개인정보처리 위탁업무 및
수탁업체 관리 지침

2025. 10.

양천구시설관리공단

[제 · 개정 이력서]

제·개정 번호	제·개정 페이지 및 내용	직위	작성자	제·개정 일자
1	제정	관리7급	강현선	2017. 06. 27.
2	개정(위탁관리지침 용어 및 내용수정)	관리7급	강현선	2018. 01. 29.
3	개정(위탁관리지침 내용 전반)	관리6급	유경용	2025. 10. 20.

[목 차]

제 1 장 개 요

1. 목적

「개인정보 보호법」 제26조 및 양천구시설관리공단(이하 “공단”) 「개인정보 내부관리계획」 제25조, 제26조에 따라 공단이 개인정보 처리가 수반되는 업무를 외부 업체·기관 등(이하 “수탁자”)에 위탁하는 경우 필요한 업무 처리 절차 및 기준 등에 관한 사항을 규정

2. 관련근거

가. 「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리 제한)

나. 「개인정보 보호법 시행령」 제28조(개인정보의 처리 업무 위탁 시 조치)

다. 「표준 개인정보 보호지침」 제16조(수탁자의 선정 시 고려사항), 제17조 (개인정보 보호 조치의무)

라. 「개인정보의 안전성 확보조치 기준」 제3조(안전조치의 적용 원칙)

마. 양천구시설관리공단 「개인정보 내부관리계획」 제25조, 제26조

3. 적용 범위

공단이 개인정보 처리 업무를 수탁자에게 위탁하는 경우에 관하여 다른 법령 또는 규정, 지침 등에서 특별히 정한 것을 제외하고 이 지침을 따름

4. 용어 정의

가. 위탁자

- 「개인정보 보호법」 제26조 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자, 이 지침에서는 공단을 의미

나. 수탁자

- 개인정보 처리 업무를 위탁받아 처리하는 자(외부 업체· 기관 등)

다. 정보주체

- 처리되는 해당 개인정보에 의하여 알아볼 수 있는 사람으로서, 그 정보의 주체

라. 개인정보 처리

- 「개인정보 보호법」 제2조 제2호에 따라 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 의미

제 2 장 개인정보 처리 업무 위탁 개념 및 판단

1. 개인정보 처리 업무 위탁 개념

가. 계약의 형태와 종류를 불문하고 개인정보 처리가 수반되는 업무의 전부 또는 일부를 공단이 직접 수행하지 않고 수탁자에게 위탁하는 것을 의미

나. 개인정보 처리 업무 위탁과 제3자 제공의 구분

구분	업무 위탁	제3자 제공
관련 조항	「개인정보 보호법」 제26조	「개인정보 보호법」 제17조
예시	회원관리, 주차관리 시스템 등	청렴도조사, 만족도조사 등
이전 목적	정보주체의 서비스 이용을 위해 처리	제3자의 이익, 설문조사를 위해 처리
이전 방법	위탁 사실 공개 (공단홈페이지 - 개인정보처리방침)	법에 따라 제공 목적 등 고지 (공단 홈페이지 - 업무공지)
관리·감독 의무	위탁자	제공받는 자(제3자)
손해배상책임	위탁자 및 수탁자 부담	제공받는 자(제3자) 부담

2. 개인정보 처리 업무 위탁 판단 기준

가. 수탁자에게 업무를 위탁 시, 아래의 기준에 따라 개인정보 처리 업무 위탁으로 판단되는 경우 이 지침에 따라 업무 수행

나. 판단 주체 : 혁신성과팀, 각 사업장

다. 판단 기준

기 준	예 시
공단 업무 수행을 위해 보유 중인 개인정보를 수탁자에게 제공	공단 서비스 이용, 직원 교육 위탁 운영 등
공단 업무 수행을 위해 수탁자가 직접 개인정보를 수집, 관리(생성, 이용, 저장, 파기 등)	직원 채용, 설문 조사 위탁, 기록물 파기 등
(정보화사업) 수탁자가 공단 개인정보처리시스템 DB 등에 접근하여 업무 수행 ※ 단순시스템 유지 보수도 수탁자에게 개인정보가 포함된 DB에 접근할 수 있는 권한이 부여되는 경우 개인정보처리업무 위탁임 ※ 단, 시스템의 부품만 교체하는 등 서버나 DB에 대한 접근권한이 없는 경우 개인정보처리 업무 위탁에 해당하지 않음	시스템 구축·개발·운영, 통합 유지보수, 프로그램 개발 등

제 3 장 개인정보 처리 업무 위탁 절차 및 조치 사항

1. 개인정보 처리 업무 위탁 절차

절 차	소관부서	주 요 내 용
1. 개인정보 처리 업무 위탁 계약 전	각 사업장	- 개인정보 처리 업무 위탁 여부(위험성 확인) 및 범위 결정 - 수탁자 선정 시 개인정보 처리 업무위탁 점검 사항 - 개인정보 보호 계획 수립
⬇		
2. 개인정보 처리 업무 위탁 계약 시	각 사업장 혁신성과팀	- 개인정보 처리 업무 위탁 문서(계약서) 작성 - 개인정보 처리 업무 위탁 사전 점검 - 개인정보 인수증 작성 - 계약 시 개인정보 처리 업무 위탁 내용을 혁신성과팀으로 공문서 통보 ※ (혁신성과팀) 개인정보처리업무 위탁내용 홈페이지에 공고
⬇		
3. 개인정보 처리 업무 위탁 수행 중	혁신성과팀	- 수탁자 교육 실시 - 수탁자 관리 · 감독(개인정보 처리 현황 점검) - (재위탁 시) 개인정보 처리 업무 재위탁 동의서 작성
⬇		
4. 개인정보 처리 업무 위탁 종료 시	각 사업장 혁신성과팀	- 개인정보 반환 · 파기 여부 등 점검(5일 이내)
⬇		
5. 개인정보 처리 업무 위탁 현황 점검	혁신성과팀	- 개인정보 처리 업무 위탁 현황 확인 등

2. 개인정보 처리 업무 위탁 조치 사항

가. 개인정보 처리 업무 위탁 계약 전

1) 개인정보 처리 업무 위탁 여부(위험성 확인) 및 범위 결정

- 혁신성과팀(각 사업장)은 개인정보 처리 업무 위탁 시 발생할 수 있는 위험을 고려하여 위탁 여부 및 범위를 결정

※ 개인정보 유출 시 위험성이 높다고 판단된 경우 위탁 여부 재검토, 수탁자 감독 강화, 사고 발생 시 책임 소재 명확화 등의 대책 필요

- 특히, 대량의 개인정보 및 민감정보 등 처리가 포함된 업무는 유출 사고 발생 시 피해가 크므로 위탁 여부를 신중히 결정

- 혁신성과팀은 최소한의 개인정보가 처리될 수 있도록 수탁자와 사전협의 등을 통해 업무의 범위 명확화

2) 수탁자 개인정보 보호 역량 평가

- 개인정보처리 담당자는 '개인정보 처리 업무위탁 시 점검사항 **[붙임1]**'에 따라 수탁자의 개인정보 보호 역량을 평가하고 개인정보 위험성을 최소화할 수 있는 수탁자를 선정

※ 계약부서에서 수탁자를 선정하는 경우, 혁신성과팀은 최종 선정된 수탁자에 대해 개인정보 보호 역량을 평가

3) 개인정보 보호 계획 수립

- 개인정보처리 담당자는 개인정보 처리 업무 위탁 시 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 수탁자에 대한 교육 및 관리·감독 관련 내용을 포함한 개인정보 보호 계획을 수립

나. 개인정보 처리 위탁 문서 작성

1) 개인정보 처리 위탁 문서 작성

- 계약부서는 「개인정보 보호법」 제26조 제1항에 따라 개인정보 처리 업무 위탁 계약 시 아래의 내용을 포함한 '개인정보 처리 위탁 처리 업무 위탁 계약서 **[붙임2]**'를 작성

※ 계약서 작성 주체는 경영지원팀(기관장 서명·날인)

〈 개인정보 처리 업무 위탁 계약서 필수 포함 사항 〉

① 위탁 업무의 목적 및 범위
➜ 수탁자가 어떤 업무를 어떤 범위에서 처리하는지 명확하게 기재

② 재위탁 제한
➜ 수탁자가 업무를 재위탁 하는 것을 원칙적으로 금지하고, 재 위탁할 경우 사전 동의 필요 명시

③ 개인정보 접근 제한 등 안전성 확보 조치
➜ 접근통제, 암호화, 접근기록 보관 등 정보보호 조치 의무 명시

④ 위탁자의 관리·감독
➜ 위탁자가 수탁자의 개인정보 처리 현황을 관리하고 감독할 수 있는 근거를 마련

⑤ 손해배상 등 책임에 관한 사항
➜ 개인정보 유출 등 문제가 발생했을 경우, 수탁자의 책임 범위와 손해배상에 대한 내용 명시

⑥ 개인정보 파기 또는 반환
➜ 계약이 종료되었을 때 개인정보를 파기하거나 위탁자에게 반환해야 하는 의무에 대한 조항 포함

⑦ 계약 기간
➜ 위탁 계약의 유효 기간을 명시

⑧ 기타 법령에서 정한 사항

- 수탁자는 '보안 서약서**[붙임3]**'를 작성

※ 수탁 직원 변경 또는 재위탁 시에도 '보안 서약서' 작성

2) 개인정보 처리 업무 위탁 사전 점검

- 개인정보처리 담당자는 계약 시 '개인정보 처리 업무 위탁 사전 점검표**[붙임4]**'에 따라 개인정보 처리 업무 위탁 전 위험 요인 차단

3) 개인정보 인수증 작성

- 수탁자는 위탁자로부터 종이문서, 전자파일, 보안USB, CD 등의 형태로 개인정보를 제공받은 경우 '개인정보 인수증**[붙임5]**' 작성

4) 개인정보 처리 업무 위탁 내용 통보

- (각 사업장) 계약 시 위탁 내용을 혁신성과팀으로 통보
  - 통보 내용 : 위탁명, 위탁 항목, 위탁 기간, 수탁자 정보(기관명, 담당자명, 연락처), (재위탁 시)재수탁자 정보(기관명, 담당자명, 연락처)
- (혁신성과팀) 통보 받은 위탁 내용을 공단 홈페이지에 공개
  - 공개 경로 : 홈페이지 → 고객센터 → 개인정보 처리방침(개인정보 처리의 위탁현황)

다. 개인정보 처리 업무 위탁 수행 중

1) 수탁자 교육 실시

- (수행 주체) 혁신성과팀
- (교육 횟수) 연 2회 이상
- (교육 방법) 현장, 서면, 교육 기관 활용 등 수탁자 협의 후 결정

  ※ 교육은 공단 개인정보보호 담당자 직접 실시가 원칙이나, 수탁자 자체 교육도 가능

- (교육 내용) 개인정보처리의 기술적·관리적 안전 조치, 개인정보담당자 교육 사항 등

2) 수탁자 관리·감독(개인정보 처리 현황 점검)

- (수행 주체) 혁신성과팀
- (점검 횟수) 연 2회 이상
- (점검 방법) '수탁업체 개인정보처리 관리 실태 점검표**[붙임6]**'에 따라 점검

※ 공단이 수탁자를 감독하는 방법에 대하여 법률에 특별히 규정된 바는 없으므로 자료제출 요구, 현장 방문, 점검 도구 배포 등 합리적인 수단을 다양하게 활용

※ 공단이 수탁자의 개인정보 처리 현황에 대한 감독을 위하여 수탁자와 협의하여 정기적 보고를 요청할 수 있음

라. 개인정보 처리 업무 위탁 종료 시

1) 개인정보 반환·파기

- 수탁자는 위탁 문서에 명시된 개인정보 처리 기간이 종료되었거나 개인정보 처리 목적이 사라진 경우, 지체 없이(5일 이내) 개인정보를 공단에 반환하거나 파기 후 '개인정보 반환·파기 확인서**[붙임7]**' 작성

- 공단은 수탁자가 개인정보를 파기하였는지를 확인하고 반환·파기 관련 증빙 자료를 보관

〈 개인정보 파기방법 〉

수탁자는 개인정보를 파기할 때에는 복구 또는 재생되지 않도록 다음 중 어느 하나의 조치를 해야 함

① 완전 파괴(소각, 파쇄 등)
➜ 종이 문서, 하드디스크나 자기테이프는 파쇄기로 파기하거나 용해, 또는 전문 파쇄업체 이용

② 전용 소자장비를 이용하여 삭제
➜ 디가우저(Degausser)를 이용해 하드디스크나 자기테이프에 저장된 개인정보 삭제

③ 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행
➜ 개인정보가 저장된 하드디스크에 대해 완전 포맷(3회 이상 권고), 데이터 영역에 무작위 값 (0, 1 등)으로 덮어쓰기(3회 이상 권고), 해당 드라이브를 완전한 알고리즘 및 키 길이로 암호화 저장 후 삭제하고 암호화에 사용된 키 완전 폐기 및 무작위 값 덮어쓰기 등

2) 개인정보 처리 업무 위탁 종료 후 개인정보의 추가 처리

- 위탁 종료 후라도 법률상 의무 이행, 민원 등의 목적으로 개인정보의 보관 등 추가 처리가 필요한 경우, 위탁 문서에 해당 내용을 명시

제 4 장 개인정보처리 위탁 시 단계 별 안전성 확보조치

1. 용역사업 입찰 시

가. 중요 외주용역사업은 사업 착수단계부터 계획 전반을 적정 등급의 비밀 또는 대외비로 분류, 용역을 의뢰하고 모호한 표현 사용 금지

나. 입찰 공고 이전에 투입이 예상되는 자료·장비 가운데 보안관리가 필요한 사항에 대하여 관련 법규에 따라 등급을 분류하고 필요한 보안요구 사항을 마련

다. 입찰 공고 시에 해당 기관이 자체 작성한 누출금지 대상정보, 부정당업자 제재 조치, 기밀유지 의무 및 위반 시 불이익 등을 정확히 공지

라. 제안서 평가요소에 자료·장비·네트워크 보안대책 및 누출금지 대상정보 관리 방안 등 보안관리 계획마련

마. 업체가 입찰제안서에 제시한 용역사업 전반에 대한 보안관리 계획이 타당한지를 검토하여 사업자 선정 시 반영

바. 웹호스팅 등 정보시스템을 위탁 운영 시에는 해킹에 대비, 웹방화벽 등 보안시스템 구비 여부와 단순 운영 이외 보안관리가 가능한지 여부를 심층 검토

2. 용역사업 계약 시

가. 용역사업에 투입되는 자료·장비 등에 대해 대외보안이 필요한 경우 보안의 범위·책임을 명확히 하기 위하여 사업수행 계약서와 별도로 비밀유지계약서 작성

나. 비밀유지계약서에는 비밀정보의 범위, 보안준수 사항, 위반 시 손해배상 책임, 지적 재산권 문제, 자료의 반환 등이 포함되도록 명시

다. 용역사업 참여인원은 용역업체 임의로 교체할 수 없도록 명시하고 신상변동 사항 발생 시 발주기관에 즉시 보고

라. 발주기관의 요구사항을 사업자에게 명확히 전달키 위하여 작성하는 과업지시서·계약서(입찰 공고 포함)에 인원·장비·자료 등에 대한 보안조치 사항과 누출금지 대상 정보 및 부정당 업자의 제재 조치를 정확히 기술

마. 용역업체가 사업에 대한 하도급 계약을 체결할 경우 원래 사업계약 수준의 비밀유지 조항을 포함토록 조치

3. 용역사업 수행 시

가. 참여인원에 대한 보안관리

1) 용역사업 참여인원에 대해서는 '정보노출' 금지 조항 및 개인의 친필서명이 들어간 보안 서약서 징구

2) 용역사업 수행 시 참여인원에 대해 법적 또는 발주기관 규정에 따른 비밀유지 의무 준수 및 위반 시 처벌내용 등을 '**[붙임8]**'에 따라 보안교육실시

※ 누출 금지 대상정보 및 정보 노출 시 부정당업자 제재조치 등에 대한 교육 병행

3) 발주기관은 사업 수행 중 업체 인력에 대한 보안점검 실시, '노출금지 대상 정보' 외부 누출여부 확인

4) 비밀관련 사업을 수행할 경우 참여인원에 대한 비밀취급인가 등 보안조치를 수행

나. 자료에 대한 보안관리

1) 계약서에 명시한 노출금지 대상정보를 업체에 제공할 경우 사업 완료 시 관련 자료 회수

2) 사업 관련자료 및 사업과정에서 생산된 모든 산출물은 발주기관의 파일 서버에 저장하거나 보안담당관이 지정한 PC에 저장·관리

3) 용역사업 수행으로 생산되는 산출물 및 기록은 보안담당관이 인가하지 않은 비인가자에게 제공·대여·열람을 금지

다. 사무실·장비에 대한 보안관리

1) 용역사업 수행 장소는 발주 기관 내 잠금장치와 비인가자 출입통제 대책이 마련된 공간사용

2) 발주기관 내부에서 용역사업을 수행할 경우 용역 참여직원이 노트북 등 관련 장비를 외부에 반출·입 시마다 악성코드 감염여부 및 자료 무단반출 여부 확인

3) 인가받지 않은 USB메모리 등의 휴대용 저장매체 사용을 금지하며 산출물 저장을 위하여 휴대용 저장매체가 필요한 경우 발주기관의 승인 하에 사용

라. 내 · 외부망 접근 시 보안관리

1) 용역사업 수행 시 발주기관 통신망 이용이 필요한 경우

- 사업 참여인원에 대한 사용자계정(ID)은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 차등 부여하되 기관 내부문서 접근 금지

- 계정별로 부여된 접속권한은 불 필요시 곧바로 권한을 해지하거나 계정을 폐기
- 참여인원에게 부여한 패스워드는 보안담당관이 별도로 기록 관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력 확인
- 보안담당관은 서버 및 장비 운영자로 하여금 내부서버 및 네트워크 장비에 대한 접근 기록을 매일 확인하여 이상 유무 보고

2) 용역업체에서 사용하는 PC는 인터넷 연결을 금지하되, 사업 수행상 연결이 필요한 경우에는 용역업체의 관리책임자가 직접 요청하고 보안담당관은 필요성이 인정될 경우 접속할 노트북을 지정

4. 용역사업 완료 시

가. 사업 완료 후 생산되는 최종 산출물 중 대외 보안이 요구되는 자료는 삭제 및 폐기

나. 용역업체에 제공한 자료, 장비와 중간·최종 산출물 등 용역과 관련된 제반 자료는 전량 회수하고 업체에 복사본 등 별도 보관 금지

다. 저장매체는 안전성을 검증한 후 완전 삭제 후 반출

라. 용역사업 관련자료 회수 및 삭제조치 후 업체에게 복사본 등 용역사업관련 자료를 보유하고 있지 않다는 대표 명의 확약서 징구

제 5 장 기타 유의 사항

1. 손해배상책임

가. 위탁자의 사용자 책임

1) 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 발생한 손해배상책임에 대하여는 수탁자를 위탁자의 소속 직원으로 간주

2) 손해배상 청구에서 위탁자는 「민법」 제756조(사용자의 배상책임)에의한 ‘사용자 책임 (대위책임)’을 부담

- 수탁자에 대한 선정 및 교육, 관리·감독 등에 상당한 주의를 다한 경우, 위탁자는 사용자 책임을 면함

※ 선정 및 교육, 관리·감독 이행 여부에 대한 입증 책임은 위탁자가 부담

나. 수탁자의 사용자 책임

1) 수탁자의 고의 또는 과실로 「개인정보 보호법」등을 위반하여 정보주체에게 손해가 발생하였을 시, 그 불법행위에 대해 손해 배상 책임을 부담

- 「민법」 제750조(불법행위의 내용)에 따라 불법행위로 인한 손해를 배상할 책임을 부담

2. 개인정보 처리 업무 재위탁 시 준수 사항

가. 원칙

1) 개인정보 처리 업무 재위탁은 개인정보 유출 등의 위험성을 높이므로 최소한의 범위로 한정

나. 개인정보 총괄부서 조치 사항

1) 혁신성과팀은 재수탁자를 교육하고 관리·감독할 의무가 있음

2) 혁신성과팀은 재위탁하는 업무의 내용과 재수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 공개하여야 함

다. 수탁자 조치 사항

1) 「개인정보 보호법」 제26조 제6항에 따라 개인정보 처리를 제3자에게 재위탁하려는 수탁자는 재위탁 사실을 위탁부에 미리 알리고 '개인정보 처리 업무 재위탁 동의서**[붙임9]**'에 따라 동의를 받아야 함

2) 수탁자는 재수탁자의 관계에서는 「민법」 제756조(사용자의 배상책임)에 의한 '사용자책임(대위책임)'을 부담하게 되므로 재수탁자에 대한 관리·감독 의무가 있음

라. 재수탁자 조치 사항

1) 재수탁자는 수탁자와 동일하게 개인정보 보호를 위한 모든 조치를 수행해야 함

3. 상벌 규정

보안 용역 중 발생되는 보안 위규 사항 및 처리기준은 '양천구 보안용역업체 보안특약사항**[붙임10]**'에 따라 처리한다.

붙임1 개인정보 처리 업무위탁 시 점검사항

1. 점검대상

위탁사업명			
수탁기관		연락처	
점검일자		작성자	

2. 점검사항

구분	상세내역		점검결과
개인정보처리현황	개인정보수집내역		
	개인정보보유건수		
개인정보처리시스템	개인정보처리방법		아래표 참조
	개인정보접근방법		
	개인정보보호조치		

연번	점검지표	점검항목	점검결과		
1	개인정보보호 기반마련	개인정보 보호책임자와 개인정보 보호담당자는 지정하여 운영하고 있는가?	☐ Y	☐ N	☐ 해당 없음
2	개인정보보호 교육추진	연간 개인정보보호 교육계획이 수립되어 있는가?	☐ Y	☐ N	☐ 해당 없음
3		개인정보취급자, 일반직원 등에 대한 교육이 모두 이행되고 있는가?	☐ Y	☐ N	☐ 해당 없음
4	개인정보 보호책임자 역할수행	개인정보 보호책임자의 역할이 정의되어있는가?	☐ Y	☐ N	☐ 해당 없음
5		개인정보 보호책임자가 교육이수 및 관리·감독 등 역할을 수행하고 있는가?	☐ Y	☐ N	☐ 해당 없음
6	재위탁 금지	재 위탁은 하고 있지 않는가?	☐ Y	☐ N	☐ 해당 없음
7	개인정보목적외 이용 및 제3자 제공 절차	제공한 개인정보를 목적 외로 이용하거나 제3자에게 제공하고 있는가?	☐ Y	☑ N	☐ 해당 없음
8	개인정보 노출방지	개인정보 노출방지를 위해 보안시스템 및 백신 소프트웨어를 설치하고 운영(모니터링, 정기점검, 업데이트등)을 하고 있는가?	☐ Y	☐ N	☐ 해당 없음
9	개인정보 침해사고 대응절차	제공한 개인정보의 유·노출사고 및 침해사고 발생 시 대응절차를 수립하고 전파하였는가?	☐ Y	☐ N	☐ 해당 없음
10	개인정보 처리시스템 접근권한 및 접속기록	개인정보처리시스템에 접근하는 권한을 담당자별로 차등하여 부여하는가?	☐ Y	☐ N	☐ 해당 없음
11		개인정보처리시스템의 접근 권한을 부여·변경·말소한 기록을 최소 1년이상 보관하는 절차를 마련하고 이를 실행하고 있는가?	☐ Y	☐ N	☐ 해당 없음
12		개인정보처리시스템에 대한 접속기록을 점검·후속조치, 보관·관리하는가?	☐ Y	☐ N	☐ 해당 없음
13	개인정보 파기 및 관리	제공한 개인정보 처리 목적이 달성되거나 보유기간이 경과한 경우 지체없이(5일 이내) 해당 개인정보를 복원이 불가능한 방법으로 파기하고 있는가?	☐ Y	☐ N	☐ 해당 없음
14		개인정보 취급과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는 가?	☐ Y	☐ N	☐ 해당 없음
15	업무 PC 개인정보보호	업무용 컴퓨터(PC)에 저장된 개인정보는 별도로 암호화하거나 보안 USB에 저장하는가?	☐ Y	☐ N	☐ 해당 없음
16	암호화	고유식별정보, 생체인식정보 정보, 비밀번호를 개인정보처리시스템에 저장하는 경우, 해당 개인정보를 암호화하고 있는가?	☐ Y	☐ N	☐ 해당 없음

붙임2 표준 개인정보처리위탁 계약서(안)

표준 개인정보처리위탁 계약서(안)

OOO(이하 "위탁자"이라 한다)과 △△△(이하 "수탁자"이라 한다)는 "위탁자"의 개인정보 처리업무를 "수탁자"에게 위탁함에 있어 다음과 같은 내용으로 본 업무위탁계약을 체결한다.

제1조 (목적) 이 계약은 "위탁자"가 개인정보처리업무를 "수탁자"에게 위탁하고, "수탁자"는 이를 승낙하여 "수탁자"의 책임아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

제2조 (용어의 정의) 본 계약에서 별도로 정의되지 아니한 용어는「개인정보 보호법」, 같은 법 시행령 및 고시,「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2021-2호) 및「표준 개인정보 보호지침」(개인정보보호위원회 고시 제2020-1호)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) "수탁자"는 계약이 정하는 바에 따라 (_____) 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.[1)]

1.
2.

제4조 (위탁업무 기간) 이 계약서에 의한 개인정보 처리업무의 기간은 다음과 같다.

계약 기간 : 년 월 일 ~ 년 월 일

제5조 (재위탁 제한) ① "수탁자"는 "위탁자"의 사전 승낙을 얻은 경우를 제외하고 "위탁자"와의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.

② "수탁자"가 다른 제3의 회사와 수탁계약을 할 경우에는 "수탁자"는 해당 사실을 계약 체결 7일 이전에 "위탁자"에게 통보하고 협의하여야 한다.

제6조 (개인정보의 안전성 확보조치) "수탁자"는「개인정보 보호법」제23조제2항 및 제24조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조,「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2021-2호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제7조 (개인정보의 처리제한) ① "수탁자"는 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

② "수탁자"는 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보 보호법」시행령 제16조 및「개인정보의 안전성 확보조치 기준」(개인정보보호위원회 고시 제2021-2호)에 따라 즉시 파기하거나

1) 각호의 업무 예시 : 고객만족도 조사 업무, 회원가입 및 운영 업무, 사은품 배송을 위한 이름, 주소, 연락처 처리 등

"위탁자"에게 반납하여야 한다.

③ 제2항에 따라 "수탁자"가 개인정보를 파기한 경우 지체없이 "위탁자"에게 그 결과를 통보하여야 한다.

제8조 (수탁자에 대한 관리·감독 등) ① "위탁자"는 "수탁자"에 대하여 다음 각 호의 사항을 감독할 수 있으며, "수탁자"는 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속현황
3. 개인정보 접근 또는 접속 대상자
4. 목적외 이용·제공 및 재위탁 금지 준수여부
5. 암호화 등 안전성 확보조치 이행여부
6. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② "위탁자"는 "수탁자"에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, "수탁자"는 특별한 사유가 없는 한 이행하여야 한다.

③ "위탁자"는 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 (__)회 "수탁자"를 교육할 수 있으며, "수탁자"는 이에 응하여야 한다.[2)]

④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 "위탁자"는 "수탁자"와 협의하여 시행한다.

제9조 (정보주체 권리보장) ① "수탁자"는 정보주체의 개인정보 열람, 정정·삭제, 처리정지 요청 등에 대응하기 위한 연락처 등 민원 창구를 마련해야 한다.

제10조 (개인정보의 파기) ① "수탁자"는 제4조의 위탁업무기간이 종료되면 특별한 사유가 없는 한 지체 없이 개인정보를 파기하고 이를 "위탁자"에게 확인받아야 한다.

제11조 (손해배상) ① "수탁자" 또는 "수탁자"의 임직원 기타 "수탁자"의 수탁자가 이 계약에 의하여 위탁 또는 재위탁 받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 "수탁자" 또는 "수탁자"의 임직원 기타 "수탁자"의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 "위탁자" 또는 개인정보주체 기타 제3자에게 손해가 발생한 경우 "수탁자"는 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보주체 기타 제3자에게 발생한 손해에 대하여 "위탁자"가 전부 또는 일부를 배상한 때에는 "위탁자"는 이를 "수탁자"에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, "위탁자"와 "수탁자"가 서명 또는 날인한 후 각 1부씩 보관한다.

20 . . .

위탁자	수탁자
주 소 :	주 소 :
기관(회사)명 :	기관(회사)명 :
대표자 성명 : (인)	대표자 성명 : (인)

2) 「개인정보 안전성 확보조치 기준 고시」(개인정보보호위원회 고시 제2021-2호) 및 「개인정보 보호법」 제26조에 따라 개인정보처리자 및 취급자는 개인정보보호에 관한 교육을 의무적으로 시행하여야 한다.

붙임3 보안서약서(대표자, 참여직원)

(앞면)

보 안 서 약 서

주식회사 ○○○○○○○은 양천구시설관리공단 ○○○○○○○○와 관련된 업무가 기밀사항임을 인정하고, 공단의 알게 된 모든 기밀사항을 일체타인에게 누설하지 아니한다.
또한, 기밀을 누설한 때에는 어떠한 엄중한 처벌과 모든 손해배상을 변상할 것을 서약한다.

【누출금지 대상 정보】

1. 전산시스템의 내·외부 IP주소 현황
2. 전산시스템 구성현황 및 전산망구성도
3. 사용자계정 및 패스워드 등 시스템 접근권한 정보
4. 전산시스템 취약점 및 보안시스템 취약점
5. 용역사업 결과물 및 프로그램 소스코드
6. 보안시스템 및 정보보호시스템 도입현황
7. 방화벽·IPS 등 정보보호제품 및 라우터·스위치 등 네트워크장비 설정 정보
8. '개인정보보호법' 에 따른 개인정보
9. 양천구시설관리공단의 대외비 등
10. 기타 양천구시설관리공단에서 공개가 불가하다고 판단한 자료

※ 위의 모든 항목은 양천구시설관리공단에서 취급하는 모든 정보를 말한다.

※ 사업기간 중 공개불가 자료가 발생 시, 공단에서 추가 할 수 있음

※ 본 계약과 관련하여 이면 기재사항의 보안정책에 충실하며, 위반하였을 경우 관련자의 엄중한 처벌과 모든 손해배상을 변상한다.

20 년 월 일

주 소 :

상 호 :

성 명 : (인)

(뒷면)

사업자 보안정책

1. 비밀 및 대외비 급 정보 등 유출금지

(정보시스템 구조, 데이터베이스, 개인정보 및 비공개 정보 등 유출금지)

2. 정보시스템에 대한 불법적 행위 금지

(관련 시스템의 해킹, 시스템 구축 결과물의 유출 및 시스템 내 인위적인 악성코드 유포 금지)

※ 용역업무 수행 목적 외 개인정보의 처리 및 접근 금지

3. 비공개 정보 관리 강화

(비공개 정보, 개인정보를 책상 위 등에 방치 및 휴지통·폐지함 등에 유기 또는 이면지 활용 금지)

4. 사무실·보호구역 보안관리 강화

(통제구역 출입문을 개방한 채 퇴근, 인가되지 않은 작업자의 내부 시스템 접근, 통제구역 내 장비·시설 등 무단 사진촬영 금지 및 용역관련 사전승인을 받지 않은 하도급 금지 등)

5. 전산정보 보호대책 강화

- 업무망 인터넷망 혼용사용, 보안 USB 사용규정 위반 및 보안관련 프로그램 강제 삭제 금지
- 웹하드·P2P 등 인터넷 자료공유사이트를 활용하여 용역사업 관련 자료 수발신 금지
- 개발·유지보수 시 원격작업 사용 및 저장된 비공개 정보 패스워드 미부여 금지
- 인터넷망 연결 PC 하드디스크에 비공개 정보 저장 및 외부용 PC를 업무망에 무단연결사용 금지
- 사용자 계정관리 미흡 및 오남용 금지(시스템 불법접근 시도 등)
- 개인정보에 대한 접근제한 등 안전성 확보 조치
- 비인가 메신저 무단 사용 및 비인가 보조기억매체 무단 사용 금지
- PC내 보안성이 검증되지 않은 프로그램 사용 금지
- 보안관련 소프트웨어의 주기적 점검

6. 주기적 보안점검 실시

(보안관리자를 지정하여 용역관련 별도의 물리적·관리적·기술적 보안점검 실시)

붙임4 개인정보 처리 업무 위탁 시 사전 체크리스트

점검 사항	결과	비고
① 위탁자(공단)는 업무 위탁의 개인정보 위험성을 확인하였는가?		• 개인정보 유 · 노출 위험성 등을 고려하여 위탁 여부 결정 • 개인정보 위험성이 높다고 판단된 경우, 위탁 여부 재검토 • 수탁자 감독 강화 • 사고 발생 시 책임소재 명확화 등의 대책 마련 필요
② 위탁자(공단)는 수탁자의 개인정보 보호 역량을 확인하였는가?		• 수탁자 개인정보 보호 역량 분석 평가 지표 참고
③ 위탁자(공단)는 위탁하여 처리할 개인정보의 범위를 명확히 하고 수탁자와 사전 협의하였는가?		• 필요 최소한의 범위 설정
④ 위탁자(공단) 및 수탁자는 다음 6가지 내용이 포함된 위·수탁 문서를 작성하였는가? - 위탁 업무의 목적 및 범위 - 위탁 업무 수행 목적 외 개인정보 처리 금지 사항 - 위탁 업무 관련 보유하고 있는 개인정보 처리 현황 점검 등 감독에 관한 사항 - 개인정보의 기술적·관리적 보호조치 사항 ※ 개인정보에 대한 접근 제한 등 안전성 확보 조치 사항 및 재위탁 제한 사항 등 - 수탁자 준수 의무 위반한 경우 손해배상 등 책임에 관한 사항		
⑤ 위·수탁 업무 종료 후에도 수탁자가 개인정보를 보관하는 등 추가 처리를 해야하는 사유가 있다면, 사전에 위·수탁 문서에 이를 포함하였는가?		
⑥ 법령상 수탁자에게 개인정보를 보관해야 하는 의무가 발생하는 경우 위탁자에게 이를 미리 알리고 위·수탁 문서 내 법률상 근거와 개인정보 보관 기간·목적 등을 명시하였는가?		

※ 상기 점검 항목은 관련 법령의 변경 등에따라 변경·적용할 수 있음

※ 점검 결과는 '양호', '미 흡', 또는'해당없음' 표 기

점검일자 : 점검자 : (서명)

붙임5 개인정보 인수증

제공자	**기관명**	양천구시설관리공단	**소속 부서**	
	직위		**성명**	
제공받는 자	**기관명**			
	직위		**성명**	
제공 일자	*0000년 00월 00일*			
제공 목적	*00업무*			
제공 항목	*성명, 연락처, 주소 등*			
제공 형태	*보안USB*			
제공 건수	*00건*			

당사는 상기 자료를 제공받았음을 확인하며, 제공받은 자료는 업무 위탁 목적으로만 사용하고, 타 기관에 재제공 금지 및 사용 후 즉시 반환·파기하는 등 개인정보 보호 관련 법규를 준수하여 제공받은 자료의 안전성을 확보하기 위해 최선을 다할 것을 서약합니다.

년 월 일

소 속 :

직 위 :

서 약 자 : (서명)

붙임6 수탁업체 개인정보처리 관리 실태 점검표

□ 개인정보처리 위탁 현황

개인정보처리 위탁 업무명		위탁 개인정보 항목	
수탁업체		대표	

□ 수탁업체 개인정보처리 점검 확인

점검일자	2025. . .	수탁업체(책임자)	(인)

□ 수탁업체 개인정보처리 점검 확인

점 검 항 목		예	아니오	해당 없음	비 고
1. 개인정보 보호책임자의 지정 여부					법 제31조
2. 내부관리계획의 수립 여부					법 제29조
3. 개인정보처리방침의 수립 및 공개 여부					법 제30조
4. 개인정보취급자의 개인정보보호서약서 작성 여부					표준지침 제18조
5. 개인정보취급자에 대한 교육 실시 여부					법 제28조
6. 개인정보 암호화	고유식별정보의 내부저장, 외부 송·수신 시 암호화 조치 여부				안전성 확보조치 기준고시 제7조
	안전한 암호 키 생성, 이용, 보관,배포 및 파기 등에 관한 절차 수립·시행 여부				
	바이오정보의 내부저장, 외부 송·수신 시 암호화 조치 여부				
	비밀번호의 내부저장, 외부 송·수신 시 암호화 조치여부				
7. 접근통제 시스템	침입차단시스템 또는 침입탐지 시스템의 설치 및 운영 여부				안전성 확보조치 기준고시 제6조
	비 인가된 p2p, 웹하드, 공유 설정에 대한 차단 여부				

점 검 항 목		예	아니오	해당 없음	비 고
8. 보안프로그램설치 및 정기적 업데이트 수행 여부					안전성 확보조치 기준고시 제9조
9. 관리용 단말기에 대해 다음의 안전조치 적용 여부 9-1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 9-2. 본래 목적 외로 사용되지 않도록 조치 9-3. 악성프로그램 감염 방지 등을 위한 보안조치 적용					안전성 확보조치 기준고시 제10조
10. 물리적 접근방지	전산실, 자료보관실 등 물리적 보관장소에 대한 출입통제 절차 수립 여부				안전성 확보조치 기준고시 제11조
	개인정보가 포함된 서류 및 저장 장치를 안전한 장소에 보관 여부				
	개인정보가 포함된 보조저장매체의 반출•입 통제를 위한 보안대책을 마련				
11. 개인정보처리시스템에 대한 접근권한 차등 여부					안전성 확보조치 기준고시 제4조
12.접속기록의 보관 및 점검	12-1. 개인정보처리시스템 접속 기록의 보관 및 접속 기록의 위변조 및 도난, 분실되지 않도록 관리 (보관) 여부				안전성 확보조치 기준고시 제8조
	12-2. 개인정보의 분실/도난/유출/위조/변조/훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록을 반기별 1회 이상 점검 여부				
13. 개인정보 목적달성 시 지체 없이 파기 여부					법 제21조
14. 출력물 폐기 시 안전한 방법으로 파기 여부					법 제21조
15. 재 위탁 시 위탁사의 승인 획득 여부					개인정보처리위탁계약서

※ 수탁사의 개인정보 처리에 해당하는 항목에 대하여 점검함

※ “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말함

붙임7 개인정보 반환·파기 확인서

□ 개인정보처리 위탁 현황

위탁자(공단)		개인정보처리 위탁 업무명	
수탁업체		위탁기간	

□ 반환·파기 내역

제공받은 일자	0000년 00월 00일
제공받은 자료	제공·수집된 개인정보 등 항목 및 건수 기재
파기 일자	0000년 00월 00일
파기 방법	구체적인 파기 방법 기술 ※ 소각, 파쇄, 전용 소자 장비 이용, 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행 등

당사는 (위탁명) 수행을 위해 제공받은 개인정보 등을 다음과 같이 반환·파기하였으며, 이 정보로 인해 발생된 문제에 대해 모든 책임을 부담할 것을 서약합니다.

년 월 일

소 속 :

직 위 :

서 약 자 : (서명)

붙임8 개인정보 위탁업무 처리업체 보안교육 자료

1. 일반사항
   - 양천구시설관리공단의 정보보호 정책, 지침 및 매뉴얼을 준수하여야 한다.
   - 양천구시설관리공단의 자산에 접근하기 위해서는 양천구시설관리공단의 접근 통제 절차를 준수한다.
   - 양천구시설관리공단은 계약서의 보안사항을 준수하고 있는지를 감사할 권한을 가진다.
2. 참여 직원에 대한 보안관리
   - 참여직원에 대해서 각 개인의 친필 서명이 들어간 보안서약서를 제출한다.
   - 참여직원은 임의로 교체할 수 없으며, 교체 시 양천구시설관리공단의 승인을 받는다.
3. 내부 자료에 대한 보안관리
   - 제공된 내부 자료에 대해 복사 및 외부반출을 할 수 없으며, 업무 완료 후 양천구시설관리공단에 반환한다.
4. 장비에 대한 보안관리
   - 최신 바이러스 백신프로그램 설치 및 바이러스 감염 여부를 확인하여야 한다.
   - USB 등의 보조기억매체 및 카메라는 사용할 수 없다. 다만, 불가피한 경우는 양천구시설관리공단의 승인 후 사용할 수 있다.
5. 내외부망 접근에 대한 보안관리
   - 양천구시설관리공단에서 허용한 계정 이외 에는 접속할 수 없다.
   - PC(노트북 포함)는 인터넷 연결을 금지한다. 다만, 불가피한 경우는 최신 바이러스 백신프로그램 설치를 통해 바이러스 감염 검사를 실시하고 양천구시설관리공단의 확인 후 사용한다.
6. 기타 산출물에 대한 보안관리 등
   - 업무 수행 시 생산되는 모든 산출물은 양천구시설공단에서 지정한 PC에 저장하고 저장된 자료는 암호화해서 보관한다.
   - 업무 수행 시 생산되는 모든 산출물 및 기록은 양천구시설관리공단에서 인가하지 않는 자에게 제공·대여·열람을 금지한다.
   - 업무 수행으로 생산되는 모든 산출물 및 기록의 소유권 및 지적재산권은 양천구시설관리공단에 있다.
   - 참여직원에 의한 보안사고 발생 시 민·형사상의 모든 법적 책임은 계약상대자에게 있다.
7. 정보노출 시 관련법령 및 지침에 의해 부정당업자 제재조치 및 민형사상의 모든 책임을 감수해야 한다.

년 월 일

회사명 : 직급 : 성명:

붙임9 개인정보 처리 업무 재위탁 동의서

1. 양천구시설관리공단(이하 “위탁자”라 한다)과 (수탁자명)(이하 “수탁자”라 한다)가 체결한 “개인정보 처리 업무 위탁 계약서”를 바탕으로, “수탁자”는 위탁받은 개인정보 처리 업무를 재수탁자에 다시 위탁하려는 경우 아래 사항을 준수하여야 한다.

가. “수탁자”는 재위탁 시 개인정보 위험 증가 요소, 정보주체의 권리 불이익 영향 등 개인정보 보호 역량을 종합적으로 검토하여 개인정보 위험을 최소화할 수 있는 기관을 “재수탁자”로 선정하여야 한다.

나. “수탁자”는 재위탁 시 위탁받은 개인정보 처리 업무 수행을 위한 필요한 최소한의 개인정보가 처리될 수 있도록 처리 범위를 명확히 하여야 한다.

다. “수탁자”는 재위탁 시 「개인정보 보호법」에서 부여된 일반적인 의무 및 관계 법령 등에서 요구하는 사항을 반드시 준수하여야 하며, “재수탁자”와 개인정보 처리 업무 위탁 계약서를 체결하여야 한다.

라. “수탁자”는 재위탁 시 “위탁자”의 개인정보를 안전하게 보호할 수 있도록 “재수탁자”를 교육하고, 「개인정보 보호법」 제29조에 따른 관리적·기술적·물리적 안전조치를 이행하는지 관리·감독하여야 한다.

마. “수탁자”는 기존에 동의 받은 재위탁에 관한 내용이 변경되는 경우, “위탁자”에 이를 알리고 다시 동의를 구하여야 한다.

▲ 재수탁자 현황

재수탁자	재위탁 업무 목적 및 범위	재위탁 기간

2. 위 동의 내용을 증명하기 위하여 동의서 2부를 작성하고 서명 또는 날인하여, 동의서는 “위탁자”와 “수탁자”가 각각 1부씩 보관한다.

년 월 일

위탁자
주 소 :
기관(회사)명 :
대표자 성명 : (인)

수탁자
주 소 :
기관(회사)명 :
대표자 성명 : (인)

주 용역사업 보안특약 조항

① 사업자는 양천구의 보안정책을 위반하였을 경우 [별표1]의 위규처리 기준에 따라 위규자 및 관리자를 행정조치하고 [별표2]의 보안 위약금을 공단에 납부한다.

② 사업자는 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 [별표3]의 '누출금지 대상정보'에 대한 보안관리 계획을 사업제안서에 기재하여야 하며, 해당 정보 누출 시 양천구는 '지방자치단체를 당사자로 하는 계약에 관한 법률 시행령' 제92조에 따라 사업자를 부정당업체로 등록한다.

③ 사업 수행과정에서 취득한 자료와 정보에 관하여 사업수행 중은 물론 사업 완료 후에도 이를 외부에 유출해서는 안 되며, 사업 종료 시 정보보안담당자의 입회하에 완전 폐기 또는 반납해야 한다.

④ 사업자는 사업 최종 산출물에 대해 정보보안전문가 또는 전문보안 점검도구를 활용하여 보안 취약점을 점검, 도출된 취약점에 대한 개선을 완료하고 그 결과를 제출해야 한다.

[별표 1] 사업자 보안위규 처리기준

[별표 2] 보안 위약금 부과 기준

[별표 3] 누출금지 대상 정보

[별표1]

사업자 보안위규 처리기준

구 분	위 규 사 항	처 리 기 준
심 각	1. 비밀 및 대외비 급 정보 유출 및 유출시도 가. 정보시스템에 대한 구조, 데이터베이스 등의 정보 유출 나. 개인정보·신상정보 목록 유출 다. 비공개 항공사진·공간정보 등 비공개 정보 유출 2. 정보시스템에 대한 불법적 행위 가. 관련 시스템에 대한 해킹 및 해킹시도 나. 시스템 구축 결과물에 대한 외부 유출 다. 시스템 내 인위적인 악성코드 유포	○ 사업참여 제한 ○ 위규자 및 직속 감독자 등 중징계 ○ 재발 방지를 위한 조치계획 제출 ○ 위규자 대상 특별 보안교육 실시
중 대	1. 비공개 정보 관리 소홀 가. 비공개 정보를 책상 위 등에 방치 나. 비공개 정보를 휴지통·폐지함 등에 유기 또는 이면지 활용 다. 개인정보·신상정보 목록을 책상 위 등에 방치 라. 기타 비공개 정보에 대한 관리소홀 2. 사무실·보호구역 보안관리 허술 가. 통제구역 출입문을 개방한 채 퇴근 등 나. 인가되지 않은 작업자의 내부 시스템 접근 다. 통제구역 내 장비·시설 등 무단 사진촬영 3. 전산정보 보호대책 부실 가. 업무망 인터넷망 혼용사용, 보안 USB 사용규정 위반 나. 웹하드·P2P 등 인터넷 자료공유사이트를 활용하여 용역사업 관련 자료 수발신 다. 개발·유지보수 시 원격작업 사용 라. 저장된 비공개 정보 패스워드 미부여 마. 인터넷망 연결 PC 하드디스크에 비공개 정보를 저장 바. 외부용 PC를 업무망에 무단 연결 사용 사. 보안관련 프로그램 강제 삭제 아. 사용자 계정관리 미흡 및 오남용(시스템 불법접근 시도 등)	○ 위규자 및 직속 감독자 등 중징계 ○ 재발 방지를 위한 조치계획 제출 ○ 위규자 대상 특별 보안교육 실시

구 분	위 규 사 항	처 리 기 준
보 통	1. 기관 제공 중요정책·민감 자료 관리 소홀 가. 주요 현안·보고 자료를 책상위 등에 방치 나. 정책·현안자료를 휴지통·폐지함 등에 유기 또는 이면지 활용 2. 사무실 보안관리 부실 가. 캐비넷·서류함·책상 등을 개방한 채 퇴근 나. 출입키를 책상위 등에 방치 3. 보호구역 관리 소홀 가. 통제·제한구역 출입문을 개방한 채 근무 나. 보호구역내 비인가자 출입허용 등 통제 미실시 4. 전산정보 보호대책 부실 가. 휴대용저장매체를 서랍·책상 위 등에 방치한 채 퇴근 나. 네이트온 등 비인가 메신저 무단 사용 다. PC를 켜 놓거나 보조기억 매체(CD, USB 등)를 꽂아 놓고 퇴근 라. 부팅·화면보호 패스워드 미부여 또는 "1111" 등 단순숫자 부여 마. PC 비밀번호를 모니터옆 등 외부에 노출 바. 비인가 보조기억매체 무단 사용	○ 위규자 및 직속 감독자 등 경징계 ○ 위규자 및 직속 감독자 사유서 / 경위서 징구 ○ 위규자 대상 특별 보안교육 실시
경 미	1. 업무 관련서류 관리 소홀 가. 진행 중인 업무자료를 책상 등에 방치, 퇴근 나. 복사기·인쇄기 위에 서류 방치 2. 근무자 근무상태 불량 가. 각종 보안장비 운용 미숙 나. 경보·보안장치 작동 불량 3. 전산정보 보호대책 부실 가. PC내 보안성이 검증되지 않은 프로그램 사용 나. 보안관련 소프트웨어의 주기적 점검 위반	○ 위규자 서면·구두 경고 등 문책 ○ 위규자 사유서 / 경위서 징구

*** 보안위규사항 및 처리기준은 기관별 실정에 맞도록 조정**

[별표2]

보안 위약금 부과 기준

1. 위규 수준별로 A~D 등급으로 차등 부과

구분	위규 수준			
	A급	B급	C급	D급
위규	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금 비 중	부정당업자 등록	계약금액의 5%	계약금액의 3%	계약금액의 1%

* 위약금 규모는 기관별 사업규모에 따라 조정

* 위규 수준은 [별표1] 참고

2. 보안 위약금은 다른 요인에 의해 상쇄, 삭감이 되지 않도록 부과

* 보안사고는 1회의 사고만으로도 그 파급력이 큰 것을 감안하여 타 항목과 별도 부과

3. 사업 종료 시 지출금액 조정을 통해 위약금 정산

[별표3]

누출금지 대상정보

1. 기관 소유 정보시스템의 내·외부 IP주소 현황

2. 세부 정보시스템 구성현황 및 정보통신망 구성도

3. 사용자계정·비밀번호 등 정보시스템 접근권한 정보

4. 정보통신망 취약점 분석·평가 결과물

5. 용역사업 결과물 및 프로그램 소스코드

6. 국가용 보안시스템 및 정보보호시스템 도입 현황

7. 침입차단시스템·방지시스템(IPS) 등 정보보호제품 및 라우터·스위치 등 네트워크 장비 설정 정보

8.「공공기관의 정보공개에 관한 법률」제9조제1항에 따라 비공개 대상 정보로 분류된 기관의 내부문서

9.「개인정보보호법」제2조제1호의 개인정보

10.「보안업무규정」제4조의 비밀 및 동 시행규칙 제7조제3항의 대외비

11. 그 밖에 각급기관의 장이 공개가 불가하다고 판단한 자료