안상 유해로운 비밀문서는 비밀용기에 수집하여 세절 또는 소각한다.
③ 비밀보관책임자가 비밀용기 열쇠를 보안 및 방화점검 책임자에게 보관하도록 한다.
④ 비밀문서 세절 또는 소각은 반드시 입회자 1명과 함께 실시한다.

제47조(안전반출 및 파기계획) ① 구청장은 비상안전반출 및 파기계획에 따라 비상시 행동한다.
② 보안담당관은 자체 실정에 적응할 수 있는 안전반출장소, 운반기구 등에 대한 반출계획표를 작성하되 토요일·공휴일 및 야간 등 평상시 지휘계통이 없을 때에 중점을 두어 작성·비치한다.
③ 공간정보의 안진반출 및 파기계획은 별표1과 같으며, 공간정보를 관리하는 부서의 장은 자체 실정에 맞는 공간정보 안전반출 및 파기계획을 작성·비치하여야 한다.

제48조(외국인에게 자료 제공 시 보안대책) ① 외국인에게 각종 자료를 제공하고자 할 때에는 사전에 외국인의 국적, 직업, 성명, 연령, 제공자료명, 제공목적 및 기타 참고사항을 포함한 신청서에 제공하고자 하는 자료 사본 1부를 첨부하여 보안담당관 또는 분임보안담당관에게 제출하여야 한다. 다만, 관광안내서 등과 같이 수시 외국인에게 제공하도록 되어 있는 자료는 제외한다.
② 제1항의 신청서를 받은 보안담당관 또는 분임보안담당관은 그 내용을 검토하여 보완 및 제공목적상 필요하다고 인정될 때에는 구청장의 결재를 득

하여 승인하고 그 통제사항을 별지 제9호서식의 대장에 기록·유지한다.
③ 제1항에 따라 제공된 자료 사본은 3년간 보관한다.

제49조(외국인 접촉 시 보안관리) ① 정보활동이 예상되는 외국공관원 등과 접촉할 경우에는 미리 별지 제10호서식의 외국공관원 접촉신청서를 작성하여 소속 부서장의 승인을 받아야 한다.
② 제1항에 따른 외국인 접촉 종료 시 별지 제11호서식에 따라 외국공관원 접촉결과 보고서를 작성하여 소속 부서장에게 보고하고 보안담당관에게 이를 통보하여야 한다.
③ 보안담당관은 소속 직원들의 외국공관원 접촉과정에서 보안상 위해로운 사항이 발견된 경우 지체 없이 국가정보원에 통보하여야 한다.

제50조(국회·시의회·구의회 등 자료 제공 시 보안대책) 국회·시의회·구의회 등 대외기관에 비밀 및 보안성이 요구되는 자료를 제공 또는 설명하고자 할 경우에는 위원회 심의 등 사전 보안성 검토를 실시하여야 하며, 자료제공 또는 설명창구는 정책기획담당관으로 일원화 하여야 한다.

제51조(비밀과제 외주 용역 시 보안대책) ① 비밀문서의 외주 용역 시에는 의뢰부서의 장이 사전에 보안성검토를 하고 적정 비밀로 분류하여 용역을 의뢰하여야 한다.
② 비밀과제의 용역계약서에는 비밀엄수의무와 임의사용 시 손해배상 책임을 명시하여야 하며, 의뢰부서의 장은 참여자의 신원확인, 보안준수의무 고지, 서약집행 등 보안조치를 마련하고 보안관리책임자를 지정하여 연구수행 과정의 보안감독업무를 수행하도록 하여야 한다.
③ 보안관리책임자는 용역 종료 시 성과물, 각종 제공자료 및 저장매체를 전량 회수하고 PC 내 용역관련 자료를 삭제한다.
④ 비밀정책 또는 비밀과제연구 관련 회의를 개최하는 부서의 장은 참여자에 대한 사전 보안준수사항을 고지한 후 보안서약을 집행하고, 회의자료를 적정 비밀로 분류하여 회의종료 후 회수하는 등 회의장 접근통제 및 자료의 유출방지대책을 마련하여야 한다.

제52조(중요 정책자료 등에 대한 보안관리) ① 중요정책 및 사업 중 누설되면 그 정책 및 사업추진에 지장을 초래할 우려가 있거나, 직무수행상 특별한 보호가 필요한 자료는 입안단계에서부터 적정등급의 비밀 또는 대외비로 분류하여야 한다.

② 비밀(대외비) 정책 또는 사업의 추진을 위하여 관계자 회의 등을 개최하는 기관(부서)의 장은 참여자에게 사전에 보안준수사항을 고지한 후 서약을 집행하고, 회의 시 배포하는 자료는 적정등급의 비밀 또는 대외비로 분류하고 회의종료 후 회수하는 등 비밀(대외비)정책 및 자료의 유출방지대책을 마련하여야 한다.

제5장 정보통신보안

제53조(정보통신보안업무) 보안담당관의 정보통신보안업무는 다음 각 호와 같다.

1. 정보통신보안 활용계획 수립 및 시행
2. 자체 정보통신망에 대한 보안대책 수립 및 시행(신·증설 포함)
3. 정보화자료 보안 관리
4. 보안시스템 및 보안자재 운용 관리
5. 정보통신보안사고의 처리
6. 정보통신보안교육 계획수립 및 시행
7. 정보통신보안업무 지도·조정 및 감독
8. 그 밖의 정보통신보안업무 관련 사항

제54조(정보통신보안성 검토) ① 정보통신담당 부서장은 업무에 대한 정보화를 추진하려면 계획수립 단계부터 자체 보안대책을 강구하여야 한다.

② 다음 각 호의 어느 하나에 해당하는 경우에는 서울특별시 보안담당관을 경유하여 국가정보원장의 보안성 검토를 받아야 한다.

1. 홈페이지, 업무시스템 등 정보시스템 구축
2. 인터넷전화, CCTV, 무선 WiFi 등 유·무선 네트워크 시스템 구축
3. 정보통신기반시설의 제어시스템 구축

4. 원격근무시스템, 원격 화상회의시스템 구축
5. 와이브로·스마트폰 등 첨단 IT기술을 업무에 활용하는 시스템 구축
6. 국가용 보안시스템과 상용 암호모듈·정보보호시스템을 도입 운용하고자 할 경우
7. 내부 정보통신망을 인터넷이나 타 기관 통신망 등 외부망과 연동하는 경우
8. 업무망과 인터넷 분리 사업
9. 외부업체 보안컨설팅 실시
10. 그밖에 정보통신담당 부서장이 보안성검토가 필요하다고 판단하는 정보화사업

제55조(정보화자료의 보호대책) 정보통신담당 부서장은 자료의 유출 파괴 등에 대비하여 다음 각 호의 어느 하나에서 정한 보호대책을 강구하여야 한다.
1. 자료복사본(예비) 확보 및 안전지역 별도 보관
2. 정보화자료(보조기억매체) 보유현황 관리
3. 정보화자료 및 장비의 반출·입 통제
4. 정보통신망 불법침입(해킹) 및 바이러스 피해 예방

제56조(정보통신실의 보호대책) 정보통신담당 부서장은 다음 각 호 사항을 참고하여 지정된 보호구역에 대한 보안대책을 마련해야 한다.
1. 방재대책 및 외부로부터의 위해(危害)방지대책
2. 상시 이용하는 출입문은 한 곳으로 정하고 이중 잠금장치 설치
3. 출입자 인증·식별 등을 위한 출입문 보안장치 설치 및 주야간 감시대책
4. 휴대용 저장매체를 보관할 수 있는 용기 비치
5. 정보시스템 안전지출 및 긴급 파기 계획 수립
6. 관리책임자 및 자료·장비별 취급자 지정 운용
7. 정전에 대비한 비상전원 공급, 시스템의 안정적 중단 등 전력관리 대책
8. 비상조명 장치 등 비상탈출 대책
9. 전자파 누설 방지 대책
10. 카메라 장착 휴대폰 등을 이용한 불법 촬영 방지 대책 등

제57조(보호우선순위 부여) ① 정보통신담당 부서장은 보유·관리하고 있는 정보화자료의 중요도를 고려하여 자료를 체계적으로 분류·관리하여야 한다.
② 정보통신실에 보관되어 있는 각종 정보화자료를 별표 2의 분류기준에 따라 가급·나급·다급 등 보호등급으로 구분 관리하여야 한다. 다만, 비밀자료는 제4장 문서보안 규정을 따른다.

제58조(자료접근 범위의 제한) ① 시스템관리자는 자료사용을 필요 정도에 따라 최소한의 자료만 사용하도록 자료접근 범위를 제한하여야 한다.
② 자료접근 범위는 다음 각 호와 같이 구분한다.
1. 자료별로 접근 권한이 있는 사람을 제한
2. 작업범위는 소관 업무에 따라 열람·출력·갱신 등으로 제한
3. 열람항목을 필요 정도에 따라 기본항목·전항목 등으로 제한

제59조(서버 보안관리) ① 서버 관리자는 서버를 도입·운용할 경우, 정보통신담당 부서장과 협의하여 해킹을 이용한 자료 절취, 위·변조 등에 대비한 보안대책을 수립·시행하여야 한다.
② 서버 관리자는 서버내 저장자료에 대해 업무별·자료별 중요도에 따라 사용자의 접근권한을 차등 부여하여야 한다.
③ 서버 관리자는 사용자별 자료의 접근범위를 서버에 등록하여 인가여부를 식별토록 하고 인가된 범위 이외의 자료접근을 통제하여야 한다.
④ 서버 관리자는 서버의 운용에 필요한 서비스 포트 외에 불필요한 서비스 포트를 제거하며 관리용 서비스와 사용자용 서비스를 분리 운용하여야 한다.
⑤ 서버 관리자는 서버의 관리용서비스 접속시 특정IP와 MAC주소가 부여된 관리용 단말을 지정·운용하여야 한다.
⑥ 서버 관리자는 서버 설정 정보 및 서버에 저장된 자료에 대해서는 정기적으로 백업을 실시하여 복구 및 침해 행위에 대비하여야 한다.
⑦ 서버 관리자는 Database에 대하여 사용자의 직접적인 접속을 차단하고 개인정보 등 주요정보를 암호화하는 등 Database별 보안조치를 실시하여야 한다.
⑧ 정보통신담당 부서장은 제1항부터 제7항까지에서 수립한 보안대책의 적

절성을 수시로 확인하되, 연1회 이상 보안도구를 이용하여 서버 설정 정보 및 저장자료의 절취, 위·변조 가능성 등 보안취약점을 점검하여야 한다.

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

② 정보통신담당 부서장은 비인가자가 PC 등을 무단으로 조작하여 전산자료를 절취, 위·변조 및 훼손시키지 못하도록 다음 각 호의 보호대책을 사용자에게 공지하며, 사용자는 이를 준수하여야 한다.

1. 장비(CMOS 비밀번호)·자료(문서자료 암호화 비밀번호)·사용자(로그온 비밀번호)별 비밀번호의 주기적 변경
2. 10분 이상 PC 등의 작업 중단시 비밀번호 등이 적용된 화면보호 조치
3. PC 용 최신 백신 운용·점검, 침입차단·탐지시스템 등을 운용하고 운영체제(OS) 및 응용프로그램(아래아한글, MS Office, Acrobat 등)의 최신 보안패치 유지
4. 음란·도박·증권 또는 메신저·P2P·웹하드 등 업무상 불필요한 응용프로그램 설치 금지 및 접근차단 조치
5. 비인가 또는 보안에 취약한 프로그램·장치의 설치 금지 및 공유 폴더 삭제
6. 그 밖에 국가정보원장이 안전성을 확인하여 배포 승인한 프로그램의 운용 및 보안권고문

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

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

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

제61조(비밀번호 관리) ① 시스템관리자는 정보시스템 비밀번호의 무단 사용 방지를 위하여 다음 각 호와 같이 비밀번호를 구분하여 사용하여야 한다.

1. 비인가자의 정보시스템 접근방지를 위한 장비 접근용 비밀번호(1차)
2. 사용자가 정보시스템 접속 시 인가된 인원인지 여부를 확인하는 사용자 인증 비밀번호(2차)
3. 문서의 열람·수정 및 출력 등 사용권한을 제한할 수 있는 자료별 비밀번호(3차)

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

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

1. 사용자계정(ID)과 동일하지 않은 것
2. 개인 신상 및 부서명칭 등과 관계가 없는 것
3. 일반 사전에 등록된 단어는 사용을 피할 것
4. 동일단어 또는 숫자를 반복하여 사용하지 말 것
5. 사용된 비밀번호는 재사용하지 말 것
6. 동일 비밀번호를 여러 사람이 공유하여 사용하지 말 것
7. 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지

④ 서버에 등록된 비밀번호는 암호화하여 저장하여야 한다.

제62조(비밀자료 입력) ① 대외비 이상의 비밀자료를 입력하려면 반드시 해당 비밀등급과 예고문을 동시에 입력하여 열람 또는 출력 시 비밀등급과 예고문이 표시되도록 하여야 한다.

② 비밀자료를 입력할 때에는 미리 비밀자료만을 입력할 컴퓨터 또는 개인용컴퓨터로부터 분리가 가능한 보조기억매체를 별도로 지정하여 사용하고 그 보조기억매체에는 비밀자료만을 입력하여야 한다. 다만, 주전산기와 분리가 불가능할 경우에는 독립된 파일을 지정하여 입력한다.

③ 비밀자료를 입력한 때에는 비밀 입·출력 및 작업대장(별지 제5호서식)에 작업내용을 기록·유지하여야 한다.

제63조(보조기억매체 보안대책) ① 보조기억매체 관리책임자는 보조기억매체를 사용하여 업무자료를 보관할 필요가 있을 때에는 위변조, 훼손, 분실 등

에 대비한 보안대책을 강구하여 정보통신담당 부서장의 승인을 받아야 한다.

② 보조기억매체 관리책임자는 보조기억매체를 비밀용, 일반용으로 구분하고 주기적으로 수량 및 보관 상태를 점검하며 반출·입을 통제하여야 한다.

③ 보조기억매체 관리책임자는 USB 관리시스템을 도입할 경우 국가정보원장이 안정성을 확인한 제품을 도입하여야 한다.

④ 보조기억매체 관리책임자는 사용자가 USB메모리를 PC 등에 연결시 자동실행되지 않도록 하고 최신 백신으로 악성코드 감염여부를 자동 검사하도록 보안 설정한다.

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

⑥ 보조기억매체를 파기 등 불용처리 하거나 비밀용을 일반용 또는 다른 등급의 비밀용으로 전환하여 사용할 경우 저장되어 있는 정보의 복구가 불가능하도록 완전삭제 프로그램을 사용하여야 한다.

⑦ 정보통신담당 부서장은 사용자의 보조기억매체 무단 반출 및 미등록 보조기억매체 사용 여부 등 보안관리 실태를 주기적으로 점검하여야 한다.

제64조(비밀자료의 출력) ① 비밀자료의 열람 또는 출력을 의뢰하려면 비밀자료출력(열람) 신청서(별지 제17호서식)에 따라 미리 자료제공출력부서에 제출하여야 한다.

② 비밀자료를 출력할 때에는 출력일시, 면표시 및 출력한 정보통신장비의 고유번호가 자동표시 되도록 하여야 한다.

③ 비밀자료가 입력된 보조기억매체를 이용하여 비밀자료를 출력(생산) 완료한 후에는 입력된 비밀내용을 소자 처리하여야 하며, 그 중 업무상 계속 보관이 필요한 경우에는 보안책임자의 승인을 받아 소자하지 아니할 수 있다.

④ 취급자가 비밀자료를 열람 또는 출력한 때에는 비밀 입·출력 및 작업대장(별지 제5호서식)에 열람 및 출력사항을 기록하고, 열람자 및 출력자료 수

령자의 서명을 받아야 한다.

⑤ 취급자는 비밀자료 출력 시 발생한 파지 등을 작업종료 후 회수하여 즉시 파기하고 비밀자료 입·출력대장의 비고란에 기록하여야 한다.

⑥ 출력된 비밀자료는 제4장 문서보안 규정에 따라 취급·관리하여야 한다.

제65조(접근기록 관리) ① 시스템관리자는 정보시스템의 효율적인 통제·관리, 사고발생시 추적 등을 위하여 사용자의 정보시스템 접근기록을 유지·관리하여야 한다.

② 제1항의 접근기록에는 다음 각 호의 내용이 포함되어야 한다.

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

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

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

제66조(비밀정보화자료 송·수신시 보안대책) 정보통신망을 이용하여 비밀자료를 송·수신하려면 다음 각 호에 정하는 보호대책을 강구하여야 한다.

1. 자료내용을 암호화하여 송·수신할 수 있는 인가된 보안시스템 부가 설치·운영
2. 통신선로 및 배전반에 대한 보호대책 강구

제67조(정보통신망 접속시 보안대책) ① 정보통신담당 부서장은 자료의 유출 방지 등을 위해 내부망과 외부망과의 접속을 최소한으로 제한하여야 한다.

② 내부망과 외부망을 접속하려면 비인가자의 무단침입 방지를 위해 비인가자를 색출하고 차단하는 정보통신망 보호조치를 취하여야 한다.

제68조(정보통신망 유지·보수 시 보안대책) 컴퓨터, 프로그램, 통신망 등의 유

지·보수 시 외부업체의 온라인 유지·보수 작업을 금하여야 한다.

제69조(암호프로그램의 개발) ① 정보통신망을 이용하여 Ⅱ급 비밀 이하 내용을 소통하려면 국가정보원이 인가한 기관에 요청하여 지원받은 암호프로그램을 사용하여야 한다.

② 정보통신망을 이용하여 Ⅲ급 비밀 이하 내용을 소통하려면 소요기관 자체에서 암호프로그램을 개발하여 사용할 수 있다.

제70조(암호프로그램의 운영) 암호프로그램을 운용하거나 변경하려면 국가정보원장의 비밀 승인을 받은 후 사용하여야 한다. 이 경우 비밀승인에 필요한 사항은 별도로 정한다.

제71조(암호프로그램의 변경) 정보통신담당 부서장은 자료 내용의 보안을 위하여 암호프로그램을 주기적으로 변경·운영하여야 한다. 이 경우 변경주기는 별도로 정한다.

제72조(암호프로그램 취급자 지정) 다음 각 호에 해당하는 사람은 암호 프로그램의 취급관리를 위해 암호자재 취급인가를 받아야 한다.

1. 암호프로그램 취급기관의 정보통신 분임보안담당관
2. 암호프로그램 개발요원

제73조(암호프로그램의 관리) 승인된 암호프로그램은 Ⅱ급 비밀로 분류하여 보안자재에 준하여 취급·관리하여야 한다.

제74조(암호자재 수령 및 배포) ① 암호자재를 수령받은 보안담당관은 수령기관용 암호자재관리기록부(시행규칙 별지 제3호서식)에 기록·관리하여야 한다.

② 수령받은 암호자재를 그 각 부서 및 소속기관에 배부할 때에는 배부기관용 암호자재관리기록부(시행규칙 별지 제3호서식)에 기록하고, 암호자재증명서(시행규칙 별지 제2호서식) 2부를 작성하여 늦어도 사용기간 3일전에 해당 부서에 도착되도록 배부하여야 하며, 암호자재증명서 1부는 수령부서에

서, 1부는 배부부서에서 보관하며 이면증명란에 따라 수수 증명한다.
③ 암호자재 사용기관의 범위는 서울특별시장이 지정한다.
④ 사용기간이 만료된 암호자재는 암호자재증명서에 따라 지체 없이 서울특별시 보안담당관에게 반납한다.
⑤ 암호자재는 취급자의 접촉에 의하여 튼튼한 용기에 담아 수발한다.

제75조(암호자재의 보관관리) ① 보안자재를 수령받은 보안담당관은 규정 제22조제1항에 따라 암호자재기록부에 기록·관리한다.
② 암호자재는 비밀캐비닛 내에 별도의 자재함을 비치하여 보관하여야 하며, 현재용, 과거용, 미래용으로 구분하되, 자재 외의 물건과 함께 보관하여서는 아니 된다.
③ 암호자재는 Ⅲ급 비밀취급 인가를 받은 사람은 누구나 취급할 수 있으며, 암호자재의 복제·복사는 불허한다.
④ 보관책임자는 암호자재를 주 1회 이상 점검하고, 보안담당관은 월1회 이상 보관책임자의 점검사항을 확인하여야 한다.

제76조(음어문의 관리) ① 전언통신 또는 그 밖의 통신수단에 의하여 수령받은 음어문은 이를 평문화하여 비밀문서인 경우에는 비밀관리기록부에 등재·관리하여야 한다.
② 음어문은 해독한 후 평문과 동시에 보관하여서는 아니 되며, 즉시 파기하여야 한다.
③ 음어문의 작성은 2개 종류의 음어표를 혼합하여 사용하여서는 아니 된다.
④ 음어문을 해독 또는 작성하기 위하여 사용된 작업지, 그 밖의 사용된 용지 등은 보안담당관 또는 보관책임자 입회하에 파기하여야 한다.

제6장 시설보안

제77조(업무담당) ① 시설보안에 관한 일반적 업무는 보안담당관의 조정을 받아 각 기관 시설관리 책임부서가 이를 수행한다. 다만, 보호구역의 운용에 대해서는 구역책임자가 이를 수행한다.

② 시설관리책임자는 보안담당관이 정하는 시설보안에 관한 기본지침을 이행하여야 한다. 시설의 변경(개축・증축・보수)등 보안관리상의 변경을 하고자 할 때에는 사전에 보안담당관과 협의하여야 하며 특히 시설의 고장, 파손 또는 이에 대한 보수공사는 사전에 보안담당관에 통보하여야 한다.

③ 제2항의 협의에 있어 보안담당관은 필요하다고 인정할 때에는 위원회의 심의에 부의할 수 있다.

제78조(보호구역 설정) ① 규정 제32조에 따른 통제 및 제한구역은 다음과 같이 설정한다.

1. 통제구역

가. 지하종합상황실(전시 또는 훈련기간에 한한다)

나. 정보통신실(주요정보화자료 및 정보통신장비 설치 장소에 한한다)

다. 기타 보안상 특별한 통제가 요구되는 지역 또는 시설

2. 제한구역: 방송실, 기관실, 전기실, 통합관제센터, 지하종합상황실 및 정보통신실

② 제1항 각 호에 정하지 아니한 보호구역의 추가 설정이 필요한 경우에는 시행규칙 제53조 및 제55조와 제1항을 준용하여 구청장이 정한다.

③ 보안담당관(분임보안담당관)은 별지 제12호 서식의 보호구역대장을 비치하여야 한다.

④ 제한구역 및 통제구역에는 중앙 또는 잘 보이는 곳에 보호구역표지 (별지 제13호 서식)를 부착하여야 한다. 다만, 보안상 표시하지 않는 것이 타당할 경우에는 부착하지 아니할 수 있다.

제79조(보호구역 운영방침) ① 보호구역은 시행규칙 제54조에 따라 필요한 보안대책을 마련하여야 한다.

② 보호구역 중 통제구역에는 출입인가자 명단을 그 구역내부에 게시하되 가림막을 쳐야 한다.

③ 보호구역 중 제한구역 및 통제구역에는 별지 제14호서식의 출입자명부를 비치하고 고정출입자 이외의 자의 출입상황을 기록・유지하여야 한다.

④ 보안담당관(분임보안담당관 포함)은 보호구역에 대한 자체점검을 수시 실시하여야 한다.

제80조(주·야 경계 및 순찰) ① 주간에는 방호원, 청원경찰 및 감독자에 의해 시간마다 순찰을 실시하며, 야간 및 토요일·공휴일에는 당직사령 책임하에 당직근무자, 방호원, 청원경찰 등이 주기적으로 순찰근무를 실시하여야 한다.

② 구청장은 순찰함을 주요지점(취약지점)에 비치하고 야간순찰 시 순찰점검 기기 등을 활용하여 순찰한다.

③ 구청장은 사전지시 및 현지 근무상태를 점검하기 위한 감독반을 편성하여 다음 각 호의 사항을 수시로 점검하여야 한다.

1. 야간근무자의 근무상태
2. 초소근무자의 근무상태
3. 비상대기 상태
4. 순찰지역 적정여부 및 순찰근무 상태
5. 보안 및 방화점검 실시 상태
6. 비상대기차량의 확보 및 유지상태
7. 근무수칙의 숙지여부

제81조(자체 방호계획 수립·운영) ① 구청장은 비상시를 대비하여 인명과 재산을 보호하고 국가보안의 유지를 위하여 자체 실정에 맞는 방호계획을 수립·운영하여야 한다.

② 제1항에 따른 자체 방호계획에는 청사 출입보안대책을 반드시 포함하여야 한다.

③ 제1항의 자체 방호계획에는 청사를 개방구역(민원실, 주민개방시설 등)과 신분확인 등 출입관리가 요구되는 업무구역을 분리하여 출입보안을 강화하는 사항과 방문객 출입통로 제한, 방문증(출입증 등) 교부, 취약지역 방호강화 등에 관한 세부사항이 포함되어야 한다.

제82조(방화시설 및 방화훈련) ① 구청장은 소방기본법에 따른 방화기구를 비치하고 화재로 인한 시설물보호를 위하여 연 2회 이상 정기방화훈련 및 소방교육을 실시하여야 한다.

② 구청장은 방화 등 재해로 인한 시설물 및 장비 등의 피해를 미연에 방지하기 위하여 인화물질 저장소 및 전기누전 사항 등을 수시로 점검하여야 한

다.

③ 구청장은 자체방화계획을 수립·시행하여야 한다.

제7장 보안조사

제83조(보안사고의 처리) ① 보안사고를 발견한 사람 또는 이를 인지한 사람은 즉시 보안담당관과 행정자치부장관 등에 보고하여야 한다.

② 보안사고 보고사항은 다음 각 호와 같다.

1. 일시, 장소
2. 사고자 인적사항
3. 사고내용(육하원칙에 따라)
4. 조치사항

③ 보안시스템, 보안자재 사고 시에는 시행규칙 제8조제1항 각 호에서 정하는 바에 따라 조치하여야 한다.

④ 비밀이 누설 또는 분실 되었을 때에는 그 비밀의 발행기관 및 배포기관에도 통보하여야 한다.

⑤ 보안사고의 내용은 발생 경위 및 이에 대한 전말조사가 종결될 때까지 공개하여서는 아니 된다.

제84조(보안사고 관계자 및 보고 불이행에 대한 조치) 보안사고가 발생하였을 때는 사고를 범하였거나 이를 인지하였음에도 불구하고 소정의 보고 조치를 이행하지 않았거나 보안사고를 은닉한 사람은 물론 보안사고 관계자와 직근 상급자에게 관계 법규에 따라 조치하고 그 처리 결과를 국가정보원장에게 통보한다.

제85조(자체보안감사의 실시) ① 구청장은 보안담당관으로 하여금 보안업무의 감독 및 비밀의 관리실태를 조사하기 위하여 구 본청 및 산하기관을 연 1회 이상 정기보안감사를 실시할 수 있다.

② 보안담당관이 보안감사를 실시할 경우 감사반은 분야별 보안업무담당 직원으로 편성한다.

③ 구청장은 제1항 및 제2항을 준용하여 해당 기관 및 산하기관에 대하여

보안감사를 실시하고 그 결과를 시 보안담당관에게 통보하여야 한다.

제86조(감사결과 조치) 국가정보원, 행정자치부의 지도점검 및 자체감사 결과 중대한 위반 사실이 지적되었을 때에는 관계 공무원과 직근 상급자 및 감독직에 있는 공무원에게는 관계 법규에 따라 필요한 조치를 취하여야 한다.

제87조(자체보안진단) ① 보안담당관은 보안진단의 날(매월 세번째 수요일)을 지정 자체보안진단을 실시하여야 한다.

② 자체보안진단 실시는 다음 사항에 유의하여 세부사항은 보안담당관이 수시로 정하되 지적사항은 즉시 시정조치 하여야 한다.

1. 부서별 현재원과 비밀취급 인가자의 현황 파악
2. 소유비밀의 일체정리와 현황 파악
3. 외래인 출입통제의 강화
4. 청사경비·방호요원에 대한 교육훈련
5. 분야별 보안관리실태 진단
6. 직무교육 실시
7. 개별업무 중 문제점 발견과 개선 대책

제88조(보안 및 방화점검부 활용) 보안담당관은 부서별로 보안 및 방화점검부(별지 제15호서식)를 비치(다만, 전자경비시스템으로 보안점검을 할 수 있다)하여 다음과 같이 활용하게 한다.

1. 보안 및 방화점검부는 각 부서의 최종 퇴청자가 항목별 점검을 실시하고 기록하여 다음 날 부서의 장에게 보고한다.
2. 일과시간 이후에는 당직사령 책임하에 당직근무자가 각 부서를 순회 점검하여 이상 유무를 확인 기록한다.

제8장 기타 보안관리

제89조(설계도서의 관리) ① 보안성이 요구되는 설계도서는 작성·접수되는 순서에 따라 관리번호를 부여하고 설계도서관리대장(별지 제16호 서식)에 등재 관리하여야 하며, 대외유출 통제를 위해 일반문서와 분리하여 별도 지

정된 캐비넷 또는 보관함에 일괄 보관한다.

② 설계도서를 시공업자에게 배부할 때에는 공사감독관으로 하여금 보관책임자를 지정하게 하고 보관관리에 필요한 모든 보안조치를 취한 후 배부하여야 하며 시공업자에 배부된 설계도서는 공사완료와 동시에 발행부서에서 반드시 전량 회수하여야 한다.

③ 설계도서를 접수한 기관이 설계도서를 복제·복사한 때에는 설계도서 말미의 적당한 여백에 시행규칙 제43조에 정한 사본 근거를 표시하여야 한다.

④ 시공업자에 배부된 설계도서는 복제·복사할 수 없다. 다만, 필요할 때에는 발행부서에 복제·복사를 요청하여야 한다.

⑤ 설계도서의 보관이 불필요하다고 인정할 때에는 폐기 또는 발행부서에 반납하여야 하며, 폐기 또는 반납하였을 때에는 설계도서관리대장에 폐기(반납)일자 및 폐기(반납) 확인을 보안담당관 또는 분임보안담당관에게 받아야 한다.

제90조(보안목표시설 등 주요시설 신축·증축 보안대책) ① 주요건설 사업은 계획수립 시 사전에 국가안보 상황을 고려한 보안대책을 마련하여 위원회의 심의를 거친 후 이를 설계서에 반영 하여야 한다.

② 제1항의 보안대책 마련에는 최소한 다음 사항이 고려되어야 하며 그 결과는 사업계획서 및 설계서에 명시되어야 한다.

1. 보안방호 시설
   가. 입지선정 또는 지형 조건
   나. 방호시설(내·외곽 포함) 계획
   다. 방호(경비)활동 대책
   라. 기타 시설방호상 필요한 대책
2. 정보통신방호 시설
3. 군작 전 및 전략계획 기타 국가보안상에 미치는 영향
4.「군사기지 및 군사시설 보호법」 및 기타 관계 법규에 저촉 여부
5. 기 건설된 시설과의 관련성 및 조정
6. 관계부서간 문제점 사전 협의 조정

제91조(보안목표시설 관리) ① 보안목표시설 또는 보안목표시설로 지정 예정

인 중요 시설 신축·증축 시에는 규정 제35조부터 제37조까지의 소요 보안대책을 마련하고 시 보안담당관을 경유 국가정보원장에게 보안측정을 요청하여야 한다.

② 보안목표시설 이외의 중요시설에 대해서도 필요시에는 국가정보원에 보안측정을 요청할 수 있다.

제92조(비밀관리부철의 보존) ① 다음 각 호의 부철은 5년간 보존하여야 하며 그 이전에 파기하고자 할 때에는 국가정보원장의 승인을 얻어야 한다.

1. 비밀관리기록부
2. 비밀문서 접수·발송부
3. 비밀열람기록전(철)
4. 비밀 입력·출력 및 작업대장
5. 암호자재(장비) 관리기록부
6. 서약서철

② 다음 각 호의 대장과 문건은 2년간 보존하여야 한다.

1. 보안담당관 인계인수서
2. 그 밖의 보안관련대장

제9장 공간정보보안

제93조(공간정보 보안업무) ① 보안담당관이 수행하여야 할 공간정보 보안업무는 다음 각 호와 같다.

1. 공간정보 보안업무의 계획수립 및 시행
2. 공간정보의 생산·구축·관리·유통 및 활용에 따른 보안대책 마련
3. 공간정보의 보안관리를 위한 지도·점검·감사 및 교육
4. 기타 공간정보 관련 보안업무

② 보안담당관은 공간정보의 보안업무에 관하여 소속기관 분임보안담당관을 지휘·감독한다.

제94조(공간정보의 분류) ① 구청장은 생산 공간정보를 별표 2의 분류기준에 따라 비공개, 공개제한 또는 공개로 분류하여 관리하여야 한다.

② 비공개 또는 공개제한 공간정보가 비공개 또는 공개제한의 필요성이 없어진 경우에는 이를 재분류하여야 한다.

③ 제1항에 따른 분류기준에 따라 자체실정에 맞는 세부분류기준을 정할 수 있다.

제95조(비공개 또는 공개제한 공간정보의 취급) ① 비공개 또는 공개제한 공간정보는 그 공간정보와 업무상 관련이 있는 사람에 한정하여 취급할 수 있다.

② 비공개 공간정보는 적정등급의 비밀 또는 대외비로 분류·관리하여야 한다.

③ 공간정보 관련 업무를 하는 부서에서는 비공개 또는 공개제한 공간정보의 누설·유출 등을 방지하기 위하여 보관책임자를 다음 각 호와 같이 지정한다.

1. 보관책임자 정 : 관리부서의 장
2. 보관책임자 부 : 관리부서의 담당팀장 또는 그에 상응한 담당직원

제96조(공간정보 데이터베이스의 보호) ① 공간정보 데이터베이스의 훼손·파괴·유출 등을 방지하기 위한 보호대책은 다음 각 호와 같다.

1. 관리부서별 보안관리책임자 지정(관리부서의 장으로 한다)
2. 출입문 카드키 등 시건장치 설치로 외부인 침입 방지
3. 데이터베이스 복제(복사)본을 확보하여 철제용기 등에 별도 보관하고 관리대장(별지 제19호서식)에 기록·유지
4. 공간정보 데이터베이스에 대한 접근 차단대책 강구
   가. 부서 및 사용자별 ID·비밀번호 부여, 자료유형별 접근권한 제한
   나. 작업범위는 소관업무에 따라 열람·출력·갱신 등으로 제한
   다. 열람은 필요내용에 따라 기본항목·전항목 등으로 구분
   라. 공간정보 취급자 이외에 업무상 필요에 의하여 비공개 또는 공개제한 공간정보 데이터베이스를 이용하고자 하는 자는 보안관리책임자의 사전 허가 후 접근
5. 비공개 및 공개제한 공간정보 목록 작성 및 관리대장(별지 제18호서식)에 기록 유지

6. 해킹 등 불법접근 및 컴퓨터 바이러스 예방대책 강구

② 공간정보 데이터베이스는 열람·전송·출력 등 사용내역에 대한 확인이 가능하도록 전산시스템을 구축·관리하여야 한다.

제97조(공간정보유통망 관리) 공간정보유통망 관리부서의 장은 공간정보의 위·변조, 불법유출 등을 방지하기 위하여 다음 각 호의 공간정보유통망 보호대책을 수립·시행하여야 한다.

1. 공간정보유통관리망 보안담당자 지정(관리부서의 장으로 한다)
2. 방화벽 등 침입방지 및 감시시스템 설치·운용
3. 인터넷 등 외부망과 분리 설치 및 해킹, 컴퓨터바이러스 예방대책 강구
4. 공간정보 유통망에 대해서는 월 1회 이상 점검·확인

제98조(공개제한 공간정보의 활용) ① 구청장은 소관 공개제한 공간정보에 대하여 학술연구 등의 목적으로 공개를 요청받은 경우에는 다음 각 호의 사항을 확인·검토하여 제공할 수 있다.

1. 신청인의 인적사항(성명, 주소, 생년월일, 소속기관·단체 및 직책 등)
2. 사용목적 및 타당성
3. 활용 후 관리대책

② 제1항에 따라 공개제한 공간정보를 제공한 때에는 보안담당관은 제공일시, 자료의 내용 및 방법 등 관련 사항을 별지 제20호 서식에 기록·유지한다. 다만, 도로굴착·건축협의 등 단순 도면형태의 자료를 출력·제공한 때에는 관리부서의 장이 기록·유지한다.

제99조(비공개 또는 공개제한 공간정보의 공개) ① 구청장은 보유·관리하고 있는 비공개 또는 공개제한 공간정보를 일반에 공개하여서는 아니 된다.

② 구청장은 보유·관리하고 있는 비공개 또는 공개제한 공간정보를 일반에 공개할 필요성이 있는 경우 공개할 자료의 내용과 공개목적·시기 및 방법 등에 대하여 위원회의 심의를 거쳐 행정자치부 장관의 승인을 받아야 한다.

제100조(비공개 또는 공개제한 공간정보의 복제 등 제한) ① 비공개 또는 공

개가 제한되는 공간정보는 다음 각 호의 경우를 제외하고는 이를 복제·복사 또는 출력할 수 없다.

1.「국가공간정보 기본법 시행령」제25조에 따라 복제·관리하는 경우

2. 비공개 공간정보로서 구청장의 허가를 받은 때

3. 공개제한 공간정보로서 보안담당관의 허가를 받은 때(다만, 도로굴착·건축협의 등 단순 도면형태의 자료를 출력한 때에는 관리부서의 장의 허가를 받은 때)

② 비공개 또는 공개제한 공간정보는 그 비밀(대외비) 표지 또는 예고문 상단에 다음과 같이 적색으로 기입하여 관리하여야 한다.

이 자료는 관리책임자의 허가 없이 복제 · 복사 · 출력할 수 없음

③ 비공개 또는 공개제한 공간정보를 복제·복사 또는 출력한 때에는 그 원본과 동일하게 분류하여야 하며, 대외비 이상으로 관리되는 경우에는 사본 번호를 부여하고 예고문을 명시하여야 한다.

④ 비공개 또는 공개제한 공간정보를 복제시에는 공개 공간정보와 구분하여 별도의 저장매체에 저장한다.

⑤ 공간정보를 복제·복사 또는 출력한 때에는 별지 제20호서식의 공간 정보 자료 복제·출력대장에 기록을 유지한다.

제101조(공간정보의 국외반출 금지) ① 비공개 또는 공개제한 공간정보는 다음 각 호의 경우를 제외하고는 국외로 반출할 수 없다.

1. 외국정부와 체결된 협정 또는 합의에 의하여 상호교환하는 경우

2. 구를 대표하여 국제회의 또는 국제기구에 참석하는 자가 자료로 사용하기 위하여 반출하는 경우

② 제1항에 따라 공간정보를 국외로 반출하고자 하는 자는 구청장의 승인을 받아야 한다.

제102조(공간정보의 외주용역) ① 관리부서의 장은 비공개 또는 공개제한 공간정보의 생산·구축·관리·유통 및 활용 등을 위하여 외주용역을 하고자 하는 때에는 미리 보안담당관의 승인을 받아야 한다.

② 제1항에 따라 외주용역을 하는 경우 관리부서의 장은 보안책임자를 지정하여 용역업체에 대한 보안관리 실태를 파악하고, 대책을 마련하여야 한다.

1. 계약서에 공간정보 보호의무와 위반 시 조치사항 명시
2. 참여인원에 대한 신원확인, 서약집행 및 보안교육
3. 작업장소를 통제구역 또는 제한구역으로 설정
4. 용역종료 시 성과물과 제공된 각종 자료 회수
5. 기타 보안관리에 필요한 사항

③ 민간시설을 이용하여 비공개 공간정보를 제작하거나 인쇄·발간 또 는 복제·복사하고자 하는 때에는 시행규칙 제45조에 따른 비밀취급 특례업체를 이용하여야 하며, 시행규칙 제46조에 따라 필요한 보안조치를 취하여야 한다.

제103조(공간정보 종사 외국인 보안관리) ① 구청장은 외국인을 공간정보 관련 업무에 종사하게 하고자 하는 때에는 다음 각 호의 보안대책을 마련하여야 한다.

1. 신원확인, 신원대장 작성유지 및 보안교육·서약집행
2. 계약서에 기밀누설·유출시 해고 및 손해배상책임 명시
3. 비공개 등 중요 공간정보 취급 및 핵심시설 출입금지

② 구청장은 외국인의 특이동향 등 보안관리에 위해(危害)로운 사실을 발견한 경우에는 우선 공간정보에 대한 보호조치를 하고, 서울특별시장 및 국가정보원장에게 관련 사항을 즉시 통보하여야 한다.

제104조(공간정보 보안사고) ① 구청장은 다음 각 호의 보안사고가 발생한 때에는 사고일시 및 장소, 사고자 인적사항, 사고내용 및 경위, 조치사항 등을 지체 없이 국가정보원장 및 행정자치부장관에게 통보하여야 한다.

1. 비공개 또는 공개제한 공간정보의 누설·유출·침해·훼손·분실
2. 공간정보 데이터베이스의 침해·훼손·무단이용
3. 국가공간정보 기본법 제38조에 따른 비밀준수의무 위반행위
4. 공간정보유통망 또는 보호구역에 대한 불법 침입
5. 그 밖의 공간정보에 대한 중대한 침해 행위

② 구청장은 제1항 각 호의 보안사고가 발생한 때에는 이를 바로 서울특별시장에게 보고하여야 한다.

③ 구청장은 국가정보원 등으로부터 보안사고 조사를 받는 경우 필요한 자

료를 제공하는 등 성실히 협조하여야 하며, 조사가 종결될 때까지 이를 공개하여서는 아니된다.

④ 구청장은 보안사고 조사결과에 따라 관련자를 문책하고, 재발방지를 위한 대책을 마련하여 국가정보원장 및 행정자치부장관에게 통보하여야 한다.

제10장 보 칙

제105조(준용) 이 규칙에 명시되지 않은 사항은 다음 각 호의 관련규정·지침에 따른다.

1. 보안업무규정(대통령령)
2. 보안업무규정 시행규칙(대통령훈령)
3. 보안업무규정 시행 세부규칙(행정자치부훈령)
4. 국가사이버안전관리규정(대통령훈령)
5. 국가 정보보안 기본지침(국가정보원)
6. 서울특별시 보안업무 처리규칙
7. 서울특별시 정보통신 보안업무 처리규칙
8. 서울특별시 공간정보 보안업무 처리규칙
9. 그 밖의 정보통신보안 관련 법령 및 지침

부칙

이 규정은 발령한 날부터 시행한다.

〔별표 1〕

공간정보 안전반출 및 파기계획(제47조 관련)

1. 목적

이 계획은 전시사변, 폭동, 천재지변, 화재 또는 이에 준하는 비상사태 발생 시 서대문구가 보관·관리 및 활용하고 있는 비공개 및 공개제한 공간정보를 안전하게 반출 또는 파기함으로써 비공개 및 공개제한 공간정보의 안전한 관리를 도모함을 목적으로 한다.

2. 적용범위

서대문구가 생산·관리 및 활용하고 있는 공간정보

3. 지출 또는 파기의 시기

가. 전쟁, 사변 또는 폭동의 발발로 인하여 공간정보 등을 현 보관 장소에 안전하게 보관할 수 없게 되었을 때

나. 천재지변, 화재 등으로 공간정보 등이 누설, 전파, 분실, 도난, 손실 또는 파괴될 우려가 있을 때

다. 적, 무장공비, 폭도, 그 밖의 불순분자의 포위공격 또는 침투로 공간정보 등을 탈취당할 우려가 있을 때

라. 그 밖의 현 보관 장소에 계속 보관할 수 없는 불가피한 또는 긴박한 상황이 발생하였을 때

4. 반출 또는 파기의 절차 및 장소 등

가. 일과 중일 때의 반출절차

1) 상황파악 및 반출명령

보안담당관은 제3호에 따른 지출시기임이 파악되었을 때에는 즉시 구청장의 지출명령을 받아 보안관리책임자에게 비공개 및 공개제한 공간정보에 대한 지출을 명한다.

2) 보안관리책임자의 반출조치

가) 공간정보 등 지출요원 소집 및 인출지시

지출요원은 보안관리 부책임자 및 그 소속직원이 된다.

나) 공간정보 등의 보관용기 개방과 인출작업

지출요원은 보관용기를 개방하여 공간정보 등을 인출한 후 이를 비상 반출낭에 넣어 반출준비를 완료한다.

다) 반출

반출요원은 승강기 또는 비상계단을 통하여 공간정보 등을 지출장소까지 가장 신속하고 안전한 방법으로 반출한다.

라) 반출시 호위

반출시 호위는 각 지출요원 또는 지명 받은 보조요원이 행한다.

나. 일과 후 및 공휴일의 반출절차

1) 상황파악 및 지출명령

당직책임자는 제3호에 따른 반출시기임이 파악되었을 때에는 즉각 보안담당관에게 보고한 후 보안담당관의 명에 따라 비밀 등에 대한 지출을 명한다.

2) 비상소집 조치(예비군 포함)

당직책임자는 판단된 상황에 따라 전 직원 또는 예비군에 대한 비상소집 조치를 취한다.

3) 반출조치

가) 안전함 개방, 보관용기 열쇠 및 다이얼번호 등 확인

당직책임자는 당직실에 보관되어 있는 안전함을 열어 각 부서 보관용기 열쇠 및 다이얼번호를 확인한다.

나) 인출조 편성 및 인출지시

당직책임자는 당직자(수위 포함)로 구성된 인원으로 각 부서별로 분담한 인출조를 편성하여 해당되는 열쇠와 다이얼 번호를 인계하여 인출토록 지시한다.

다) 인출조의 인출작업

분담 받은 해당 부서의 공간정보 등 보관용기를 개방하여 공간정보 등을 인출한 후 이를 비상 반출낭에 넣어 반출준비를 완료한다.

라) 반출

인출 또는 인출준비 완료와 동시에 비상계단을 통하여 공간정보 등을 지출 장소까지 가장 신속하고도 안전한 방법으로 반출한다.

마) 반출시 호위

반출시의 호위는 우선 확보된 인출조원이 이를 하되, 비상소집 되어 도착된 예비군 또는 직원이 이를 호위한다.

다. 지출장소

1) 상황에 따라 보안담당관은 안전지출 장소를 변경할 수 있다.

2) 지출장소는 보안담당관이 이를 작성하여 안전함 내부에 비치한다.

라. 파기절차 및 장소

1) 적, 무장공비, 폭도, 그 밖의 불순분자의 포위공격 또는 침투로 인하여 공간정보 등의 안전지출이 도저히 불가능하거나 공간정보 등을 탈취당할 긴박한 상태가 야기되었을 때는 긴급 파기할 수 있다.

2) 파기절차는 지출절차 제4호 가, 나에 준하여 시행하고 파기장소는 원칙적으로 소각장으로 하되, 상황의 진척에 따라 보안담당관의 판단에 따라 별도의 장소를 지정할 수 있도록 한다.

〔별표 2〕

등급별 공간정보의 분류기준(제93조 관련)

등급	분 류 기 준	
비 공 개	기준	◦ 공개될 경우 국가안보에 유해로운 결과를 초래할 우려가 있는 정보 ◦ 법령에 따라 비공개 사항으로 규정된 공간정보
	사례	〈항공사진〉 ◦ 일반인 출입이 통제되는 국가보안시설 및 군사시설(휴전선 접경지역내 시설 포함)이 노출된 사진 및 영상, 3차원 입체자료 〈위성영상〉 ◦ 일반인 출입이 통제되는 국가보안시설 및 군사시설(휴전선 접경지역내 시설 포함)이 노출된 3차원 위성자료 〈수치지도〉 ◦ 축척에 관계없이 일반인 출입이 통제되는 국가보안시설 및 군사시설(휴전선 접경지역내 시설 포함)이 포함된 지도 〈해저영상물〉 ◦좌표가 표기되어 있고 10m 이상 정밀한 3차원 해저 영상자료 ◦좌표가 표기되어 있고 30m 이상 정밀하고 국가보안시설(항만, 군사시설, 중요시설 등)이 노출된 3차원 해저 영상자료 〈그 밖의 공간정보〉 ◦ 일반인 출입이 통제되는 국가보안시설 및 군사시설이 노출된 3차원 공간정보 ◦ 일반인 출입이 통제되는 국가보안시설 및 군사시설의 명칭 및 속성자료
공 개 제 한	기준	◦ 공개될 경우 공공의 안전과 이익을 해할 우려가 있다고 인정되는 공간정보 ◦ 공개될 경우 개인정보를 침해할 우려가 있는 공간정보 ◦ 공개될 경우 관리기관의 업무수행에 지장을 초래한다고 인정되는 공간정보
	사례	〈항공사진〉 ◦ 일반인 출입이 통제되는 국가보안시설 및 군사시설이 삭제된 흔적이 남아있는 사진 및 영상, 3차원 입체자료 ◦ 2차원 좌표(緯·經度)가 포함된 해상도 30m 초과 자료 ◦ 3차원 좌표(緯·經·高度)가 포함된 해상도 90m 초과 자료 〈위성영상〉 ◦ 정밀보정된 2차원 좌표가 포함된 해상도 30m 초과 자료 ◦ 일반인 출입이 통제되는 국가보안시설과 군사시설이 노출된 해상도 4m 초과 자료 ◦ 3차원 좌표가 포함된 해상도 90m 초과 자료 〈수치지도〉 ◦ 군사 지도 ◦ 전력·통신·가스 등 공공의 이익 및 안전과 밀접한 관계가 있는 국가기간시설이 포함된 지도

등급	분 류 기 준	
공 개 제 한	사례	〈수치지도(계속)〉 ◦ 국가공간정보정책 기본계획에 따른 7대 지하시설물도 ◦ 아래의 시설물이 표기된 수치지도 - 전력 : 발전소, 변전소, 지상송전선, 송전탑 - 상수도 : 저수탑, 취수탑, 급수탑, 수문, 댐, 지상상수관, 지상용수관, 양배수장경계, 양배수장 기호 - 가스관 : 지상가스관 - 송유관 : 지상송유관, 저장소 - 그 밖의 관 : 기타 수송관 - 맨홀 : 공동구맨홀, 송유맨홀, 가스맨홀, 전기맨홀, 통신맨홀, 전화맨홀, 기타 맨홀(지형코드상의 기능이 미확인된 특정한 맨홀) - 특정건물 : 교도소, 구치소, 가스공사지사 등 통제기능을 가진 지사 및 공급관리소 〈해저영상물〉 ◦좌표가 표기되어 있고 90m 보다 정밀한 3차원 해저 영상자료 ◦좌표가 표기되어 있고 150m 보다 정밀하며 국가보안시설(항만, 군사시설 등)이 노출된 3차원 해저 영상자료 ◦좌표가 없고 4m 이상 정밀한 3차원 해저 영상자료 ◦좌표가 없고 30m 이상 정밀하며 국가보안시설(항만, 군사시설 등)이 노출된 3차원 해저 영상자료 〈영해기점도〉 ◦영해기점자료 및 영해기점도 〈국가해양기본지리정보〉 ◦축척 1:250,000보다 대축척의 국가해양기본지리정보도 〈그 밖의 공간정보〉 ◦공공의 이익 및 안전과 밀접한 관계가 있는 국가기간시설의 명칭 및 속성자료 ◦격자간격이 90m 보다 정밀한 3차원 공간정보중 3차원 좌표가 포함된 자료
공 개	기준	◦비공개 및 공개제한 공간정보 외의 공간정보로서 불특정인을 대상으로 공개 또는 제공되는 공간정보
	사례	〈항공사진〉 ◦“비공개” 및 “공개제한” 대상 이외의 항공사진 및 영상, 3차원 입체자료 (인터넷·내비게이션·휴대폰에는 좌표 표시 불가) ◦해상도 50cm급 초과 항공사진은 건물·토지 소유자, 「국가공간정보 기본법」 제2조제4호의 관리기관 및 관리기관의 장이 승인한 경우에 한정하여 제공 또는 판매하고, 인적사항 및 사진 내용을 기록·유지하여야 한다. ※ 다만, 국가정보원장이 별도 통보한 지역의 해상도 25~50cm급 항공사진을 일반인에게 제공 또는 판매시 기록·유지를 생략할 수 있다. 〈위성영상〉 ◦“비공개” 및 “공개제한” 대상 이외의 위성영상 및 3차원 위성자료

등급	분 류 기 준	
공 개	사례	◦촬영 당시 위성자세정보가 포함된 일반지역 자료(인터넷·내비게이션·휴대폰에는 좌표 표시 불가) ※ 다만, 해상도 50cm급 초과 위성영상 제공 또는 판매시 인적사항 및 사진내용 기록·유지 〈수치지도〉 ◦“비공개” 및 “공개제한” 대상 이외의 지도(인터넷·내비게이션·휴대폰에는 좌표 표시 불가) ※ 다만, 1/1,000 이상 수치지도를 일반에 제공시에는 인적사항 기록·유지 〈해저영상물〉 ◦“비공개” 및 “공개제한” 대상 이외의 3차원 해저 영상자료로서 좌표가 표시되지 않은 자료 〈국가해양기본지리정보〉 ◦“공개제한” 대상 이외의 국가해양기본지리정보도(인터넷·내비게이션·휴대폰에는 좌표 표시 불가) ※ 다만, “수치지도”의 “비공개”, “공개제한” 등급기준을 적용하며 해저지형은 격자수심으로 처리 〈지적공부〉 ◦지적도, 임야도, 토지대장, 임야대장, 경계점 좌표등록부, 공유지 연명부, 대지권 등록부 〈그 밖의 공간정보〉 ◦좌표가 없는 일반지역 3차원 영상자료 ◦3차원 좌표가 포함된 격자간격 90m 이상 입체 영상자료 ※ 토양·지질도, 도시계획도, 도로건설계획도, 지번도, 전자해도 등 ◦“비공개” 및 “공개제한”이 아닌 공간정보

* 국가보안시설과 군사시설은 각각 국가정보원과 국방부가 정하는 바에 따름

[별지 제1호서식]

퇴직자 보안 서약서

본인은 년 월 일자로 퇴직함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 ○ ○ ○ ○ 근무 중 업무와 관련하여 알게 된 기밀은 국가안전보장에 관한 기밀임을 인정한다.

2. 본인은 퇴직 후에 알게 된 제반 기밀사항을 일체 누설하지 않을 것을 서약한다.

3. 본인이 이 기밀을 누설한 때에는 동기여하를 막론하고 엄중한 처벌을 받을 것을 서약한다.

20 년 월 일

서 약 자 소속 직 성명 (인)

서약집행관 소속 직 성명 (인)

[별지 제2호서식]

비 밀 취 급 인 가 대 장

발행 번호	결재		취급 등급	사진	소속	직위	직급	성명	인가 년월일	해제 년월일	발생사유	비고
	담당	팀·과장										

[별지 제3호서식]

신 원 대 장

연 번 (1)	직 급 (2)	직 책 (3)	성 명 (4)	신 원 조 사				임용또는 전입일자 (9)	비 고 (10)
				목 적 (5)	의뢰일자 (6)	회부일자 (7)	내 용 (8)		

[별지 제4호서식]

서 약 서

본인은 서대문구 ○○○의 직무를 성실히 수행하며, 본인의 잘못으로 발생하는 문제에 대해서는 그 책임을 다하기로 하면서 다음과 같이 서약합니다.

1. 근무 중에 알게 된 기밀사항은 계약기간 중은 물론, 계약만료 후에도 외부에 일체 누설하지 않는다.
2. 직무 관련 법령을 준수하고 감독공무원의 직무상 명령에 따른다.
3. 출 · 퇴근시간 및 서대문구의 모든 근무수칙을 준수한다.
4. 업무와 관련된 자료를 부당하게 유출하지 않는다.
5. 업무 수행 중 특이한 사항이 있을 때에는 즉시 감독공무원에게 보고하고 지시에 따른다.
6. 상급자가 공정한 직무 수행을 현저하게 해치는 부당한 지시를 하였을 때 거부할 권리가 있으며, 이를 차상급자에게 보고한다.

20 . . .

서약자: (인)

서대문구청장 귀하

[별지 제5호서식]

비밀 입·출력 및 작업대장

[대상: , 관리번호:]

일자	제 목	비밀 등급	건수 (매수)	작업 구분	작업자	열람 또는 수령자			비고
						소속	성명	서명	

○ 대상에는 하드디스크, 디스켓, CD 등 구분

○ 작업구분은 입력, 출력, 열람으로 구분

○ 비고란에는 비밀을 지속 보관하고자 할 경우 관리책임자의 승인 서명 구분

○ 기록은 대상별, 비밀등급별로 구분 작업

[별지 제6호서식]

기 관 명

분류기호 20 . . .

수 신 발신 ㊞

참 조

비밀(대외비)문서발간신청서

발간장소	업체 및 대표자명			비밀취급 인가등급		
	주 소			인가근거		
가제목				문서비밀 등급		
부 수		사정부수		구 분	타자, 프린트 마스터, 인쇄	
기 간	20 . . .부터 20 . . .까지(시간)					
자체보안책						
입회관	비밀취급 인가등급	급	직 급		성명	
배부처						

[별지 제7서식]

비밀(대외비)문서 통제대장

일련번호	통제일	발신	수 신	제 목	비밀등급	사본부수	형태	입회관	인쇄처	비 고

[별지 제8호서식]

비밀문서조달의뢰확인서

제 목 또 는 가제목	비밀 등급	발간 의뢰 부수	납품 기일	조달 의뢰 일자	원고 수교 일자	프린트 공 판 인 쇄	의 뢰 업체명	입 회 관		
								인 가 등 급	직 명	성 명

상기와 같이 비밀문서 조달을 의뢰하고 입회관을 파견하였음을 확인함.

20 . .

수 요 기 관

보안관리자 직책 직명 성명 ㊞

[별지 제9호서식]

외국인에 대한 자료제공 통제대장

일련번호	통제일	외국인 인적사항					제공자료명	부수	제공처 (부서 명)	비고
		국적	직위	성명	연령	내방목적				

[별지 제10호서식]

외국공관원 접촉 신청서

결재	담당	팀장	과장

접촉대상 외국공관원	성명		성별	
	국적		소속 (전화번호)	
	국내체류지 (전화번호)			
면담일시	년 월 일 ~		면담장소	
접촉목적				

년 월 일

신청자 소속 직급 성명 (인)

[별지 제11호서식]

외국공관원 접촉결과 보고서

결재	담 당	팀 장	과 장

접촉 외국공관원	성 명		성 별	
	국 적		소 속 (전화번호)	
	국내체류지 (전화번호)			
면담일시	년 월 일 ~		면담장소	
접촉결과				

년 월 일

신청자 소속 직급 성명 (인)

※ 결과란에는 접촉 시 나눈 대화 중 주요내용을 기재하되 자료제공 요청, 특정현안에 대한 브리핑 요청, 과분한 선물·향응 제공 등 특이사항 있을 경우 그 내역을 상세히 기재

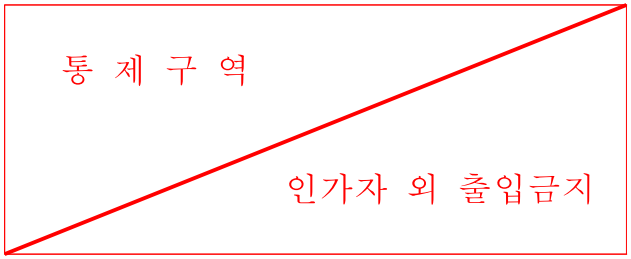
[별지 제12호서식]

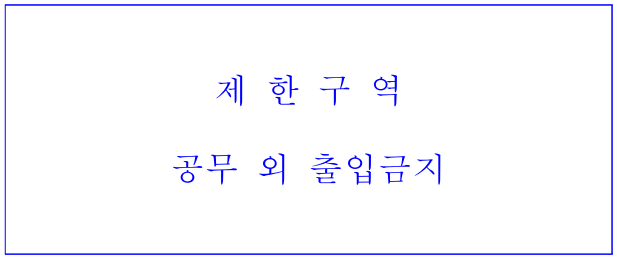
보호구역대장

구 분	장 소	관리팀·과명	사유 및 기타사항	설정 연월일	해제 연월일

[별지 제13호서식]

보 호 구 역 표 시





※ 통제구역은 백색바탕 적색글씨·적색 테 및 대각선, 제한구역은 백색바탕 청색 글씨·청색 테

※ 규격은 부착 장소에 따라 적의 조절하며, 송판·합판 또는 아크릴 등 견고한 재질 사용(종이는 불가)

[별지 제14호서식]

[제한구역 / 통제구역] 출 입 자 명 부

소 속	신분증번호	직 위	직 급	성 명	용 건	출 입 일 시	
						부 터	까 지

[별지 제15호서식]

보 안 및 방 화 점 검 부

구 분			①서류보관상태		② 청소상태		③ 소등상태		④화기단속상태		⑤문단속상태		⑥비고	점검시간 및 점검자				결 재	
월	일	요일	최 종 퇴청자	당 직 근무자	최 종 퇴청자	당 직 근무자	최 종 퇴청자	당 직 근무자	최 종 퇴청자	당 직 근무자	최 종 퇴청자	당 직 근무자		최종퇴청자		당직근무자		팀 장	과 장
														점검 시간	성 명	점검 시간	성 명		

1. 점검사항별로 이상이 있을 때에는 ×표, 이상이 없을때에는 ○표로 기재한다.
2. 점검결과 이상이 있을 때에는 비고란에 그 내용을 기재한다.

[별지 제16호서식]

설계도서관리대장

관리번호	수 발			형태	건명	사본	수량	처리담당	보관장소	반 납		폐 기	
	월일	발행처	수신처							일자	확인	일자	확인

[별지 제17호서식]

비밀자료출력(열람) 신청서

제 목	비밀 등급	자 료 (매수)	출력(열람) 목 적	열람 또는 수령자		
				소 속	성 명	생년월일

상기 비밀자료의 출력(열람)을 신청합니다.

20 년 월 일

신청자 : 직책 직급 성명 (인)

상기 비밀자료의 출력(열람)을 신청합니다.

20 년 월 일

승인관 : 직책 직급 성명 (인)

[별지 제18호서식]

공간정보 목록 관리대장

관리 번호	생산년도	공간정보 목록	자료 구분	자료형태 및 수량	보관장소	비고

* 자료구분란에는 “비공개” 또는 “공개제한”으로 기재

[별지 제19호서식]

데이터베이스 복제(복사)본 관리대장

관리 번호	제작일자	제 목	형태	관리 매체	수량 (건)	보호 기간	보관 장소	비고

* 비고란에는 보호기간 경과자료의 처리결과 기재

[별지 제20호서식]

공간정보자료 복제(복사)·출력대장

일자	제 목	자료 구분	건수 (매수)	출력자 (복제자)	사 유	열람·수령자		예고문	승인관
						소속	성명		

* 자료구분란에는 “비공개” 또는 “공개제한”으로 기재