KISA 안내 · 해설 제2011-09호

IT 외주인력 보안통제 안내서

2011. 12

방송통신위원회
KOREA COMMUNICATIONS COMMISSION

KISA 한국인터넷진흥원
Korea Internet & Security Agency

제 · 개정 이력

순번	제 · 개정일	변경내용	발간팀	연락처
1	2011. 12. 30	제정	전자정부보안팀	
2				
3				
4				

본 안내서는 매년 정보보호 환경 변화를 반영하여 개정할 예정임.

CONTENTS

표 목차

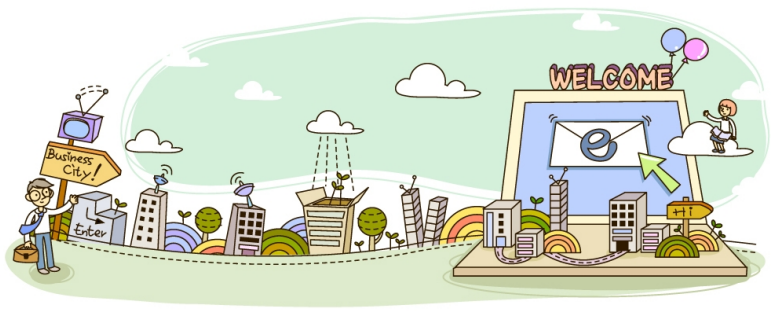
표 목차

그림 목차

제1장 소 개

1

제1장 소개



제1장 소개

제1절 개요

현황

- 최근 정보통신서비스의 일반화로 인해 다양한 산업 및 서비스 분야의 기반 환경이 정보시스템을 기반으로 운영
- 이러한 환경의 또 다른 특성은 정보시스템의 구축 및 운영에 대한 외주용역의 활용 증가

문제점

- 외주인력을 포함한 내부자에 의한 정보유출 및 보안 사고가 급증하고 있으나, 기업의 보안시스템은 외부자 공격대응 위주로 구축
- 외주용역에 참여하고 있는 인력에 대한 적절한 기술적 · 관리적 보안대책을 마련하지 않아 발생하는 보안사고로 인하여 기업의 막대한 피해가 발생한 사례 등장

  ※ 최근 발생한 농협 전산사고, 네이트 개인정보 해킹 등의 보안사고는 조직의 소홀한 내부인력 통제 관리부실이 원인

방향

- 민간기업의 IT 외주인력 보안통제를 위해 필수적으로 준수해야 할 보호대책을 제시하는 안내서 개발
- 안내서는 IT 환경의 개발 · 구축 및 운영에 대한 외주용역을 추진하고자 하는 기업들이 외주 용역의 형태를 이해하고, 각 유형별 적용가능한 기술적 · 관리적 대응방안을 제시
- 특히, 현재 운영 중인 IT 자원을 직접적으로 접근하는지에 대한 구분과 기업 내의 물리적 공간 이용여부에 따라, 유형별 차별화된 대응체계 수립에 대한 안내서 제공

제2절 구성 및 활용방안

1. 구성

[표 1-1] 보안안내서 구성

구분	내용
2장	• 전체적인 외주용역의 유형을 분류하고, 본 안내서가 다루는 외주용역의 유형을 정의
3장	• IT 외주용역 유형별 사고사례를 제시하고 외주용역의 문제점 및 보안위협에 대해 제시
4장	• 입찰 · 계약, 개발 · 구축, 사업완료, 운영 · 유지보수 단계 등 IT 외주용역 추진 단계별 보안 고려사항 도출
5장	• IT 외주인력 통제 강화를 위한 전략, 보안대책 및 적용가능 솔루션 제시 – (물리적) 인력 출입통제 및 이동장비 반출입 통제 방안 – (기술적) 계정관리, 접근권한 차등화 등 외주인력 접근통제 및 내부 중요정보 유출방지 방안 – (관리적) 시스템 작업내역 관리 · 감독 강화 등 내부통제 감시체계 구축 방안
부록	• IT 외주인력 보안강화를 위한 체크리스트 • IT 외주인력 보안 관리지침(샘플) • IT 외주인력 보안 관련 서식

2. 활용방안

[표 1-2] 보안안내서 활용방안

활용방안
• 해당기업이 수행하고자 하는 외주용역의 유형을 판단하여, 본 안내서에서 제시되는 기술적 · 관리적 보호대책을 선택적으로 적용

제2장 IT 외주용역의 분류 및 특성 정의

2

제2장 IT 외주용역의 분류 및 특성 정의

2 제2장 IT 외주용역의 분류 및 특성 정의

이번 장에서는 전체적인 IT 외주용역의 유형을 분류하고, 외주용역 유형별 특성을 정의한다. 본 안내서에서는 IT 외주용역의 유형을 외주용역이 접근할 수 있는 기업의 IT 자원유형 및 사용권한, 자원에 대한 온라인 또는 오프라인을 통한 접근경로에 따라 분류하고, 상세한 유형의 분류 및 특성은 각 절에서 제시한다.

제1절 IT 외주용역 유형

본 안내서에서는 IT 외주용역 유형을 [표 2-1]과 같이 접근 IT 자원, 자원 사용권한, 접근경로에 따라 5개의 유형으로 정의한다.

[표 2-1] IT 외주용역 유형 분류표

IT 외부용역 유형		용역 특성				
		접근 IT 자원		자원 사용 권한		접근경로
유형1	운영 용역	내부 데이터	○	읽기	○	온라인
		IT 시스템	○	쓰기	○	
유형2	유지보수 용역	내부 데이터	○	읽기 (내부직원 동행)	× (○)	온라인
		IT 시스템	○	쓰기 (내부직원 동행)	× (○)	
유형3	SI 용역	내부 데이터	○	읽기	○	온라인
		IT 시스템	○	쓰기	×	
유형4	데이터 처리 용역	내부 데이터	○	읽기	○	온라인
		IT 시스템	×	쓰기	×	
유형5	오프라인 지원	내부 데이터	○	읽기	○	오프라인
		IT 시스템	×	쓰기	×	

IT 외주용역이 접근할 수 있는 기업의 IT 자원유형은 기업 내부의 중요 데이터에 대한 접근인지 IT 시스템에 대한 접근인지에 따른 구분이며, 용역 수행원별로 자원의 갱신 가능여부에 따라 권한을 분리하여 읽기/쓰기 권한을 차등 부여한다. 또한, 접근 경로를 온라인 또는 오프라인으로 구분하고 있는데 이것은 각각 네트워크 보안 및 물리적 보안을 좀 더 고려해야하는 특성을 갖는다.

본 안내서에서 제시하는 IT 외주용역 유형들은 업무수행 시 발생할 수 있는 기업의 정보유출 방지를 위하여, 5장에서 제시하는 외주인력 통제를 위한 물리적/관리적/기술적 대책을 만족시켜야 하며, 특히, 유형2와 유형3의 경우, 각각 4장 4절 및 2절에서 제시하는, 유지 · 보수단계, 개발 · 구축단계에서의 보안 요구사항 및 보안대책을 반영하여 업무를 수행해야 한다.

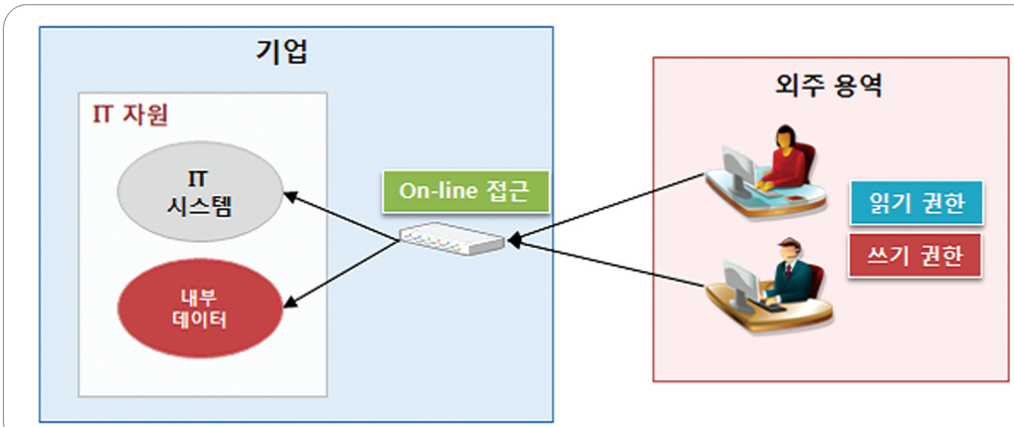
제2절 유형별 외주용역 세부 운영방식

1. IT 자원 운영 용역(유형 1)

기업 내의 IT 자원을 전담운영하는 외주용역 유형으로서 기업내의 모든 IT 시스템 및 내부 데이터에 온라인으로 접근할 수 있다. IT 외주용역 중 가장 높은 권한을 부여받는 유형으로서 모든 IT 자원에 읽기 및 쓰기 권한으로 접근하여 업무를 수행할 수 있다.

이 유형에서 IT 용역 수행원은 내부직원과 동일한 권한으로 온라인 상으로 자원에 접근하기 때문에 용역수행원은 NAC(Network Access Control)[1] 에이전트가 설치된 PC를 이용하여 업무를 수행해야하며, (그림 2-1)은 유형 1의 용역 수행원이 IT 자원에 접근하는 방법을 보여준다.

1) 사전에 인가되지 않은 사용자 및 보안문제를 가지고 있는 사용자의 IT 장치에 대해 네트워크 접근을 차단 또는 제어해주는 보안 솔루션

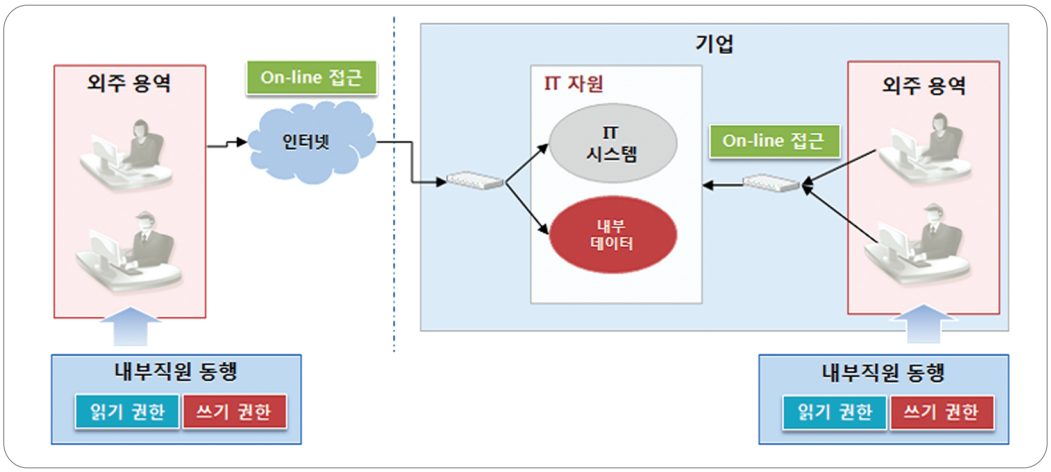


(그림 2-1) IT 자원에 대한 운영용역 유형 접근

2. IT 자원 유지보수 용역 (유형 2)

기업의 IT 자원에 대한 유지 보수 업무를 수행하는 유형으로서 유지보수 업무수행을 위해서는 유형 1과 같이 모든 IT 자원에 대한 접근이 가능하고, 모든 업무를 수행할 수 있는 권한이 필요하다. 그러나 유지보수 업무의 경우, 외주용역 업체 내에서 업무를 수행하거나 요청에 의해 단기간 동안만 작업을 할 수 있기 때문에 높은 권한을 부여할 수 없다. 따라서 용역 수행원은 IT 자원 사용에 대한 모든 권한을 부여 받지는 못하고, 업무수행 시에는 기업의 내부직원과 동행함으로써 필요한 권한을 획득하게 한다.

유형 2는 다른 유형과 달리, 외주용역 수행원의 물리적 위치에 따라 상주 및 비상주 유형으로 세분화될 수 있지만, 두 개 세부 유형 모두 온라인으로 자원에 접근하고, 내부직원에 의해 읽기 및 쓰기 권한을 획득할 수 있다는 공통된 특성을 갖는다. (그림 2-2)는 유형 2의 용역 수행원이 IT 자원에 접근하는 방법을 보여준다.



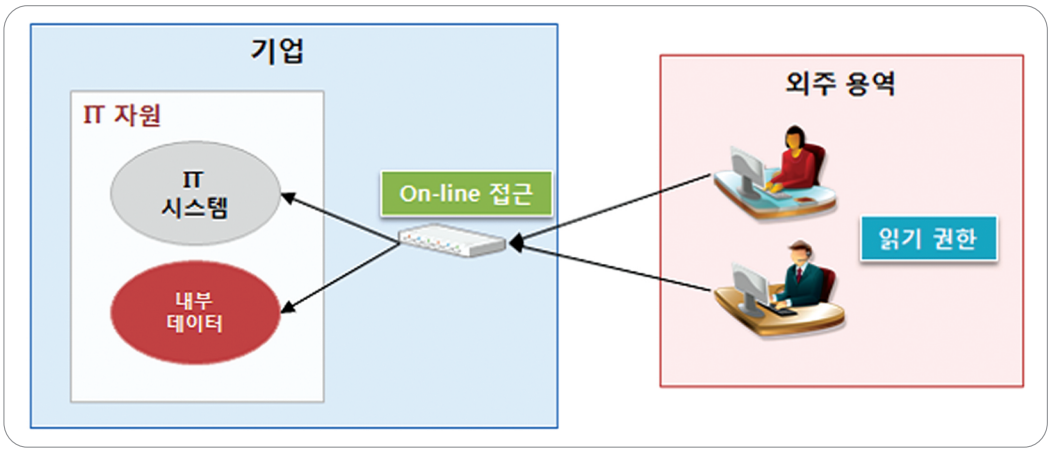
(그림 2-2) IT 자원에 대한 유지보수 용역 유형 접근

3. IT 자원 SI 용역 (유형 3)

기업의 IT 자원을 구축하는 업무를 수행하는 용역 유형으로서 현재 기업의 IT 환경에 적합한 시스템을 구축하기 위해서는 모든 IT 자원에 접근할 수 있어야 한다. 그러나 개발용역 수행 중, 내부 데이터를 수정 또는 삭제하는 등의 오류를 범하는 것을 예방하기 위하여 쓰기 권한을 부여하지 않는다.

대신, 외주용역 수행원은 모든 IT 시스템 및 내부 데이터에 접근하여 읽기 권한을 통해 원하는 정보를 획득할 수 있기 때문에 내부 데이터의 복사본을 이용하여 개발된 시스템의 검증을 수행할 수 있다. (그림 2-3)은 유형 3의 용역 수행원이 IT 자원에 접근하는 방법을 보여준다.

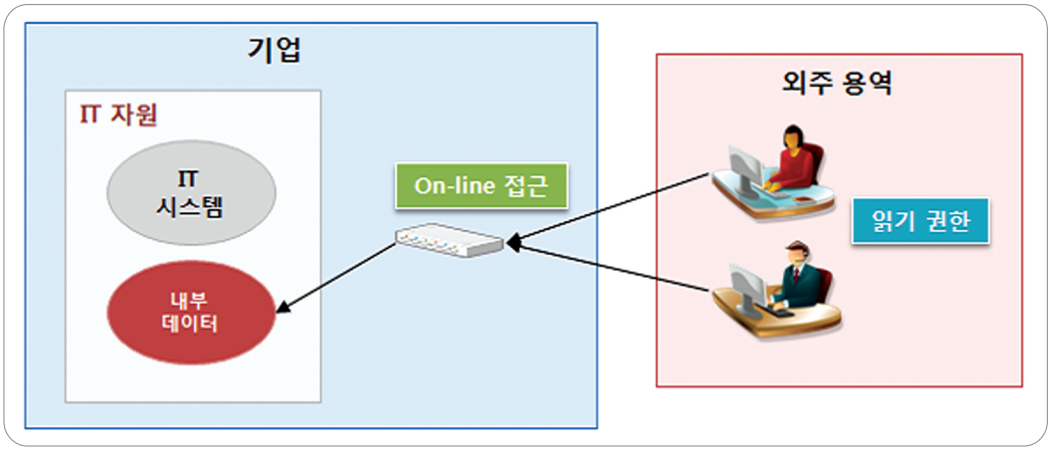
SI 용역 유형은 개발 및 구축단계에서 발생할 수 있는 기업의 정보유출을 방지하기 위하여 기업에서 정한 보안 요구사항 및 보안대책을 반영하여 업무를 수행해야 하며, 이와 관련된 자세한 사항은 4장 2절에서 다룬다.



(그림 2-3) IT 자원에 대한 SI 용역 유형 접근

4. IT 자원 데이터 처리 용역 (유형 4)

기업의 내부 데이터를 활용하여 업무를 수행하는 용역 유형으로서 헬프데스크 또는 대리점이 이 유형에 속한다. (그림 2-4)는 유형 4의 용역 수행원이 IT 자원에 접근하는 방법을 보여준다.

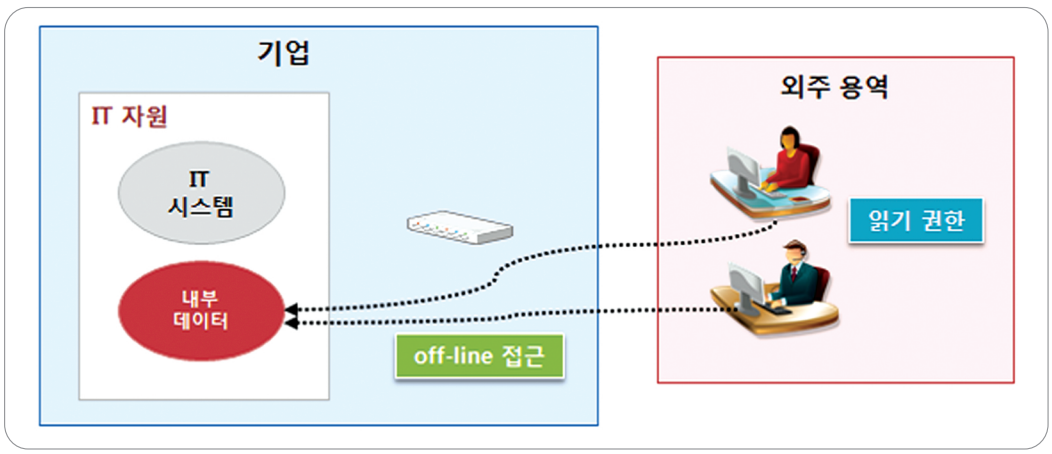


(그림 2-4) IT 자원에 대한 데이터 처리 용역 유형 접근

유형 1, 2, 3과 달리 IT 시스템에 대한 접근은 불가능하고, 온라인 접속을 통해 내부 데이터에 접근할 수 있다. 단, 내부 데이터의 수정 및 삭제를 방지하기 위하여 "읽기 권한"만 부여받게 된다. 기업의 IT 자원에 대한 로그를 유지하고, 관리하는 데이터보안 용역업체 또한 이 유형에 속한다.

5. IT 자원 오프라인 지원 용역 (유형 5)

유형 4와 같이 기업의 내부 데이터를 활용하여 업무를 수행하지만 오프라인으로만 접근 가능하다는 특성을 갖는다. 따라서 오프라인으로 출력된 산출물을 관리하는 용역업체가 이 유형에 해당되고, 출력된 내부 데이터에 대해 "읽기 권한"을 부여받아 면담 및 상담을 통해 컨설팅을 수행하는 회계 또는 보안컨설팅 등도 이 유형에 속할 수 있다. (그림 2-5)는 유형 5의 용역 수행원이 IT 자원에 접근하는 방법을 보여준다.



(그림 2-5) IT 자원에 대한 오프라인 지원 용역 유형 접근

6. 외주용역 유형의 용역 예

외주용역의 각 유형별 용역의 예는 아래 [표 2-2]와 같이 분류된다.

[표 2-2] 외주용역 유형별 예

IT 외주용역 유형		외주용역 예
1	운영 용역	• 업무망 내 IT 시스템 네트워크 및 보안 장비 운영 • 기업 내부망에 대한 취약점점검 및 모의해킹
2	유지 보수 용역	• 업무망에 온라인 접속권한으로 수행된 업무에 대한 유지보수 • 기업 내 온라인으로 진행되는 IT 시스템 네트워크 및 보안장비 유지보수 • IT 외주업체 내에서 운영되는 IT 시스템 네트워크 및 보안장비 유지보수 • 원격시스템 네트워크 및 보안장비 유지보수 • 원격 유지보수 및 장애 관리
3	SI 용역	• IT 업무지원 시스템 개발 구축
4	데이터 처리 용역	• 기업 내의 헬프데스크 운영 • 기업 내부데이터를 활용한 대리점 운영
5	오프라인 지원	• 오프라인으로 출력된 산출물을 관리하는 용역업체 • 오프라인으로 출력된 내부데이터를 활용하여 면담으로 진행되는 정보보호컨설팅 • 오프라인으로 출력된 내부데이터를 활용하여 진행되는 기업 회계감사 및 보안컨설팅

3

제3장 IT 외주용역 유형별 사고사례 및 보안 위협

제3장 IT 외주용역 유형별 사고사례 및 보안 위협

● 이번 장에서는 IT 외주용역 유형별 사고사례를 제시하고 외주용역의 문제점 및 보안위협에 대해 제시함

외주용역을 활용하여 시스템을 운영하는 기업 중 외주용역 기관의 과실 등의 이유로 정보유출 등의 사고가 발생한 주요사례를 정리해 보면 아래 [표 3-1]과 같다.

[표 3-1] 외주용역 정보유출 사례 및 피해 건수

일시	위치(기업)	유출 피해건수	시스템 운영방법	정보유출 방법
'10.9	OO교육 관리기관	630만명	외주업체에서 시스템 전반을 위탁 관리	서버 유지보수 업체 직원이 서버에 해킹 프로그램을 설치해 개인정보를 빼돌림
'11.3	OO캐피탈	175만명	외주업체에서 보안업무 위탁관리	업무성격상 불필요한 권한 부여 및 퇴직자 계정 정보 미삭제 등의 시스템 접근권한관리 미흡
'11.4	OO은행	-	외주업체에서 서버관리	외주업체 직원 노트북을 통한 해킹으로 전산망 마비
'11.5	OO증권사	2.7만명	외주업체에서 전산망 관리	외주업체에서 공격 탐지 후 모기업에 알렸으나, 안일하게 대처
'11.9	OO 국가기관	92만명	전자여권 발급기 시스템 운영을 외주업체에 맡김	여권발급기 부품교체 주기를 파악한다는 명목으로 신상정보를 매주 본사로 보내 여권발급에 필요한 개인의 신상정보가 무단으로 유출
'11.9	OO구청	60만명	구청 호적등본 자료의 전산화 작업을 외주업체에 맡김	문서고에서 호적등본을 전산화하는 과정에서 외주업체 직원이 주민정보를 스캔한 파일이 저장된 외장하드를 분실

제1절 IT 외주용역 유형별 사고사례

2장에서는 IT 외주용역 업체가 접근하는 IT 자원과 자원에 대한 권한을 기준으로 하여 IT 자원 운영 용역(유형 1), IT 자원 유지보수 용역(유형 2), IT 자원 SI 용역(유형 3), IT 자원 데이터처리 용역(유형 4), IT 자원 오프라인 지원 용역(유형 5) 등 총 5개의 유형으로 분류하였다.

이번 절에서는 각 유형별로 존재할 수 있는 보안위협과 이에 따른 사고사례 및 시나리오를 제시하고자 한다.

1. IT 자원 운영 용역(유형 1)

유형 1은 기업내의 IT 자원을 운영하는 외주용역을 위탁하는 경우이다. 따라서 외주용역은 업무지원 시스템 운영 또는 네트워크 및 보안장비 운영시 업무망에 대한 온라인 접속권한을 이용하여 개인정보를 탈취할 수 있다. 즉, 온라인 업무망 접속권한을 가진 IT 외주용역 수행자가 업무목적 이외에 기업 내부정보를 열람하거나 쓰기권한을 사용하여 기업내부의 정보를 조작 또는 설정을 변경하여 외부 유출하는 형태와, 백도어 구축 또는 해킹 프로그램 설치를 통해 무단으로 정보를 유출시키는 형태의 보안위협이 존재한다. 또한 보안관리 업무 수행 시, 의도/비의도적인 보안 공격에 의해 업무망 마비 또는 데이터 손실을 발생시키는 형태의 위협 등이 존재한다.

〈세부 유형〉

- 업무망 내 IT 시스템 네트워크 및 보안장비 운영
- 기업 내부망에 대한 취약점점검 및 모의해킹

■ (보안위협1) IT 외주용역 수행자의 기업 내부 정보 조작

〈시나리오〉 포털게임 외주업체 직원, 1억 빼돌려...

• 사고 개요
- 포털게임 업체 A사의 고객 정보관련 DB업무를 위탁관리하고 있는 외주용역 업체 직원이 업무 외의 목적으로 고객정보를 무단으로 열람하고 조작 및 로그 등을 삭제하는 행위를 함
- 해당직원은 DB접근 권한을 이용하여 수백 명에 달하는 회원들의 게임머니를 조작하고 로그를 삭제하여 1억원 상당의 부당이득을 얻음

• 사고 원인
- 고객정보를 다루는 외주업체 직원의 보안인식 미흡 및 외주용역 직원의 행위에 대한 감사기능 미비

■ (보안위협2) 외주직원의 보안관리 업무수행시, 의도/비의도적인 공격

〈시나리오〉 인가되지 않은 USB 이용으로 전산망 장애

• 사고 개요
- OO기관은 보안관리를 위해 A보안업체에 취약점 점검 및 모의해킹을 의뢰하여 업무종료 후 작업에 들어갔으나 알 수 없는 악성코드로 인해 작업이 지연되어 다음 날까지 전산망에 문제 발생
- 취약점 점검툴을 설치하기 위해 보안업체 직원은 USB를 이용하였고 이를 통해 OO기관 전산망에 악성코드가 감염됨

• 사고 원인
- 외부에서 반입된 인가되지 않은 USB의 사용과 같이, 이동저장매체에 대한 관리적 · 기술적 통제대책 미흡

■ **(보안위협3) IT 외주용역 수행자의 보안관리 용역 업무수행 시, 의도/비의도적인 보안 공격**

〈시나리오〉 보안관리 업체 직원의 원격접속 PC 관리소홀로 시스템 장애유발

• 사고 개요
  – 원격 취약점점검 및 모의해킹을 수행하는 외주용역 직원의 PC가 DoS공격과 관련된 악성코드에 감염되어 있었고, 원격접속된 OO기관 시스템에도 퍼져 좀비PC로 이용
  – 특정 IP로 과도한 요청을 지속적으로 전송하여 OO기관 시스템에 장애가 발생함

• 사고 원인
  – 외주직원의 보안인식 및 원격접속 허용된 PC에 대한 관리 소홀

■ **(보안위협4) IT 외주용역 업체 내 'IT 자원 접근권한'이 없는자에 의한 기업 내부정보 무단 열람 및 외부 유출**

〈시나리오〉 외부인의 부탁을 받고 개인정보를 무단 열람

• 사고 개요
  – OO기관 IT시스템 운영업무를 담당하는 외주업체 직원이 특정인의 개인정보를 업무목적과는 다른 용도로 열람, 제 3자에게 제공함

• 사고 원인
  – 외주용역 직원의 기업내 온라인 접속 및 개인정보 DB 접속 권한에 대한 통제 미흡
  – 외주용역 직원의 업무목적과는 다른 용도로 열람한 사실은 개인정보취급자가 권한 없이 처리하지 못하도록 되어 있는 법률에 위반됨

■ (보안위협5) IT 외주용역 업체 내 취약한 IT 시스템에 의한 기업 내 IT 시스템의 감염 위협

〈사례〉 시스템 계정관리 부실 취약점을 악용한 전산망 마비

• 사고 개요
- 지난 4월 11일 발생한 OO은행 전산 장애로 창구거래 등 전반적인 금융 서비스가 마비되는 사건이 발생하여 은행 고객의 카드 결제, 교통카드 사용, 체크카드 사용내역 조회 등에 불편함을 겪음
- OO은행의 서버관리 협력업체인 △△기업 직원의 노트북을 통해 OO은행 서버에 삭제명령이 입력됨
- OO은행이 전산망 마비 사고로 입은 경제적 피해는 최소 80억원 규모로 추정

• 사고 원인
- 금융감독원의 OO은행 감사 결과 OO은행은 시스템 계정의 비밀번호 변경관리 부실, 단순 비밀번호 사용
- 외주직원의 보안인식 및 관리감독 미흡, 정보시스템 접근관리 미흡
- 외주용역 직원이 보유한 노트북 등 이동저장매체에 대한 통제 미흡

■ (보안위협6) IT 외주용역 수행자에 의한 기업 IT 시스템 설정변경 및 시스템 내 정보유출

〈시나리오〉 업체 내 개인정보를 자신의 PC로 무단저장

• 사고 개요
- OO업체에서 서비스 운영(개인정보 포함)을 담당하던 외주업체 직원이 원격으로 관리자 권한을 부여받아 업무를 수행하고 있으며, 고객들의 개인정보를 몰래 자신의 PC로 전송하여, 이를 대부광고업체에 팔아 넘김

• 사고 원인
- 외주직원의 핵심정보에 대한 원격접근 허용 및 관리적 · 기술적 통제대책 수립, 감사기능 미흡

2. IT 자원 유지 보수 용역(유형 2)

유형 2는 IT 시스템과 내부 데이터 모두 접근할 수 있는 권한을 가지고 있으나 내부 직원과 동행시에 해당 자원에 대한 읽기 및 쓰기 권한을 획득할 수 있다. 따라서 IT 시스템 접근권한이 제대로 관리되지 않는 경우, 보안인식이 미흡하거나 사적인 목적달성을 위하여 IT 시스템 접근권한을 소유한 IT 외주용역 수행자가 기업 내부 IT 시스템에 무분별하게 접근하여 기업 IT 시스템의 설정 변경할 수 있다. 또한 이를 통해 업무수행 불능 시스템으로 유도할 가능성이 존재하며 시스템 내 정보 유출의 가능성도 배제 할 수 없다. 한편, 외주업체 직원의 USB 등의 외부 장치를 통해 악성 프로그램을 유포시켜 시스템에 장애를 발생시키거나 해킹 프로그램 설치를 통한 개인 및 기업 정보 유출 가능성도 존재한다.

〈세부 유형〉

- 업무망 온라인 접속 권한으로 수행된 용역 업무에 대한 유지보수
- 기업 내 온라인으로 진행되는 IT 시스템 네트워크 및 보안 장비 유지보수
- IT 외주업체 내에서 운영되는 IT 시스템 네트워크 및 보안 장비 유지보수
- 원격 시스템 네트워크 및 보안 장비 유지보수
- 원격 유지보수 및 장애 관리

■ (보안위협1) 업무수행 시 기업의 내부 직원과 동행하지 않고 IT자원 접근권한 획득

〈사례〉 OO기관, 외주업체 직원에게 승인 없이 개인정보 열람 허용 (2008.10)

- 사고 개요
  - OO기관은 외주용역업체 업무수행을 위해 기관 승인하에 담당직원과 함께 관련 정보에 접근토록 하고 있으나, 부처 감사결과 외주용역직원에게 기관 직원 ID를 공동으로 사용할 수 있도록 허용
  - 외주용역업체 직원은 기관 직원 ID를 이용하여 종합전산망에 접속 총 1,066회의 개인정보에 접근한 것으로 확인됨

• 사고 원인
– 외주용역 직원에 의한 기업 내부 IT 시스템 접근은 책임자 승인하에 담당직원과 함께 화면조회가 가능하나 외주직원의 무분별한 접근에 대한 관리적 · 기술적 통제대책 수립 및 감사기능 미흡

■ (보안위협2) 업무 목적 외 기업 내부정보 열람, 외부 유출

〈사례1〉 OO교육기관 해킹당해...630만 학생 개인정보 유출(2010. 09)

• 사고 개요
– 서버 유지보수 업체 직원 등 IT업체 대표와 개발자 등이 OO기관이 관리하는 전자도서관 서버에 해킹 프로그램을 설치해 학생들의 개인정보를 탈취하고, 이를 독서통장 사업자에게 팔아 부당이득을 챙김
※ 독서통장은 책을 빌리고 반납한 기록을 통장 형태로 보여주는 것으로 많은 초, 중, 고등학교 학생들이 사용
– 전자도서관 서버에 대한 유지보수를 위탁받은 외주업체 직원들은 서버 점검시 방화벽이 해제된 틈을 타 불법 프로그램을 설치하여 개인정보를 유출

• 사고 원인
– 유지보수 업체 작업에 대한 관리감독 및 기술적인 통제 부족

〈사례2〉 전자여권 92만명 정보 유출 (2011.09)

• 사고 개요
– 전자여권 신청자의 주민번호와 여권번호 등 개인 신상정보 92만여건이 여권발급기 운용업체 직원들에 의해 무단 유출
– 조폐공사 보안 규정에 따르면 여권 신청자의 신상정보는 여권제작 후 조폐공사 전산서버에서 곧바로 삭제되어야 하지만, 해당 외주사 직원들은 여권발급기 부품 교체주기를 파악한다는 명목으로 신상정보를 매주 본사로 전송

• 사고 원인
– 외주직원에 대한 보안인식 교육 및 관리감독이 미흡함
– 기관의 보안규정에 맞게 개인정보 데이터가 제대로 관리되지 않음

■ (보안위협3) 외주직원의 업무 목적 외 기업 내부정보 열람 및 변조, 외부 유출

〈시나리오〉 외주직원, 서버 접근계정 공유하여 부당이득 취해..

• 사고 개요
– A업체 서버 유지보수를 담당하고 있는 외주업체 직원이 A업체에 상주하지 않고 본사에서 원격으로 A업체 서버에 접근하기 위한 계정을 소유함
– 외주직원은 A업체 서버에 접근하기 위한 관리자 계정을 제 3자에게 유출하여 A업체 서버내 정보가 유출되고, 서버접근 계정을 공유한 댓가로 부당이득을 취함

• 사고 원인
– 외주용역 직원에 대해 관리자 계정, 암호 공유 및 원격접속 허용 등 적절한 시스템 접속 권한 관리 미흡

■ (보안위협4) 외주용역 직원에 의한 기업 IT 시스템 설정 변경 및 시스템 내 정보 유출

〈시나리오〉 시스템 유지보수 직원이 백도어 설치...외부로 개인정보 전송

• 사고 개요
– 외주용역 업체 직원이 전산망 구성도와 개인정보가 저장된 서버의 관리자 권한을 소유한 내부 담당자에게 악성코드가 포함된 이메일을 전송, 메일을 열어본 내부 담당자의 PC에 백도어가 설치됨
– 설치된 백도어를 이용하여 외주 직원은 외부의 특정서버로 개인정보 전송

사고 원인
– 외주용역 직원에 대한 신원조회, 보안교육 등 관리가 소홀하며, 이메일에 대한 보안통제 대책 미흡

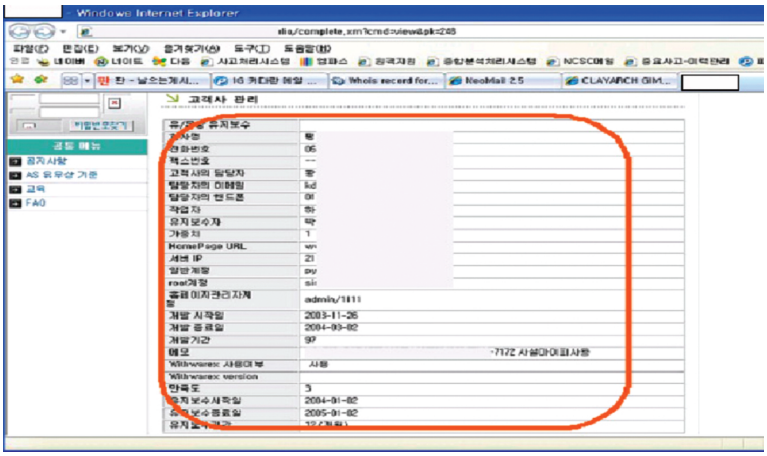
■ (보안위협5) IT 외주용역 업체 내 용역 수행자 외의 인력에 의한 기업 내부 정보 유출

〈사례〉 홈페이지 유지보수 업체 홈페이지 취약점을 이용하여 205개 공공 · 민간업체 정보 노출 (2007. 08)

• 사고 개요

– 홈페이지 유지보수 업체의 홈페이지에 취약점이 존재하여 홈페이지에 저장되어 있던 205개 공공 · 민간업체의 홈페이지 관리자 ID · 패스워드 등의 정보가 검색사이트에 노출

(그림 3–1) 검색사이트에 노출된 관리자정보 위치(URL)



(그림 3–2) 노출된 기관별 홈페이지 관리자 정보

• 사고 원인
– 외주용역 업체의 고객사 홈페이지 계정정보 관리 부실

■ **(보안위협6) IT 외주용역 수행자에 의한 기업 내부 정보 외부 유출**

〈사례〉 기업자료의 무단반출 및 관리부실로 정보노출 (2007.09)

• 사고 개요
– OO사 유지보수담당 직원이 9개 정부부처 정보화사업 자료를 OO기관의 유지보수 프로젝트에 활용키 위해 자택PC에 보관
– 해당 자료들이 공유폴더로 설정된 폴더에 저장되어 있어 P2P에 접속하자 자택PC에 저장되어있던 자료들이 노출됨

• 사고 원인
– 기밀자료에 대한 무단 반출 및 P2P 공유 프로그램 사용으로 자료 유출
– 기밀자료에 대한 접근통제, 보안관리 강화 및 외주용역 직원에 대한 보안 교육 미흡

3. IT 자원 SI 용역(유형 3)

유형 3은 IT 시스템 및 내부 데이터 모두에 대한 접근권한을 가지고 있는 경우로서 기업 내부 데이터에 대한 수정을 방지하기 위하여 읽기 권한만 부여한다. 본 유형에서는 IT 외주용역 수행자가 기업 내부정보를 분실하거나 의도적인 목적을 가지고 외부로 유출할 가능성이 존재한다.

〈세부 유형〉

• IT 업무지원 시스템 개발 구축

■ (보안위협1) IT 외주용역 수행자에 의한 기업 내부 정보 외부 유출

〈사례1〉 OO부처 비공개 자료 웹하드에 보관 중 노출 (2007.07)

• 사고 개요
- OO부처 정보화사업을 담당하는 하도급업체 직원이 네트워크 구성도, IP할당내역 등 전산망 이전 관련 자료를 웹하드에 보관
- 인터넷 웹하드의 비밀번호를 설정하지 않아 해당 웹하드 가입자들이 제한 없이 자료에 대한 검색은 물론 다운로드 가능하여 정보 유출

• 사고 원인
- 외주용역 직원이 기업 핵심정보를 인가받지 않은 방식으로 관리

〈사례2〉 OO구청 주민정보 60만건을 담은 외장하드 분실로 인한 중요정보 노출 (2011. 09)

• 사고 개요
- 구청 호적등본 자료 전산화 업무를 맡고 있는 외주업체 직원이 호적등본을 전산화하는 과정에서 주민정보를 스캔한 파일 60여만 건이 저장된 외장하드 분실
- 조사결과 OO구청 공익요원이 종합문서고에 방치된 외장 하드디스크를 보고 충동적으로 가지고 나온 것으로 밝혀짐

• 사고 원인
- 외주직원의 보안인식 및 관리감독이 미흡하고, 문서고의 출입문은 이중통제가 적용되어 있으나 제대로 운용하지 않아 비인가 직원의 출입 가능

4. IT 자원 데이터 처리 용역(유형 4)

유형 4는 기업 내부 데이터 자원을 읽을 수 있는 권한을 가지고 온라인으로 접근이 이루어지는 경우를 말한다. 용역 업무수행을 위해 온라인 업무망 접근 권한을 소유한 IT 외주용역 수행자는 기업 내부정보를 분실하거나 의도적인 목적을 가지고 외부로 유출할 가능성이 존재한다.

〈세부 유형〉

- 기업내의 헬프데스크 운영
- 기업 내부 데이터를 활용하여 대리점 운영

■ (보안위협1) IT 외주용역 수행자에 의한 기업 내부 정보 외부 유출

〈사례〉 대형 포털사이트 고객상담 내용 일부 유출 (2007.10)

- 사고 개요
  - 해커는 외주업체가 운영관리하는 국내 포털사이트의 고객상담 관리시스템을 해킹 후 이를 볼모로 금품을 요구
  - 고객상담 관리를 맡은 외주업체는 적절한 보안시스템을 구축하지 않아 시스템이 외부 IP에서의 접근이 가능하였고, 이를 이용해 고객상담 관리자의 아이디와 비밀번호를 알아내 관리자 페이지에 접근

- 사고 원인
  - 외주업체의 보안관리 감독 미흡

5. IT 자원 오프라인 지원 용역(유형 5)

유형5는 IT자원에 대한 간접접근이 이루어지며, 면담/상담이 주 업무가 되어 노트북 컴퓨터 등을 내부에 도입하여 진행하는 경우이다. 회계감사 또는 컨설턴트 등 용역업무 수행을 위해 오프라인 업무망 접근권한을 소유한 IT 외주용역 수행자는 기업 내부 정보를 분실하거

나 의도적인 목적을 가지고 외부로 유출할 가능성이 존재한다. 한편, 용역 수행자가 기업체에 비상주하는 경우에는 IT 외주용역 업체 내 용역 수행자 외의 인력 즉, 권한을 가지지 않은 자에 의해 기업 내부 정보가 열람되거나 유출될 수 있다.

〈세부 유형〉

- 오프라인으로 출력된 산출물을 관리하는 용역 업체
- 오프라인으로 출력된 내부 데이터를 활용하여 면담으로 진행되는 정보보호컨설팅
- 오프라인으로 출력된 내부 데이터를 활용하여 진행되는 기업 회계감사 및 보안컨설팅

■ (보안위협1) IT 외주용역 업체 내 용역 수행자 외의 인력에 의한 기업 내부 정보 유출

〈사례〉 고객사의 내부정보 무단유출로 부당이익 취득 (2011.06)

• 사고 개요
  – 세계적인 컨설팅 회사인 OOO의 선임 파트너가 고객사인 반도체 회사 내부 정보를 헤지 펀드로 넘긴 혐의로 미국 검찰에 체포됨
  – 관련자 들은 고객 회사의 내부정보에 대한 비밀을 유출하여 이를 이용해 2500만 달러의 부당 이익을 취한 혐의를 받음

• 사고 원인
  – 기업 내에서 진행되는 기업 경영 컨설팅 자료에 대한 통제 부재
  – 외주용역 사업 종료시 자료 반납 및 폐기 절차 미이행

제2절 IT 외주용역 사고원인 및 보안위협

1. IT 외주용역 사고원인 분석

- 해킹 등 외부자 공격대응 위주의 대책 및 투자로 외주용역 직원을 포함한 내부자에 대한 보안위협 예방 · 대응 관련 보안 인프라 투자는 매우 미흡
  - 최근 발생한 농협 전산사고(4.12), 네이트 해킹(7.12) 등의 보안사고는 조직의 소홀한 외주용역 인원의 통제 관리부실이 원인
  - IT 업무 특성 상 아웃소싱 의존도가 높은 반면, 내부자 보안에는 소홀

- IT 외주용역에 의한 정보유출 및 보안사고는 급증하고 있으나, 기업의 보안시스템은 외부자 공격대응 위주로 구축
  ※ 보안사고의 60% 이상이 내부자에 의해 발생(IDC 조사, 2009년)
  ※ '07년 이후 내부자에 의한 자료유출 사건이 3배 이상 증가(KPMG, 2010년)
  ※ 외부자 대응 : 침입방지(90%), 웹방화벽(85%)
  내부자 대응 : 서버보안(18%)(전자정부 대민서비스 실태조사, 2011년)

- 출입통제, 보안서약서 징구, 관리대장 기록 등 기본적인 수준의 보안 활동 · 점검은 이루어지고 있으나,
  - 내부자 보안위협에 대한 인식 미흡, 시스템적 관리환경 취약, 형식적인 점검 등으로 접근통제 및 모니터링, 사후추적 등이 취약

[표 3-2] 내부자 보안사고 피해사례 및 특징

사례	유출경로 · 원인 및 내용	비고(대응방안)
OOO 해킹 ('11.7.26)	– 중국해커 악성코드 제작 → 이스트 소프트 서버감염 →알집 다운받은 직원 PC감염 → DB 접속 → 3500만 정보 유출	– 정보시스템 접속 시 악성코드 감염 여부 확인
OO 전산사고 ('11.4.12)	협력업체 직원이 악성코드에 감염된 노트북 반입 → 삭제명령 실행 → 주요서버 공격 및 전산마비 사태	– 반출입 매체에 대한 악성코드 감염여부 검증 – 금지명령어 차단을 위한 기술적 조치

OO 정보유출 사건 ('11.4.7)	– 인천의 OO기관 직원이 공모하여 내부망의 개인정보 유출 → 부당이득	– 내부자간 감시체제 강화 및 작업내역 모니터링
OO부처 서버 해킹 ('10.9.29)	– OO부처 협력업체 직원이 서버에 해킹 프로그램 설치 → 630만 개인정보 유출 → 불법 판매로 부당이득	– 협력업체 직원의 작업내역 기록 및 관리감독 강화 – 반출입 매체의 자료검증

2. 영역별 보안위협

2.1 물리적 영역

■ **물리적 접근영역의 보안위협은 아래와 같음**

[표 3-3] 물리적 접근영역 보안위협

– **(접근통제)** 인가받은 자가 기업 내부의 중요정보가 보관된 장소에 접근하여 업무외의 목적으로 정보를 열람하는 경우 또는 비 인가자가 침입하는 경우에 의한 중요 정보 유출
– **(출입탐지)** 비 인가자 출입탐지를 위한 CCTV의 사각지대 존재
– **(출입관리)** 기업 내부의 중요정보가 존재하는 장소에 출입통제 내역을 관리하지 않아 중요정보에 불법적인 접근 위협
– **(정보 시스템 접근 관리)** 중요정보가 유출되거나 중요시스템에 피해가 발생했을 때, 책임에 대한 배상을 요구할 수 없음
– **(반입 매체통제)** 허가되지 않은 매체 반 · 출입으로 인한 악성코드 감염 또는 정보유출의 위협

2.2 기술적 영역

■ **기술적 접근영역의 보안위협은 아래와 같음**

[표 3-4] 기술적 접근영역 보안위협

- **(인증수단)** 정보시스템 접근시 ID/PW만을 사용할 경우, 노출 또는 낮은 패스워드 설정 등으로 인한 침해요소
- **(인증정보)** IT 외주 개별 인력에 내부시스템 사용자 인증 정보를 제공해 주지 않아 사후 관리 불가 및 중요정보에 대한 접근, 유출 위협
- **(네트워크 통제)** 업무수행 중 공개망에 접속하여 악성코드 감염, 취약점이 발생하여 시스템 파괴 또는 공개망을 통해 내부정보를 외부로 유출할 위협이 존재
- **(반출 매체 통제)** 직원출입시 노트북, USB 등에 대한 바이러스 점검 부재시 악성코드 감염 등 위험
- **(출력물 통제)** 개인정보, 내부 네트워크 구성도 등 중요문서를 출력하여 유출할 위험

2.3 관리적 영역

■ 관리적 접근영역의 보안위협은 아래와 같음

[표 3-5] 관리적 접근영역 보안위협

- **(작업내역)** 작업 중 불필요한 저장 또는 중요 정보 유출을 목적으로 작업 수행의 결과물을 저장/보관함으로써 중요정보 유출
- **(접근권한)** 중요 정보 접근에 대한 관리가 이루어지지 않아 허가받지 않은 정보에 접근을 시도하거나, 접근허가가 만료된 계정을 처리하지 않아 시스템에 접근을 시도하여 중요정보 유출
- **(접근이력 및 작업내용에 대한 보안감사)** 정보시스템 유지보수 및 관리시 접근이력 및 작업내용에 대한 보안감사 기록 부재로 보안사고 원인 추적불가
- **(악성코드)** 악성코드 감염 등과 같은 사전 검열 작업을 수행하지 않아 USB, 외장하드 등을 사용하는 장비를 통해 악성코드가 내부 망에 침입하여 중요정보를 유출하거나 내부 시스템에 치명적 오류를 발생
- **(체계적 인력관리 계획)** 체계적인 인력 관리 계획이 존재하지 않아 정보시스템 불법접근, 정보유출을 시도하여도 인력의 이동 및 행동 등에 대한 빠른 파악이 불가능
- **(인력배치)** 업무에 적합하지 않은 상주 유지보수 인력배치로 인한 내부시스템의 취약점 발생 및 중요정보 유출
- **(인력감사)** 인력에 대한 감사를 실시하지 않아 중요 정보 유출의 가능성 존재

3. IT 외주용역 발주시 정보보호 고려사항

- 외주용역 업체와의 서비스계약 진행 시 외주 직원의 보안을 위한 정보보호를 위해 아래 사항을 포함 하여야 함

[표 3-6] 용역 발주시 정보보호 고려사항

- 기관 정보보호에 대한 일반 정책 준수
- 정보자산에 대한 보호
- 데이터 및 소프트웨어를 포함하는 기관의 정보자산을 보호
- 정보자산 변경(데이터 손실 또는 수정)이 발생하는지를 판별
- 정보자산의 회수 및 파기를 확인할 수 있는 통제
- 사용 가능한 서비스에 대한 설명
- 법적 문제에 대한 책임
- 다음을 포함하는 접근통제 협의
  - 사용자 인증(사용자 ID 및 비밀 번호)의 사용 및 통제
  - 사용자 접근 및 권한에 대한 허가 절차
  - 서비스의 사용이 허가된 개인들의 명단과 서비스 사용에 있어서의 권리와 특권이 무엇인지를 규정하는 목록
  - 협력업체 직원의 행위를 모니터링하고 권한을 해지할 수 있는 권리
  - 방법, 절차에서의 사용자 및 관리자 교육
  - 정보보호 사고 및 정보보호 침해에 대한 보고 및 통지, 조사에 대한 합의
- 협력업체 직원의 내부/외부 접속
  - 업무상 필요에 의해 협력업체 직원의 기관 정보시스템에 대한 접속 및 외부로의 접속이 요구되는 경우 정보보호 담당자의 사전 승인 획득

4

제4장 IT 외주용역 단계별 보안 강화 방안

4 제4장 IT 외주용역 단계별 보안 강화 방안

● 이번 장에서는 IT 외주용역 추진시 담당자 관점에서 단계별 정보보호 고려사항 및 대응지침을 제시함

이번 장에서는 용역 추진 담당자가 고려해야할 정보보호 고려사항 및 대응지침을 제시하되, 크게 ①입찰 및 계약 단계 ②개발 및 구축 단계, ③사업 완료 단계, ④운영·유지보수 단계 등 4단계로 구분한다.

제1절 입찰 및 계약 단계

IT 외주용역 선정 및 계약 단계는 용역 환경에 대한 사업계획서 작성 단계에서부터 사전 보안 요구사항 도출 및 계약서에 보안대책을 반영

- 입찰 및 계약단계에서는 외주용역사업의 보안요구사항을 정의하여 제안서 상에 반영하고, 실제 사업계획서 및 계약서상에 법적 · 기술적 보안 요구사항을 반영함
- 입찰시 보안 요구사항에 대한 자체적인 보안성 점검기준을 마련하고, 이를 바탕으로 입찰 평가시 사업계획서를 검토하고 필요한 보안대책을 마련해야 함

정보보호 활동	세부 내용
1. 보안 요구 기준 마련	· 외주용역 추진에 있어서 제도, 정책, 지침 등에 따라 요구되는 정보보호 요구사항, 수준 등 기준을 마련하고 확인
2. 보안을 고려한 계약 체결	· 정보보호 요구사항이 반영된 사업자를 선정하고 미흡한 경우에는 기술협상 과정에서 정보보호 요구사항을 명확히 반영하여 계약 체결

1. 보안 요구 기준 마련

- 외주용역과 관련된 정보 및 시스템에 대한 보안위험을 파악하고, 적절한 통제 방안을 구상

[표 4-1] 외주용역 통제 기준

- 외부자가 접근 가능한 정보 및 정보처리 시설 식별, 접근 형태의 분석
- 접근 가능한 정보의 중요 가치, 사업에 미치는 영향
- 비 인가된 정보에 대한 접근제한을 위한 통제 방안
- 인가된 외부자의 식별 방법 및 승인 사항의 재확인
- 필요한 외부자의 접근 요구가 불가능할 경우 미치는 영향
- 침해사고 및 잠재적인 손실 발생시 외부자 접근 방안
- 외부자에게 제공하는 정보통신망 구성도, 세부 IP현황, 개인정보 등 중요 정보 보안대책
- 용역 직원의 노트북 등 장비 반출 · 입에 대한 보안조치
- 업무과정에서 생산되는 산출물 및 최종 산출물 보안 관리
- 위탁서비스 운영시 발생하는 보안사항의 위반 또는 침해사고 조치 방안

- 입찰공고 이전에 투입이 예상되는 자료, 장비 가운데 보안이 요구되는 사항에 대하여 관련 법령 및 자체 규정이 정하는 바에 따라 등급을 분류하고 필요한 보안요구기준을 마련

- 정보시스템을 위탁운영시에는 해킹에 대비해 관련 보안시스템이 구비되어 있는지 여부와 단순 운영 이외 보안관리가 가능한지 여부를 심층 검토

- 입찰공고시에 용역사업 관련 기밀유지 의무 및 위반시 불이익 등의 내용 사전 고지

- 제안서의 평가요소에 문서 · 시설 · 장비 등 보안관리 계획에 대한 평가항목 및 배점기준 마련

[표 4-2] 외주용역 보안관리 평가 기준

- 기밀보안 체계의 적정성
  - 기밀이 요구되는 정보에 대한 관리계획, 보안책임자의 의무사항 등이 정의된 문서에 대한 평가
- 기밀보안 대책의 확신성
  - 기밀이 요구되는 정보 관리시 비밀유지 의무조항, 책임소재 등 보안 대책에 대한 평가
- 보안통제를 위한 제반 사항 기술
  - 기밀이 요구되는 정보를 관리하기 위한 통제시스템 등 용역업체의 제반 사항에 대한 평가

- 외주업체가 입찰제안서에 제시한 용역사업 전반에 대한 보안관리 계획이 타당한지를 검토하여 사업자 선정시 이를 반영

- 사업추진에 적용되는 법 · 제도, 정책, 지침의 정보보호 요구사항 분석

[표 4-3] 사업추진시 정보보호 고려사항

- 정보화사업 추진목표 및 사업 특성분석을 통해 정보보호 적용여부 결정
- 정보화사업 추진에 관련된 법령, 훈령, 예규, 고시, 지침, 조직의 정책 등에서 정보보호 요구사항 도출
- 정보보호 요구사항 만족을 위한 정보보호 현황, 조직, 활용가능 자원 등의 정보보호 수행능력 점검

2. 보안을 고려한 계약 체결

- 용역사업 자체 또는 투입되는 자료 · 장비 등에 대한 대외보안이 필요한 경우 보안의 범위 및 책임을 명확히 하기 위해 사업수행 계약서와 별도로 비밀유지계약서를 작성

- 비밀유지계약서에는 비밀정보의 범위, 보안 준수사항, 위반시 손해배상책임, 지적재산권 문제, 자료의 반환 등이 포함되도록 명시

- 용역사업 참여인원은 용역업체 임의로 교체할 수 없도록 명시하고 신상변동사항 발생시 발주업체에 즉시 보고

- 발주업체의 요구사항을 사업자에게 명확히 전달하기 위해 작성하는 과업지시서에 자료 보안관리 방법, 인원 · 장비 · 시설 등에 대한 보안점검 · 교육 등 보안관련 제반사항을 상세히 기술

- 용역업체가 사업에 대한 하도급 계약을 체결할 경우 본 사업계약 수준의 비밀유지 조항을 포함토록 조치

- 기관의 정보 또는 정보처리시설에 대하여 외주용역 직원의 접근을 허용할 경우 기관의 보안 요구사항을 계약서 상에 명시

[표 4-4] 외주용역 시스템 접근시 보안요구사항

- 정보보호에 대한 절차 및 책임 명시
  - 기관의 자산에 대한 접근 절차
  - 기밀성, 무결성, 가용성에 대한 정보보호 방안
  - 계약 종료 시점의 정보자산의 반납 및 폐기
  - 외주용역 직원의 적격성 및 교육 훈련 보장
  - 정보시스템의 설치 및 유지보수에 대한 책임
  - 변경관리 절차 및 보고 체계
  - 정보시스템 접근방법, 권한 승인 절차의 통제
  - 계약 불이행 또는 침해사고 발생시 해결방안
- 발주업체의 용역업체에 대한 감사 권한 및 용역업체의 협조의무 명시
- 계약위반, 만기 전 해지 등에 따른 위약금 명시

제2절 개발 및 구축단계

IT 외주용역 과정 중에 발생할 수 있는 정보 유출 등 보안 위협 요소에 대한 보안 요구사항 도출 및 보안대책을 반영

- 개발 및 구축단계에서는 내부 중요정보 유출 방지를 위한 기술적 조치와 외주인력의 정보유출 방지를 위한 인력관리 대책을 마련해야 함

정보보호 활동	세부 내용
1. 자료에 대한 보안 관리	· 내부자료 관리 계획을 수립하여 내부정보 유출 방지
2. 사무실 · 장비에 대한 보안 관리	· 외주업체 사무실의 물리적 보안조치에 대해서 확인하고 외주인력이 반 · 출입하는 장비에 대한 보안관리 계획을 수립하고 이행
3. 내 · 외부망 접근 관리	· 외주인력의 내부시스템 접근에 대한 관리 및 외부망 접근 제어
4. 외주인력 신원조회	· 외주인력을 통한 정보유출을 막기 위해 보안서약서 작성 및 사전 신원조사 실시

1. 자료에 대한 보안관리

- 네트워크 구성도, IP현황, 개인정보 등 용역업체에 제공하는 비공개자료는 자료 관리대장을 작성하여 인계자(보안 책임자)와 인수자(용역업체 관리책임자)가 직접 서명한 후 인계 · 인수

[표 4-5] 자료관리대장 샘플

관리 번호	자 료 명	접수 일자	발행처	보관팀	배 포		폐 기		비고
					배포처	확인	내용	승인	

- 용역사업 관련자료 및 사업과정에서 생산된 모든 산출물은 발주업체의 파일서버에 저장하거나 보안책임자가 지정한 PC에 저장 · 관리

- 용역사업 관련자료는 인터넷 웹하드 등 인터넷 자료공유사이트 및 개인 메일함에 저장을 금지하고 전자우편을 이용해 자료전송이 필요한 경우 자체 전자우편을 이용, 첨부자료는 암호화 후 수 · 발신(단, 대외비 이상의 비밀은 전자우편으로 수발신 금지)

- 발주업체가 제공한 사무실에서 사업을 수행할 경우 제공한 비공개자료는 매일 퇴근시 반납토록 하며 비밀문서를 제외한 일반문서는 용역업체에 제공된 사무실에 시건장치가 된 보관함이 있을 경우 이에 보관 가능

- 용역사업 수행으로 생산되는 산출물 및 기록은 보안책임자가 인가하지 않은 비인가자에게 제공 · 대여 · 열람을 금지

- 정보시스템은 사용자별, 업무별 접근권한을 설정

- 입 · 출력 및 수정사항, 관련자의 시스템 데이터 접근 내역 등에 대한 기록 관리

2. 사무실 · 장비에 대한 보안관리

- 용역사업 수행 장소는 발주업체가 시건장치와 통제가 가능한 공간을 제공하거나 협의를 통해 동일한 환경이 구축된 외부 사무실을 사용

- 용역업체 사무실 또는 용역업무를 수행하는 공간에 대한 보안점검을 정기적으로 실시

- 발주업체 사무실에서 용역사업을 수행할 경우 용역 참여직원이 노트북 등 관련 장비를 반출 또는 반입시 악성코드 감염여부 및 자료 무단반출 여부를 확인

- 인가받지 않은 USB 등의 보조기억매체 사용을 금지하며 산출물 저장을 위해 보조기억매체가 필요한 경우 보안책임자의 관리하에 사용

[표 4-6] 용역업체 사무실 보안 점검항목

- 방재대책 및 외부로부터의 위해 방지대책
- 상시 이용하는 출입문은 한 곳으로 정하고 이중 잠금장치 설치
- 출입문 보안장치 설치 및 주야간 감시대책
- 보조기억매체를 보관할 수 있는 용기 비치
- 보조기억매체에 대한 안전지출 및 긴급파기 계획 수립
- 관리책임자 및 자료 · 장비별 취급자 지정 운용
- 전산 자료별로 접근권한을 제한
- 산출물 등 각종 자료는 업무에 따라 입력 · 출력 · 열람 등으로 제한
- 각종 자료의 열람은 필요에 따라 기본항목 · 전항목 등 범위를 제한

3. 내 · 외부망 접근 시 보안관리

● 용역사업 수행시 발주업체 전산망 이용이 필요한 경우 각 호의 사항을 준수

[표 4-7] 외주업체 전산망 접근시 보안요구사항

- 사업 참여인원에 대한 사용자 계정(ID)은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 부여
- 계정별로 부여된 접속권한은 불필요시 곧바로 권한을 해지하거나 계정을 폐기
- 참여인원에게 부여한 패스워드는 보안책임자가 별도로 기록 관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력 확인
- 보안책임자는 서버 및 장비 운영자로 하여금 내부서버 및 네트워크 장비에 대한 접근기록을 매일 확인하여 이상유무 보고
- 용역업체에서 사용하는 노트북PC는 인터넷 연결을 금지, 다만 사업 수행상 필요한 경우에는 용역업체의 관리책임자가 직접 요청하고 보안책임자는 필요성이 인정될 경우 접속할 노트북을 지정하고 필요한 사이트에만 접속토록 방화벽 등을 통해 통제 후 사용

[표 4-8] 원격접속 관리 대장 샘플

사용자명	서버명	원격접속 계정(ID)	접속시 비밀번호	접속주소	접속사유	접속시간	관리자 조치사항	확인

※ [부록 4-3] 외주인력 ID 신청서 참조

- 발주업체 및 용역업체 전산망에서 P2P, 웹하드 등 인터넷 자료공유 사이트로의 접속을 방화벽 등을 이용해 원천 차단

4. 외주인력 신원확인

- 용역사업 참여인원에 대해서는 각 개인의 친필 서명이 들어간 보안서약서를 징구

※ [부록 4] 영업비밀보호 서약서 참조

- 용역사업 수행전 참여인원에 대해 법적 또는 발주업체 규정에 의한 비밀유지 의무 준수 및 위반시 처벌내용 등에 대한 보안교육 실시

제3절 사업 완료 단계

IT 외주용역 사업 완료 시 발생 하는 보안 위협 요소에 대한 보안 요구사항 도출 및 보안대책을 반영

- 사업 완료 시 최종결과물 및 사업 중 사용된 장비, 자료의 외부 유출을 방지하기 위하여 자료의 수거 및 처리 방법에 대한 대책을 마련함

정보보호 활동	세부 내용
1. 사업 완료 시 보안 대책	· 사업 완료 후 최종 산출물 중 보안이 요구되는 자료의 유출방지를 위해 보호 조치를 실시

1. 사업 완료 시 보안 대책

- 사업완료 후 생산되는 최종 산출물 중 대외보안이 요구되는 자료는 대외비로 작성 · 관리하고 불필요한 자료는 삭제 및 세단 후 폐기

- 용역업체에 제공한 제반자료, 장비, 서류와 중간 · 최종 산출물 등 용역과 관련된 제반자료는 전량 회수하고 업체에 복사본 등 별도보관을 금지

- 노트북 · 보조기억매체 등 전자적으로 기록된 자료는 '정보시스템 저장매체 불용처리 지침'에 따라 보안조치

[표 4-9] 정보시스템 저장매체 불용처리 지침

저장매체 \ 저장자료	공개자료	민감자료 (개인정보 등)	비밀자료 (대외비 포함)
플로피디스크	㉮	㉮	㉮
광디스크	㉮	㉮	㉮
자기 테이프	㉮, ㉯ 중 택일	㉮, ㉯ 중 택일	㉮, ㉰ 중 택일
반도체메모리 (EEPROM 등)	㉮, ㉰ 중 택일	㉮, ㉰ 중 택일	㉮, ㉰ 중 택일
	완전포맷이 되지 않는 저장매체는 ㉮방법 사용		
하드디스크	㉱	㉮, ㉯, ㉰	㉮, ㉯

㉮ **완전파괴(소각, 파쇄, 용해)**
비밀이 저장된 플로피디스켓. 광디스크 파쇄시에는 파쇄조각의 크기가 0.25mm 이하가 되도록 조치

㉯ **전용 소자장비 이용 저장자료 삭제**
소자장비는 반드시 저장매체의 자기력보다 큰 자기력 보유

㉰ **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

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

※ [부록4-5] 투입 종료 확인서 참조

제4절 유지 보수 단계

IT 외주용역을 통한 유지 보수 단계에서 발생할 수 있는 위협 요소에 대한 보안 요구사항 도출 및 보안대책을 반영

- 정보시스템 운영위탁 및 유지보수 단계에서 발생할 수 있는 시스템 불법 접근 등에 대한 대책마련과 접근방법에 대한 대책을 마련함

정보보호 활동	세부 내용
1. 정보시스템 위탁 운영시 보안 대책	· 정보시스템을 위탁운영 시 발생할 수 있는 사고에 대한 보호 조치를 실시

1. 정보시스템 위탁 운영 시 보안 대책

- 위탁업체에게 정보시스템을 위탁하여 운영할 때에 위탁업체에게 다음 사항이 포함된 정보시스템 위탁운영계획서를 제출하여 받아 사전 검토

[표 4-10] 정보시스템 위탁운영계획서 포함사항

- 위탁개요(위탁내용, 위탁업체 · 비용 · 기간, 운영인력 등)
- 정보통신망 구성현황 및 보안대책(보안체계의 세부내역 포함)
- 위탁시스템의 개인정보 보유현황 및 보호대책
- 운영효율 향상 및 서비스 개선 방안(기반시스템 공동활용, 서비스수준협약서 등)
- 위탁운영비 세부산출 내역
- 위탁시스템에 대한 향후 추진계획(시스템 고도화 등)
- 기타 보안 대책

- 위탁업체가 위탁 받아 운영하고 있는 정보시스템의 보안성 점검을 위한 다음 사항의 시행을 정기적 감사 실시

[표 4-11] 위탁 정보시스템 보안성점검 항목

- 위탁시스템에 대한 정보통신 보안 및 개인정보보호 관리 실태
- 기반시스템 공동 활용현황, 서비스수준협약서 준수사항 등 효율적 운영 및 서비스 개선상태
- 위탁비용의 적절성
- 기타 위탁계약의 이행사항 등 위탁에 따른 전반적인 사항

5

제5장 IT 외주인력 통제 강화 대책

5 제5장 IT 외주인력 통제 강화 대책

● 이번 장에서는 IT 외주인력 통제 강화를 위한 물리적, 관리적, 기술적 대책을 제시함

이번 장에서는 외주인력으로 인한 내부정보 유출 등 보안위협을 통제하기 위해 고려해야 할 정보보호 실행지침을 제시하되, 크게 ①물리적 대책, ②인적보안관리, ③관리적 대책, ④ 기술적 대책 등 4단계로 구분한다.

제1절 물리적 대책

◆ IT 외주인력이 중요정보가 보관된 장소에 대한 접근 통제와 같은 물리적 보안 대책

정보보호 활동	세부 내용
1. 물리적 접근통제	· 외주인력의 정보시스템, 정보보관소 접근 통제 · 필요시 접근 유형 및 접근 사유 파악 · 제한구역, 접견구역, 장비출하구역 등을 구분하여 보안조치와 절차 수립
2. 출입이력 관리	· 출입이력 관리대장 사용 · 접근통제의 방법과 범위 등을 문서화
3. 이동매체 반 · 출입통제	· 반 · 출입되는 이동매체에 대한 파악 · 이동매체 반 · 출입 과정의 문서화 · 반 · 출입되는 이동매체의 보안검사

1. 물리적 접근 통제

IT 외주인력이 중요정보 보관장소에 접근시 접근통제 등 물리적 보호대책 적용

- IT 외주인력의 업무에 불필요한 곳에 접근하거나, 정보시스템이 운영되고 있는 곳에 침입하여 중요 정보 유출
- IT 외주인력이 정보유출을 목적으로 허가받지 않은 장소에 접근하거나, 중요한 시스템이 운영되고 있는 장소 혹은 정보시스템이 운영되고 있는 장소에 침입하여 중요정보 유출 가능성이 존재

- 실행 지침

  - 보호 필요시설 및 장비에 대한 권한 없는 자의 물리적 접근 및 각종 물리적, 환경적 재난으로부터 보호하기 위한 보호구역 정의 및 이에 따른 보안대책 수립

  - 제한구역, 접견구역, 장비출하구역 등을 별도로 지정하여 각각에 적합한 보안 조치와 절차 수립

[표 5-1] 접근통제 절차에 포함되는 사항

- 물리적 보호구역의 중요도에 따라 접근통제 정도의 명시
- 접근통제 방법 명시(카드 센서 장치, IC카드, 광카드, 출입관리장치, 암호 입력장치, 생체인식 장치 등)
- 정보시스템 및 중요시설에 대한 물리적 접근통제 방법 기록

  - IT 외주인력의 정보시스템 혹은 정보 보관소에 대한 접근을 통제하고 업무상 불가피한 접근 허용 시 접근 유형 및 접근 사유를 파악하고 위험 요소를 고려하여 출입을 허가

[표 5-2] IT 외주인력의 보안구역 출입시 고려사항

- 보안구역 출입시 책임자의 사전승인
- 내부 직원이 동행하여 출입 및 작업내용을 직접 관리감독
- 출입내역(출입목적, 출입자, 입 · 퇴실 시각, 작업내용 등)의 기록
- 출입내역 기록의 책임자에 의한 정기적 또는 비정기적 점검

● 필수/선택사항

(○ : 필수사항, △ : 선택사항)

세부 지침	용역유형	
	상주	비상주
보호구역 정의 및 이에 따른 보안대책 수립 및 이행	○	△
제한구역, 접견구역, 장비출하구역 등을 별도 지정	△	△
IT외주 인력의 정보시스템 혹은 정보 보관소에 대한 접근 통제	○	○

2. 출입이력 관리

IT 외주인력의 출입통제지역 출입시 이력관리와 같은 물리적 보호대책 적용

- IT 외주인력의 출입통제 내역을 관리하지 않아 중요정보에 불법적인 접근 위협
- IT 외주인력이 중요정보 및 정보시스템에 접근하는 내역을 관리하지 않아 중요정보가 유출되거나 중요시스템에 피해가 발생했을 때, 책임에 대한 배상을 요구할 수 없음

● 실행 지침

- 외주인력이 업무 수행을 목적으로 보안구역에 출입할 때 출입내역 관리 대장과 같은 출입내역을 확인할 수 있는 대책 수립

■■■ [표 5-3] 출입이력 관리방안

- 접근통제가 요구되는 업무를 정의하고, 이 업무에 대한 접근통제의 방법과 범위 등을 문서화
- 외부인 출입 시 출입자, 출입시간, 출입목적에 대한 내용을 기록하고 관리
- 출입자 기록의 재검토(시설 보안등급에 따른 출입자 권한, 출입 목적, 출입시간의 적정성)

■■■ [표 5-4] 출입이력 관리대장

연월일	출입 시간	용무	출입자		입회자		비고
			소속	성명	직급	성명	

● 필수/선택사항

(○ : 필수사항, △ : 선택사항)

세부 지침	용역유형	
	상주	비상주
접근통제 요구 업무의 정의 및 접근통제 방법과 범위 문서화	○	△
출입자, 출입시간, 출입목적의 기록 · 관리 및 재검토	○	○

3. 이동매체 반 · 출입 통제

IT 외주인력이 반 · 출입하는 이동매체에 대한 물리적 보호대책 적용

- IT 외주인력이 반입하는 이동매체의 악성코드 감염 및 중요정보를 이동매체에 저장하여 반출하여 중요정보의 유출 위협
- IT 외주인력이 반입하는 이동매체에 악성코드가 감염되어 내부 시스템에 피해를 입히거나, 내부 중요정보를 이동매체에 저장하여 반출하는 경우 중요정보가 유출되는 위협이 존재

● 실행 지침

- 내부에서 사용중인 이동매체의 관리 방안 마련

■■■ [표 5-5] 내부 사용 이동매체의 관리 방안

– **(관리자 지정)** 보조기억매체 관리책임자 및 정보보안담당관 지정
  · 관리책임자 : 관리대장 등록현황 유지, 수량 및 보관상태 점검, 반출입 통제, 사용 감독 등
  · 정보보안담당관 : 관리기관의 보조기억매체 등록 현황 파악, 보조기억매체 라벨 작성, 미등록 매체에 업무자료 보관 및 비밀보관 매체의 무단반출 인지시 경위조사 · 조치
– **(매체 도입절차)** 보조기억매체 도입시 국정원 보안적합성 검증을 거친 제품을 도입
  ※ 검증기준 : 사용자 식별 · 인증, 저장데이터 암 · 복호화, 임의 복제 방지, 분실에 대비한 삭제 기능
– (매체 관리) 보조기억매체는 관리대장에 등재후 사용
  · 보조기억매체는 일반용, 비밀용(대외비용), 공인인증서 보관용으로 구분하여 사용 · 관리
– **(사용제한)** 보조기억매체는 업무목적 이외 사적인 용도로 임의 사용을 제한하고 주기적인 점검 실시
– **(불용처리 및 재사용)** 불용처리시 물리적 파기후 관리대장에 기록 · 관리하고, 용도를 전환하여 재사용시 파일 삭제, 포맷 및 파일복원 방지대책 강구
– **(분실시 대처 방안)** 관리책임자 및 정보보안담당관에게 즉시 통지하고, 경위 조사를 통해 재발방지 대책 강구
– **(고장 · 훼손, 오인 삭제시 대처방안)** 불용처리를 원칙으로 하나, 자료 복구 필요시 전문업체 의뢰 가능
  ※ 전문업체 의뢰시 보안서약서 징구 등 보안대책 강구

■■■ [표 5-6] USB에 의한 웜 · 바이러스 감염대책

– **(접속포트 봉인)** 저장 매체 사용이 필요없는 경우 매체 접속 포트를 봉인하여 바이러스 등 악성코드의 원천 차단
– **(백신프로그램 사용)** 저장매체 사용시 최신 패치된 백신 프로그램으로 웜 · 바이러스 유무를 검사
– **(악성코드 자동실행 차단)** USB 저장매체에서 악성코드 자동 실행 차단용 보안프로그램 설치 · 사용
  ※ 국가정보원에서 'USB Guard' 배포('07.12)

- 외주인력이 반출 · 입하는 이동매체 제한 및 관리를 위한 절차 수립

  · 외주인력이 반출 · 입하는 이동매체의 보안 검사 수행

  · 이동매체의 반출 · 입이 요구되는 업무가 정의되어 있고, 이 업무에 대한 반출 · 입의 방법과 범위 등을 문서화

[표 5-7] USB 등 이동매체 반출입 절차

● 필수/선택사항

(○ : 필수사항, △ : 선택사항)

세부 지침	용역유형	
	상주	비상주
반출 · 입 이동매체 관리	○	○
외주 인력 반출 · 입 이동매체 제한 및 관리절차 수립	○	△

제2절 인적보안관리

◆ IT 외주인력 통제를 위한 외주인력 신원확인 등과 같은 인적보안관리

정보보호 활동	세부 내용
1. 상주 유지보수인력 신원확인	· 외주인력의 사전 신원확인 · 보안서약서 작성 · 보안의식 강화를 위한 보안교육 실시
2. 현장 동행	· 보안구역 출입관리 대장 · 외부인이 출입제한 구역에 출입할 경우 보안관리자와 동행

1. 상주유지보수 인력 신원확인

정보시스템의 안정성과 보안성이 유지될 수 있도록 하기 위한 상주유지보수 인력의 신원확인과 같은 인적보안관리 대책 적용

- 업무에 적합하지 않은 상주유지보수 인력배치로 인한 내부시스템의 취약점 발생 및 중요정보 유출
- IT 외주인력 중 업무에 적합하지 않은 인력이 상주유지보수 인력으로 배치되어 내부 시스템에 취약점을 발생시키거나 내부 중요정보 유출 위협 존재

- 실행 지침

  - 상시유지보수 인력으로 배치되는 인력에 대한 사전 신원확인을 시행하여 업무를 수행하는데 적합한 인력인지를 사전에 확인

- 상시유지인력의 보안인식 강화와 내부 중요정보에 대한 보호를 위해 보안서약서 작성 및 보안교육 실시

[표 5-8] 보안서약서 주요내용

- 정보보호 관리유지를 위한 협조
- 정보보호규정 및 세칙준수
- 비밀분류기준에 의거한 연구관련 자료관리/보관
- 비밀자료관리 및 유출금지
- 전산저장매체 관리
- 개인전산저장매체 반입금지
- 정보보호 및 비밀유지에 관한 제반사항 서약

[표 5-9] 보안서약서 샘플

보 안 서 약 서

_____(이하 '회사')의 업무를 수행하는 협력회사, 상주파견 업체, 기타 외부업체 직원들은 본 서약서가 근무기간뿐 아니라 파견해제 후에도 일정기간 적용될 수 있음을 인식하고 숙독하신 후 서명하기 바랍니다.

1. 나는 회사로부터 취득한 모든 정보를 회사 관련 업무에 한해 이용할 것이며, 타기업의 보호대상 정보를 회사 내 보관치 않겠다.

2. 나는 회사로부터 제공받은 정보자산(서류, 사진, 전자파일, 저장매체, 전산장비 등)을 무단변조, 복사, 훼손, 분실 등으로부터 안전하게 관리하겠다.

3. 나는 상대가 누구이건 간에(회사직원, 고객 혹은 계약직 사원 등) 알 필요가 없는 자에게 회사 혹은 제3자의 소유정보를 누설하지 않겠다.

4. 나는 명백히 허가 받지 않은 정보나 시설에 접근하지 않으며, 회사관련 업무를 수행할 때만 사내 데이터 처리시설을 이용하고, 이 시설 내에 사적 정보를 보관치 않겠다.

5. 나는 회사에서 승인 받지 않은 프로그램, 정보저장 매체(USB, Zip Drive, CD-ROM, 외장 HDD 등)을 회사 내에서 사용치 않겠다.

6. 나는 회사소유 정보자산을 외부로 발신 시 회사의 통제절차를 준수할 것이며, 회사가 정보 자산을 보호하기 위해 회사통신망을 통해 수 발신되는 전자문서를 점검할 수 있음을 알고 있다.

7. 나는 업무와 관련한 문서의 생성, 사용, 폐기시 문서권한 관리 규칙에 의거 규정을 준수하겠다

8. 나는 나에게 할당된 사용자 ID, 패스워드, 출입증을 타인과 공동사용 또는 누설치 않겠다.

9. 나는 회사의 정보보호 정책 및 지침, 절차를 준수하겠다.

10. 나는 회사에서 나의 수행 업무와 관련되어 감사를 시행하는 경우 이에 적극 협조하겠다.

11. 나는 퇴직(프로젝트 종료, 파견 해제) 시 회사에서 제공받은 회사소유 모든 정보자산을 반드시 반납할 것이며, 이후에도 회사의 모든 영업비밀은 물론이고 기타 누설됨으로 인하여 회사에 손해가 될 수 있는 각종 정보에 대하여는 이를 일절 누설치 않겠다.

상기사항을 숙지하고 이를 성실히 준수할 것을 동의하며 서약서의 보안사항을 위반하였을 경우에는 "부정경쟁방지 및 영업비밀보호에 관한 법률" "정보통신망이용촉진 및 정보보호 등에 관한 법률" 등 관련법령에 의한 민/형사상의 책임이외에도, 회사의 사규나 관련 규정에 따른 징계조치 등 어떠한 불이익도 감수할 것이며 회사에 끼친 손해에 대해 지체 없이 변상/복구할 것을 서약합니다.

20 년 월 일
관 리 부 서 :
소 속 :
부 서 장 : (서명)
주 민 번 호 :
이 름 : (서명)

● 필수/선택사항

(○ : 필수사항, △ : 선택사항)

세부 지침	용역유형	
	상주	비상주
상시유지보수 인력에 대한 사전 신원조회를 시행	○	○
보안서약서 작성	○	○
보안의식 강화를 위한 보안교육 실시	○	△

2. 현장 동행

IT 외주인력의 이동 및 행동에 대한 인적 보안 대책

- IT 외주인력이 업무에 불필요한 곳에 접근하거나, 정보시스템이 운영되고 있는 곳에 침입하여 중요 정보를 유출
- IT 외주인력이 정보유출을 목적으로 허가받지 않은 장소에 접근하거나, 중요한 시스템이 운영되고 있는 장소 혹은 정보시스템이 운영되고 있는 장소에 침입하여 중요정보를 유출

● 실행 지침

- 유지보수를 위한 외주업체 직원의 출입 또는 기타 부득이한 사유로 출입이 필요할 경우 내부 인가자의 동행 하에 출입

- 출입자는 보안구역 출입관리 대장에 신분, 목적 및 입실/퇴실 시간을 기록

● 필수/선택사항

(○ : 필수사항, △ : 선택사항)

세부 지침	용역유형	
	상주	비상주
인가자의 동행 하에 출입	○	○
출입관리 대장에 신분, 목적 및 입실/퇴실 시간을 기록	○	○

제3절 관리적 대책

◆ 정보시스템과 연관되어 있는 인원, 조직, 기술상에 대한 전반적이고 총체적인 보안대책

정보보호 활동	세부 내용
1. 작업내역 관리	· 외주인력의 내부시스템 접근 기록 상시 감독 · 저장매체 사용 방지를 위한 조치 실시
2. 시스템 접근권한 관리	· 시스템 접근 라벨 정의 및 접근권한 개별 부여
3. 정보 시스템 관리	· PC 등과 같은 장비의 반입 전 초기화/점검 실시 · 보안SW 설치 · 외주인력에 대한 보안정책 수립 및 이행
4. 조직체계 정비 및 검사	· 용역업체의 보안 관리 계획 평가 · 입찰공고 이전에 투입 예상 자료 · 장비의 보안 요구기준 마련

1. 작업내역 관리

IT 외주인력의 작업 결과물과 같은 작업내역 관리

- IT 외주인력의 작업 중 불필요한 저장 등을 통한 중요정보 유출 위협
- IT 외주인력이 중요정보 유출을 목적으로 작업 수행의 결과물을 저장/보관함으로써 통해 중요정보가 외부로 유출 될 가능성이 존재

- 실행 지침

  - 외주인력이 외주업무의 목적을 달성하기 위해 내부시스템 접근을 득한 경우 외주인력의 내부시스템 접근기록을 상시 감독하여 불법적인 접근을 방지

  - 외주인력이 인 · 허가 받지 않은 저장매체를 이용하여 내부정보를 외부로 유출하는 것을 방지하기 위해 저장매체 반입을 제한하고, 매체기록장치를 봉인

- 필수/선택사항

(○ : 필수사항, △ : 선택사항)

세부 지침	용역유형	
	상주	비상주
외주인력의 내부시스템 접근 기록 상시 감독	○	○
저장매체 반입 제한	○	○
매체기록장치를 봉인	○	○

2. 시스템 접근권한 관리

IT 외주인력의 시스템 접근권한 관리와 같은 관리적 보안대책 적용

- IT 외주인력이 시스템에 접근권한이 없는 정보에 접근 및 중요정보 유출 위협
- IT 외주인력이 중요정보 유출을 목적으로 허가받지 않은 정보에 접근을 시도하거나, 접근에 성공하여 중요정보를 유출

- 실행 지침

  - 정보시스템에 접근할 수 있는 레벨을 사전에 설정하고 정보시스템 접근목적에 따라서 접근권한을 개별 부여

[표 5-10] 정보시스템 접근 레벨

– 단순방문 : 담당자 면담 등 단순방문으로 정보시스템 반입을 사전 차단

현업담당자 신청 요청 → 보안SITE 접속 → 메인화면 내방객 신청 → 부서장 결재 → 입문

– 네트워크 접근 필요 : 단기간의 업무수행을 위해 네트워크 접속이 필요한 경우로써 보안이 되어있는 내부 장비 및 장소를 통해 업무 수행 유도

– 장기간 상주 : 내부직원과 동일한 보안 조건으로 보안정책 적용, 업무완료 후 자료 유출 위험이 존재하므로 자료 삭제 절차 수행

장기출입 신청서 작성 → 관리자결재 → 현업 담당부서 합의 → 사원증 담당자 제출 → 사원증 발급 (신분증 지참)

● 필수/선택사항

(○ : 필수사항, △ : 선택사항)

세부 지침	용역유형	
	상주	비상주
정보시스템 접근목적에 따른 접근레벨 정의	○	○

3. 정보시스템 관리

IT 외주인력이 사용하는 정보시스템에 악성코드 감염 예방 등 관리적 보호대책 적용

- IT 외주인력이 악성코드에 감염된 장비 사용으로 인해 중요정보 유출
- IT 외주인력이 사용하는 장비에 대해서 악성코드 감염 등과 같은 사전 검열 작업을 수행하지 않아 악성코드를 통해 내부 망에 침입하여 중요정보를 유출하거나 내부 시스템에 치명적 오류를 발생

● 실행 지침

- **(정보 시스템 통제)** PC 등과 같은 장비의 반입 전 초기화(포맷)를 원칙으로 하나, 초기화가 어려운 경우 외주인력은 반드시 PC점검 실시 후 사용

[표 5-11] PC 보안점검 주요내용

- 외주인력이 사용하는 PC에 사내표준 보안SW를 설치하며 외주인력 임의로 삭제 및 기능 종료 금지
- 백신 프로그램은 주기적으로 업데이트하여 최신 버전을 유지하며, 정보시스템 가동 시 백신 프로그램이 자동으로 실행
- 외주인력에 대한 보안정책을 수립하고 업무에 의해 보안정책 변경이 필요한 경우 이를 보안 담당자가 확인

※ [부록 5-2] PC 보안점검표 참조

※ [부록 5-3] 보안 정책변경 요청서 참조

- 보안교육 실시

[표 5-12] 외주용역 교육컨텐츠

- PC 등과 같은 장비의 보안 정책을 설명하고 주지시켜 안전한 장비 사용 도모
- 비인가 PC 사용 금지
- 보안 설정 준수
- 비인가 소프트웨어 설치 금지
- 비인가 사이트 접속 금지
- 외부 반출입 절차
- 공유폴더 설정 금지 등 공유정책 준수
- 반출시 노트북 자료 완전 삭제(포맷 등)

● 필수/선택사항

(○ : 필수사항, △ : 선택사항)

세부 지침	용역유형	
	상주	비상주
정보 시스템 통제	○	○
보안 교육	○	△

4. 조직체계 정비 및 감사

IT 외주인력에 대한 관리와 감사를 통한 관리적 보호 대책

- IT 외주인력에 대한 감사를 실시하지 않아 중요정보 유출의 가능성 존재
- IT 외주인력에 대한 체계적인 관리 계획이 존재하지 않아 IT 외주인력의 정보시스템 불법접근, 정보유출을 시도하여도 빠른 파악이 불가능

- 실행 지침

  - 보안 관리 계획 마련

[표 5-13] 보안관리 계획

- 제안서의 평가요소에 문서 · 시설 · 장비 등 보안관리계획에 대한 평가항목 및 배점기준 마련하고 제안요청서 작성 시 용역(아웃소싱)업체에 프로젝트 과정에 대한 보안 관리 계획을 요구
- 프로젝트 보안관리 계획은 계약서 상에 명시되거나 첨부

[표 5-14] 보안 요구 기준

- 입찰공고 이전에 투입이 예상되는 자료, 장비 가운데 보안이 요구되는 정보에 대하여 적정 보호등급으로 분류하여 보안요구기준 마련
- 웹호스팅 등 정보시스템을 위탁운영 시에는 해킹에 대비해 웹방화벽 등 관련 보안시스템이 구비되어 있는지 여부와 단순 운영 이외 보안관리가 가능한지 여부를 검토
- 내부시스템 이용시간, 작업지역을 제한하여 접근통제를 실시
- 용역(아웃소싱)업체가 제시하는 자체 통제방법에 대하여 소속업체는 이를 평가하고 채택여부 등을 결정하며 필요시 추가적인 통제방안을 요구

● 필수/선택사항

(○ : 필수사항, △ : 선택사항)

세부 지침	용역유형	
	상주	비상주
보안관리 계획 수립	○	△
보안 요구기준 마련	○	△

제4절 기술적 대책

◆ IT 외주인력 통제를 위한 접근 통제와 저장 매체 통제 등의 기술적인 대책

정보보호 활동	세부 내용
1. 접근관리	· 내부시스템에 접근하여 수행한 작업 등을 확인할 수 있는 접근이력 관리 시스템 운영 · 내부 시스템에 접근 시 두 가지 이상의 방법으로 사용자 인증 · 내부 시스템에 접근하는 기기에 대해 사전 점검
2. 출력물 유출방지	· 비공개 자료 출력 시 출력자, 출력일시 등을 기록
3. 네트워크 제한	· 외부망과 물리적 분리 · 내부 운영 시스템 별 논리적 망 분리 운영 · 네트워크를 통한 통신 시 암호화 적용
4. 반 · 출입 매체관리	· 반 · 출입매체의 악성코드 검사 · 외주업무의 특성에 따라 반 · 출입매체의 제한/점검

1. 접근관리

접근이력 관리를 통한 IT 외주인력이 불법적인 접근여부를 감시

- IT 외주인력이 허가받지 않은 시스템 혹은 접근허가가 만료된 이후에 시스템에 접근하여 중요정보 유출 위협
- IT 외주인력이 허가받지 않은 방법 혹은 기기로 내부시스템에 접근하여 중요정보 유출 위협

- 실행 지침

  - 접근이력 관리시스템 운영

  - 내부시스템에 접근하여 수행한 작업 등을 확인할 수 있는 접근이력 관리 시스템의 감사 기록은 다음항목을 포함

[표 5-15] 접근이력 관리시스템 기능

- 사용자 ID
- 핵심 이벤트 일자, 시간, 기타 상세 정보
- 시스템 접근 시고의 성공과 거부 기록
- 데이터 및 기타 자원 접근 시도의 성공과 거부 기록
- 시스템 구성의 변경
- 권한의 사용
- 시스템 유틸리티와 어플리케이션의 사용
- 접근된 파일의 접근 유형
- 네트워크 주소와 프로토콜
- 접근 이력 관리시스템에 의해 제기된 경고
- 바이러스 탐지 시스템 및 침입탐지시스템과 같은 보호시스템의 활성화 및 비활성화

- 내부 시스템에 접근하는 사용자에 대한 인증을 위해 두 가지 이상의 방법으로 사용자 인증을 수행

- 시스템 접속기기 검증

[표 5-16] 시스템 접속기기 검증 내역

- 내부 시스템에 무분별한 접근을 방지하기 위하여 시스템 접속기기에 대한 검증을 수행
- 외부에서 내부 시스템에 접근하는 경우 접근목적에 따라서 내부 감독자의 허가를 득하고, 접근하는 IP를 통제하는 등과 같은 시스템 접속기기에 대한 검증을 수행

● 필수/선택사항

(○ : 필수사항, △ : 선택사항)

세부 지침	용역유형	
	상주	비상주
접근이력 관리시스템 운영	○	○
사용자 인증 관리	○	△
시스템 접속기기 검증	△	△

2. 출력물 유출 방지

중요정보가 인쇄된 출력물을 IT 외주인력이 불법적으로 반출하는 것을 방지하기 위한 보호대책 적용

● IT 외주인력이 중요정보가 인쇄된 출력물을 외부로 유출

● IT 외주인력이 내부 중요정보가 인쇄되어 있는 출력물을 외부로 유출 시켰을 때, 워터마크 등과 같은 유출방지 시스템이 미적용되어 유출경로 파악 및 사후대책이 불가능

● 실행 지침

- IT 외주인력에게 제공한 출력물 관리

- 비공개자료 출력 시에는 출력물에 출력자, 출력일시 등을 표시

[표 5-17] 출력물 관리대장

번호	자료명	제공형태		제공자 (부서/ 담당자)	수령자	수령 일자	반납 기한	반납 일자	용도	비고
		Hard	Soft							

- 외주인력의 데이터 출력물에 대한 자동화 된 시스템에 의한 로그 및 감사 기능 구축

● 필수/선택사항

(○ : 필수사항, △ : 선택사항)

세부 지침	용역유형	
	상주	비상주
IT 외주인력에게 제공한 출력물 관리	○	○

3. 네트워크 제한

IT 외주인력의 네트워크 접근 제한 등과 같은 보안 대책

- IT 외주인력의 업무 수행 중 불필요한 네트워크 접속으로 인한 악성코드 감염 및 중요 정보외부 유출 등의 위협
- IT 외주인력이 업무수행 중 공개망에 접속하여 악성코드에 감염되어 내부 시스템의 취약점 발생 및 악의적 목적으로 내부정보를 공개망을 통해 외부에 유출되는 위협이 존재

- 실행 지침

  - 물리적 망 분리 운용

    · 네트워크관리자는 비밀을 취급하는 네트워크를 외부망과 분리 운용

    · 내부망과 외부망 연동 시 효율적인 보안관리를 위하여 연결지점을 최소화 운용

  - 논리적 망 분리 운용

    · DMZ, 인터넷서비스망, 업무전산망, PC 영역 등의 영역으로 분리

    · PC, 서버, 데이터 등 정보시스템을 물리적으로 분리된 인터넷 서비스망과 업무전산망 영역으로 분리

    · 홈페이지 및 공개 서버의 경우는 내부 네트워크와 분리하여 DMZ에 구성

    · 외주인력 등을 활용할 경우에는 내부 네트워크와 분리된 네트워크로 구성

- 데이터 통신 보안

  · 네트워크상에서 이루어지는 통신을 안전하고 신뢰할 수 있도록 하기 위하여 통신 내용에 대한 암호화 적용

● 필수/선택사항

(○ : 필수사항, △ : 선택사항)

세부 지침	용역유형	
	상주	비상주
물리적 망 분리 운용	○	△
논리적 망 분리 운용	○	△
데이터 통신 보안	○	△

4. 반출 · 입 매체관리

IT 외주인력이 반출 · 입하는 장비 및 매체에 대한 보호대책 적용

- IT 외주인력이 반출 · 입하는 매체에 악성코드 감염되어 내부시스템에 오류 발생 및 취약점 발생 위협
- IT 외주인력이 내부 정보를 허가 없이 저장매체에 저장하여 외부로 반출

● 실행 지침

- 반출 · 입매체의 악성코드 검사

  · IT 외주인력이 내부에 반출 · 입하는 매체의 악성코드 감염 여부를 검사

- 반출 · 입매체의 통제

  · IT 외주인력의 업무에 불필요한 매체에 대한 압수 보관

  · IT 외주인력이 반출하는 저장매체의 내부에 저장된 자료 검사

- 이동매체 제한 및 관리를 위한 자동화 된 시스템 도구의 도입

● 필수/선택사항

(○ : 필수사항, △ : 선택사항)

세부 지침	용역유형	
	상주	비상주
반출 · 입매체의 악성코드 검사	○	○
반출 · 입매체의 통제	○	○
이동매체 제한 · 관리를 위한 자동화 된 시스템 도입	○	○

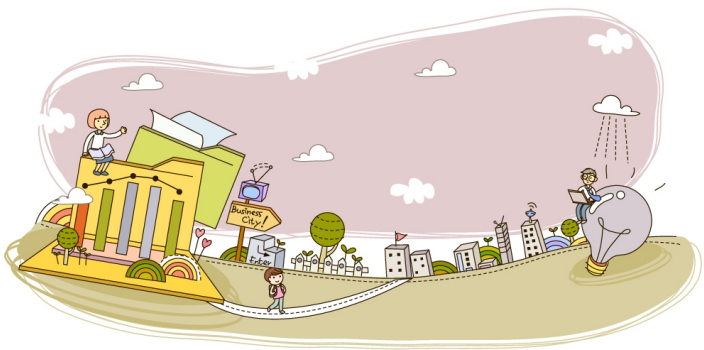
IT 외주용역 유형별 보호대책

[필수 : ○, 옵션 : △, 해당사항 없음 : ×]

외부용역의 유형		물리적 대책			인적 보안 관리		관리적 대책				기술적 대책			
		접근 통제	출입이력관리	이동매체 통제	신원조회	현장 동행	작업내역 관리	접근 권한 관리	정보 시스템 관리	조직체계 관리	접근 관리	출력물 관리	네트워크 제한	매체 관리
1	운영 용역	○	△	○	○	△	○	○	○	○	○	○	○	○
2	유지 보수 용역	○	○	○	○	○	○	○	○	○	○	○	○	○
3	SI 용역	○	△	○	○	△	○	○	○	○	○	△	○	○
4	데이터 처리 용역	×	×	×	×	×	○	○	○	○	○	○	○	○
5	오프라인 지원	×	×	○	○	×	○	△	○	○	×	○	△	△

샘플

IT 외주용역 정보보호 관리지침(샘플)



제1장 총 칙

제1조(목적) 이 지침은 OOOO 정보자산을 용역에 의해 개발 및 관리 · 운영할 경우 정보보호에 필요한 체계적 지침 및 표준을 제시하는 것을 목적으로 한다.

제2조(적용범위) ① 이 지침은 OOOO의 용역(아웃소싱) 관리 및 보안관리 업무와 관련된 업무종사자에 적용함을 원칙으로 하며, OOOO와 계약관계에 있는 업체 및 기타 업무상 조정 통제를 받는 단체의 임직원에게도 적용할 수 있다.

② 이 지침에서 정하는 용역(아웃소싱)의 범위는 정보시스템 개발 및 컨설팅 및 운영 용역(아웃소싱)에 적용한다.

제2장 프로젝트 보안관리

제3조(프로젝트관리자의 역할 및 권한) ① 프로젝트관리자의 역할은 다음 각호와 같다.

1. 프로젝트의 기본사항 파악 및 정의
2. 프로젝트 관리에 대한 계획 수립
3. 업체선정을 위한 제안요청서 발송 및 제안서 접수
4. 단계별 점검항목 선정
5. 일정 및 산출물 관리
6. 인원관리
7. 프로젝트계획서에 대한 변경 및 통제작업

② 프로젝트관리자의 권한은 다음 각호와 같다.

1. 프로젝트 구성원 선임
2. 용역(아웃소싱)업체에서 제출한 프로젝트계획서 검토 및 조정
3. 프로젝트에 대한 필요사항 자료요청

제4조(제안요청 및 계약) ① 제안서의 평가요소에 문서 · 시설 · 장비 등 보안관리계획에 대한 평가항목 및 배점기준 마련하고 제안요청서 작성시 용역(아웃소싱)업체에 프로젝트 과정에 대한 보안관리계획을 요구하여야 한다.

② 용역(아웃소싱)업체에서 제출한 제안서의 보안관리계획이 타당한지를 검토하여 사업자 선정시 이를 반영하고 필요시 추가적인 방안을 요구하여야 한다.
③ 프로젝트 보안관리계획은 계약서 상에 명시되거나 첨부되어야 한다.
④ 입찰공고 이전에 투입이 예상되는 자료, 장비 가운데 보안이 요구되는 정보에 대하여 적정 보호등급으로 분류하여 보안요구기준을 마련해야 한다.
⑤ 입찰공고시에 프로젝트 관련 기밀유지 의무 및 위반시 불이익 등의 내용을 사전에 고지하여야 한다.
⑥ 정보시스템을 위탁운영시에는 해킹에 대비해 관련 보안시스템이 구비되어 있는지 여부와 단순 운영 이외 보안관리가 가능한지 여부를 검토해야 한다.

제5조(계약체결시 정보보호 고려사항) ① 용역(아웃소싱) 계약서에는 다음 각호의 사항이 적절히 포함되어야 한다.

1. 제공되는 서비스의 구체적인 내용
2. 정보보호에 대한 책임
3. 발주기관의 용역(아웃소싱)업체에 대한 검사(감사) 권한 및 용역(아웃소싱)업체의 협조의무 명시
4. 용역(아웃소싱)제공업체의 재난복구계획을 소속기관에 제공
5. 용역(아웃소싱)제공업체의 재난복구계획에 대한 테스트결과를 발주기관이 확인할 수 있는 권리
6. 발주기관과 용역(아웃소싱)업체간에 원시데이타가 이동되는 경우 동 원시데이타에 대한 보안책임 (보험 가입 필요)
7. 오류나 누락에 의한 데이터 손실 보험 가입
8. 데이터 비밀 유지
9. 서비스대가의 변경, 계약 해제/해지시 적절한 사전 통지
10. 용역(아웃소싱)업체의 재무제표를 발주기관에게 매년 제출
11. 용역(아웃소싱)업체가 도산하는 경우 발주기관의 조치 방안
12. 계약위반, 만기전 해지 등에 따른 위약금

② 프로젝트 자체 또는 투입되는 자료 · 장비 등에 대한 대외보안이 필요한 경우 보안의 범위 및 책임을 명확히 하기 위해 사업수행 계약서와 별도로 비밀유지계약서를 작성한다.
③ 비밀유지계약서에는 비밀정보의 범위, 보안준수 사항, 위반시 손해배상 책임, 지적재산권 문제, 자료의 반환 등을 포함해야 한다.
④ 프로젝트 참여인원은 용역(아웃소싱)업체 임의로 교체할 수 없도록 명시하고 신상변동(해외여행 포함) 사항 발생시 발주기관에 즉시 보고하도록 한다.

⑤ 발주기관의 요구사항을 사업자에게 명확히 전달키 위해 작성하는 과업지시서(또는 과업내용서)에 자료 보안관리 방법, 인원
· 장비 · 시설 등에 대한 보안점검 · 교육 등 보안관련 제반사항을 상세히 기술한다.
⑥ 용역(아웃소싱)업체가 사업에 대한 하도급 계약을 체결할 경우 본 사업계약 수준의 비밀유지 조항을 포함토록 조치한다.

제6조(근무장소 및 부대시설) ① 용역(아웃소싱)업체는 프로젝트 수행장소를 프로젝트 착수 전에 관리부서와 사전협의하여 관리부서가 지정한 장소에서 수행해야 한다. 단, 프로젝트 수행 장소는 시건장치와 통제가 가능한 공간이어야 한다.
② 발주기관 내부에서 근무할 경우 전원, 통신시설 등 사무실 부대시설 공사비용은 용역(아웃소싱)업체가 부담함을 원칙으로 한다.
③ 프로젝트관리자는 용역(아웃소싱)업체 사무실 또는 용역업무를 수행하는 공간에 대한 보안점검을 정기적으로 실시해야 한다.

제7조(전산시스템) ① 프로젝트에 필요한 서버, 네트워크 장비, 프린터 등의 전산기기는 용역(아웃소싱)업체에서 자체적으로 확보하여 사용함을 원칙으로 한다. 단, 관리부서에서 필요하다고 판단되는 경우 관련 부서와 협의하여 지원할 수 있다.
② 용역(아웃소싱)업체는 발주기관의 네트워크를 사용할 수 없으며 자체적인 폐쇄망이나 별도의 인터넷망을 이용하여 네트워크를 사용해야 한다. 단, 정보보호 심의를 득한 후 사용할 수 있다.
③ 발주기관 내부에서 근무할 경우 용역 참여직원이 노트북 등 관련장비를 반출 또는 반입할 때마다 악성코드 감염여부 및 자료 무단반출 여부를 확인해야 한다.

제8조(인력관리) ① 용역(아웃소싱)업체는 프로젝트 투입인력(이하 인력이라 한다)의 이력사항을 계약체결직후 관리부서로 제출하여야 하며 제출서류는 다음 각호와 같다.
1. 재직증명서 및 최종학력증명서
2. 경력증명서
3. 자격증명서류

② 관리부서는 제1항의 서류가 접수되면 인력의 등급 및 자격을 확인한다.
③ 관리부서는 확인결과 프로젝트 수행에 부적합할 경우 용역(아웃소싱)업체에 통보하고, 용역(아웃소싱)업체는 즉시 적정인력으로 교체 투입하여야 한다.
④ 추가 또는 교체 투입되는 인력에 대해서도 동일한 절차를 적용한다.
⑤ 관리부서는 인력에게 각 개인의 친필 서명이 들어간 보안서약서를 징구하고 프로젝트

수행 전 인력에 대해 비밀유지 의무 준수 및 위반시 처벌내용 등에 대한 보안교육을 실시하여야 한다.

제9조(출입관리) 용역(아웃소싱)업체는 발주기관 내에서 근무할 인력의 출입증 발급 및 신원조회에 필요한 다음 각호의 서류를 관리부서에 제출하여야 한다.

1. 출입증발급신청서 1부
2. 보안서약서 1부
3. 신원진술서 1부

제10조(직무의 분리) 용역(아웃소싱)업체는 현재 사용중인 업무시스템에 대한 입력 및 정정 업무를 수행할 수 없는 것을 원칙으로 한다. 만약 입력 및 정정 업무를 수행한다면 프로젝트관리자의 서면승인을 득해야 한다.

제11조(내부시스템 사용자 인증 및 접근통제) ① 용역(아웃소싱)업체에서 발주기관 내부 시스템(이하 내부시스템이라 한다)을 사용해야 할 경우 다음 각 호의 사항을 준수해야 한다.

1. 용역(아웃소싱)업체 인력에 대한 사용자 계정은 하나의 그룹으로 등록하고 계정별로 정보시스템 접근권한을 부여한다.
2. 계정별로 부여된 접속권한은 불필요시 곧바로 권한을 해지하거나 계정을 폐기해야 한다.
3. 인력에게 부여한 패스워드는 프로젝트관리자가 별도로 기록 관리하고 수시로 해당 계정에 접속하여 저장된 자료와 작업이력을 확인한다.
4. 프로젝트관리자는 서버 및 장비 운영자로 하여금 내부서버 및 네트워크 장비에 대한 접근기록을 매일 확인하여 이상 유무를 정보보호담당자에게 보고해야 한다.
5. 용역(아웃소싱)업체에서 사용하는 노트북PC는 인터넷 연결을 금지한다. 단, 프로젝트 수행상 필요한 경우에는 용역(아웃소싱)업체의 관리책임자가 직접 요청하고 정보보호담당자는 접속할 노트북을 지정하여 필요한 사이트에만 접속토록 방화벽 등을 설치하도록 해야 한다.

② 내부시스템 이용시간, 작업지역을 제한하여 접근통제를 실시한다.

③ 용역(아웃소싱)업체가 제시하는 자체 통제방법에 대하여 소속기관은 이를 평가하고 채택여부 등을 결정하며 필요시 추가적인 통제방안을 요구해야 한다.

④ 용역(아웃소싱) 해당 업무에 필요한 정보 및 시스템 이외에 대한 접근은 허용하지 않는다.

⑤ 일정시간 경과 후 자동 접속차단(Automatic Timeout) 방식 적용을 검토하여야 한다.

⑥ 내부 전산망에서 P2P, 웹하드 등 인터넷 자료공유사이트로의 접속은 금하며 방화벽 등을 이용해 이를 원천 차단해야 한다.

제12조(내부시스템 관련 활동 및 예외보고서) 용역(아웃소싱)업체가 내부시스템을 사용할 경우 사용자는 내역을 작성하여 프로젝트관리자의 승인과 시스템 관리부서의 승인을 득한 후 사용한다.

제13조(기타 운영상의 통제) ① 용역(아웃소싱)업체의 개발 및 운영과 관련한 서비스에 대해 발주기관은 자체감사 기능을 가져야 한다.

② 자체 정보시스템 감사전문가 양성, 외부 정보시스템 감사인의 종합적인 감사를 검토한다.

제14조(프로젝트 중단에 대비한 비상대책) ①용역(아웃소싱)업체의 프로젝트 중단은 소속기관에 심각한 영향을 미치므로 철저한 대비책을 마련한다. 서비스 중단 형태별로 별도의 대비책을 마련해여 위험관리를 하여야 한다.

② 재해등에 해당하는 비상시에도 용역(아웃소싱)업체는 최소한 가장 중요한 응용업무를 처리할 수 있도록 비상계획을 마련해야 한다.

③ 용역(아웃소싱)업체의 재무건전성을 모니터링하여 도산에 대비하여야 하며, 지속적인 프로젝트의 진행이 어렵다고 판단되는 경우 용역(아웃소싱)업체의 교체계획을 수립해야 한다.

제15조(자료 보안) ① 네트워크구성도, IP현황, 개인정보 등 용역(아웃소싱)업체에 제공하는 중요자료는 '자료관리대장'을 작성하여 인계자(프로젝트 관리자)와 인수자(용역(아웃소싱)업체 관리책임자)가 직접 서명한 후 인계 · 인수한다.

② 관련자료 및 사업과정에서 생산된 모든 산출물은 부내 파일서버에 저장하거나 프로젝트 관리자가 지정한 PC에 저장 · 관리한다.

③ 프로젝트 관련자료는 인터넷 웹하드 등 인터넷 자료공유사이트 및 개인메일함에 저장하는 것을 금지하고 전자우편을 이용해 자료전송이 필요한 경우에는 자체 전자우편을 이용하여 첨부자료를 암호화 후 수발신해야 한다. 단, 대외비 이상의 비밀은 전자우편으로 수발신을 금지한다.

④ 발주기관이 제공한 사무실에서 사업을 수행할 경우 제공한 비공개자료는 매일 퇴근시 반납토록 하며 비밀문서를 제외한 일반문서는 용역(아웃소싱)업체에 제공된 사무실에 시건장치가 된 보관함이 있을 경우 이에 보관 가능하다.

⑤ 프로젝트 수행으로 생산되는 산출물 및 기록은 정보보호담당자가 인가하지 않은 비인가자에게 제공 · 대여 · 열람을 금지한다.

⑥인가받지 않은 USB 등의 보조기억매체 사용을 금지하며 산출물 저장을 위해 보조기억매체가 필요한 경우 프로젝트관리자의 관리하에 사용하도록 한다.

제16조(사업완료시 보안관리) ① 사업완료 후 생산되는 최종 산출물 중 대외보안이 요구되는 자료는 대외비로 작성 · 관리하고 불필요한 자료는 삭제 및 세단 후 폐기한다.

② 용역(아웃소싱)업체에 제공한 제반자료, 장비, 서류와 중간 · 최종 산출물 등 용역과 관련된 제반자료는 전량 회수하고 용역(아웃소싱)업체에 복사본 등 별도 보관을 금지한다.

③ 노트북 · 보조기억매체 등 전자적으로 기록된 자료는 '정보시스템 저장매체 불용처리 지침'에 따라 보안조치한다.

④ 용역사업 관련자료 회수 및 삭제조치 후 업체에게 복사본 등 용역사업 관련 자료를 보유하고 있지 않다는 대표 명의 확약서를 징구한다.

- [부록 4-1] 자료 관리대장

자료 관리대장

관리 번호	자 료 명	접수 일자	발행처	보관팀	배 포		폐 기		비고
					배포처	확인	내용	승인	

[부록 4-2] 원격접속 관리대장

원격접속 관리대장

사용자명	서버명	원격접속 계정(ID)	접속시 비밀번호	접속주소	접속사유	접속시간	관리자 조치사항	확인

[부록 4-3] 외주인력 ID 신청서

외주 인력 ID 신청서

승인	부 서 장

신 청 자	소 속			
	이 름			(인 또는 서명)
	신 청 일	20 년 월 일		
	신청기간	20 년 월 일 ~ 20 년 월 일		
용 도	□ 신규등록 □ 권한변경 □ 사용중지 □ 재사용 □ ID삭제			
시스템 이름	1.	4.	7.	
	2.	5.	8.	
	3.	6.	9.	
ID 이름		초기 패스워드		
사유 및 내용				

1. 최초 로그온 시 반드시 패스워드를 변경하셔야 합니다.
2. 패스워드는 최소8자리 이상이며, 영문자, 숫자는 반드시 포함하고, 특수문자 $,₩,',!,&는 사용할 수 없습니다.

정보보호 담당자	부 서 명	
	이 름	(인 또는 서명)
	처 리 일	20 년 월 일
시스템 담당자	부 서 명	
	이 름	(인 또는 서명)
	처 리 일	20 년 월 일

[부록 4-4] 영업비밀보호 서약서

영업비밀보호 서약서

성　　명
주민등록번호
주　　소

본인은 이번 귀사의 OOO 프로젝트에 그 일원으로 참여하게 되었으며 이에 아래와 같은 사항을 준수할 것을 서약합니다.

1. 본 프로젝트 추진의 사실, 그 성과 및 본 프로젝트를 수행하는 과정에서 알 수 있는 귀사의 영업비밀을 유지하고 회사 밖은 물론 귀사의 종업원이라고 하여도 프로젝트에 직접 관여하지 않는 자에 대해서는 이것을 공개 또는 누설하지 않을 것을 서약합니다.

2. 본 프로젝트 추진의 사실 및 그 성과가 귀사에 의하여 적법하게 공개된 경우라고 하여도 미공개 부문에 대해서는 앞에서와 같은 비밀유지의무를 부담할 것을 서약합니다.

3. 본 프로젝트가 완료된 경우 및 프로젝트 진행중에 어떠한 사유로든 본인이 본 프로젝트를 수행할 수 없게 된 경우, 그 시점에서 본인이 보유하고 있는 모든 영업비밀을 포함한 관련자료를 즉시 귀사에 반납하며 앞에서와 같은 비밀유지의무를 부담할 것을 서약합니다.

4. 본 프로젝트 추진의 사실, 그 성과 및 본 프로젝트를 수행하는 과정에서 알 수 있었던 귀사의 영업비밀을 재직중은 물론 퇴직후에도 년간 자신을 위해 또는 귀사와 경업하

년　　월　　일
서약인　　인
주식회사　　귀중

[부록 4-5] 투입 종료 확인서

투입 종료 확인서

1.기본정보

이 름			
소속회사		연 락 처	
근무기간	~	담 당 업 무	

※ 투입 종료 프로세스 안내

1. 아래 점검 사항의 1~6단계 절차를 모두 이행한후, 확인란에 √표시를 합니다.
2. 출입 ID카드와 투입종료확인서를 보안담당자에게 제출합니다.
3. 보안담당자는 각 단계별 이행점검을 하고 서명란에 서명을 합니다.

2. 점검사항

내 용	담당자	서명
1. 산출물 및 업무 인수 인계 – 최종 산출물을 제출해 주시기 바랍니다 – 수행하던 업무가 완료되지 않은 경우 후임자에게 인수인계 합니다.	PL/ PM	
2. 근태 확인 – 근무기간 PM Tool의 근태등록 및 승인을 받았는지 확인합니다.	PL/ PM	
3. 봉인스티커 부착 – 개인사물함의 내용을 비우고 열쇠를 서랍장 안에 넣어두시기 바랍니다.	PL/ PM	
4. 시스템 계정 삭제 요청 1)서버: 2)DB: 3)Application: 4)형상관리: 5)기타( )	PL/ PM	
5. PC 포맷 – 반드시 PC를 포맷해 주시기 바랍니다. – 담당자로부터 PC포맷S/W를 제공받아 포맷합니다.	PL/ PM	
6. 출입 ID 카드 반납 – 투입시 교부 받았던 ID카드를 PM에게 제출하시기 바랍니다. ※담당자는 반드시 ID카드 해지를 해야 함	PL/ PM	

3. 특이사항

년 월 일 작성자 성명: (인)

[부록 5-1] 출력이력 관리대장

출력이력 관리대장

연월일	출입시간	용무	출입자		입회자		비고
			소속	성명	직급	성명	

[부록 5-2] 보안 정책변경 요청서

보안 정책변경 요청서

1.정책 변경 대상자 정보

이 름			
소속회사		연 락 처	

2. 점검사항

PC	매체 권한 선택	■ FDD 쓰기허용 ■ CD-RW/DVD-RW 쓰기허용 ■ USB 쓰기허용 ■ IEEE1394 쓰기허용 ■ 모뎀 쓰기허용 ■ Serial Port 쓰기허용 ■ 적외선 포트 쓰기허용
	반출신청 유형	■ 당일반출 ■ 회의용 ■ 외근 ■ 사내 오프라인 □ 기타( )
문서	생성자 권한 선택	■ 읽기 가능 ■편집 가능 ■ 해제 가능 ■ 반출 가능 (외부전송보안파일생성) ■ 출력 가능 ※ 외부전송 보안파일 생성이란, 문서보안 미사용 외부인에게 열람이 가능하도록 보안문서를 실행파일로 만드는 기능 **(편집불가, 열람, 인쇄 가능)**

3. 특이사항

다음 각 항에 해당하는 자료유출, 변조 복사, 훼손, 분실 등으로부터 안전하게 회사 정보자산을 보호하고, 이를 충분히 숙지하여 성실히 이행하겠습니다.

1. 컴퓨터, 네트워크, 모뎀 등을 통한 회사정보를 유출하지 않는다.
2. 회사 정보가 수록된 기록매체(하드디스크, 디스켓 등)를 무단으로 공유하거나 반출하지 않는다.
3. 정보시스템의 업무용도외 사용하지 않으며 정보사용권(시스템 사용승인)을 준수한다.
4. 사용자 ID 및 Password의 불법사용, 대여하지 않는다.
5. 통신이나 불법S/W의 사용 등을 통해 Virus 유포 등을 하지 않는다.
6. 기타 컴퓨터를 통한 정보의 무단취득, 유출, 손실, 파괴 등의 행위를 하지 않는다.
7. 외부업체 직원의 반출신청시 업무 담당자(신청자)는 외부인(사용자)으로 하여금 상기 사항을 준수하도록 조치하고 이행 여부를 점검한다.
8. 본인은 상기 사항을 충분히 숙지하였음을 인정하고 성실히 준수할 것을 동의하며, 이행하지 못하였을 경우 사규 및 관련 법률에 따라 민 · 형사상 책임을 지고, 회사의 어떠한 처벌도 감수할 것이며, 회사에 끼친 손해에 대해 지체없이 변상, 복구할 것을 서약합니다.

년 월 일

작성자 성명: (인)

담당자 성명: (인)

[부록 5-3] 출력물 관리대장

출력물 관리대장

번호	자료명	제공형태		제공자 (부서/ 담당자)	수령자	수령일자	반납기한	반납일자	용도	비고
		Hard	Soft							

IT 외주인력 보안통제 안내서

2011년 12월 인쇄
2011년 12월 발행

발행처: 방송통신위원회 · 한국인터넷진흥원

서울특별시 종로구 세종대로 178
방송통신위원회
Tel: (02) 750-1114

서울특별시 송파구 중대로 109번지
대동빌딩 한국인터넷진흥원
Tel: (02) 405-5118

인쇄처: 한올
Tel: (02) 2279-8494

(비매품)

이 책을 볼 수 있는 독자는?

업무관계자
초급

업무관계자
중급

업무관계자
고급

방송통신위원회

110-777 서울특별시 종로구 세종대로 178
Tel: (02) 750-1114
www.kcc.go.kr

한국인터넷진흥원

138-950 서울특별시 송파구 중대로 109번지 대동빌딩
Tel: (02) 405-4118 Fax: 405-5119
www.kisa.or.kr