「2023년 및 2024년 주요정보통신기반시설
취약점 분석·평가 컨설팅」

과 업 지 시 서

2023. 01.

부산-김해경전철주식회사

목 차

Ⅰ 사업 개요

1. 추진배경 및 필요성

❍ 주요정보통신기반시설 관리기관은 관련법령에 의거, 보유 중인 기반시설에 대한 취약점 분석.평가 및 보호대책 수립을 매년 수행해야 함

관련근거

- 정보통신기반보호법 제5조(주요정보통신기반시설보호대책의 수립 등)
- 정보통신기반보호법 제9조(취약점의 분석·평가)
- 정보통신기반보호법 시행령 제17조(취약점 분석·평가의 시기)

❍ 주요정보통신기반시설 취약점 진단 및 잠재된 취약점 제거, 기반시설 담당자 역량 강화를 통해 기반시설 정보보호 수준 강화 필요

2. 사업 개요

❍ 사 업 명 : 주요정보통신기반시설 취약점 분석·평가 컨설팅

❍ 사업기간 : 계약일 ~ '24.12.31(2년간)

3. 주요 사업내용

❍ 취약점 분석·평가, 진단 및 조치

❍ 모의해킹 및 침해사고 대응훈련

❍ 정보보호 교육(전 직원대상)

❍ 보호대책 작성 및 중장기계획 갱신 등

4. 수행 인원

❍ 수행인원 : 계약 체결 후 별도 협의

5. 사업 대상

❍ 기반시설 지정 현황

기반시설 명	지정년도	지정기관	관리기관	비고
경전철 종합관제시스템	2014	행정자치부	부산-김해경전철(주)	

❍ 부산-김해경전철 기반시설 38개

주요정보통신기반시설		구분			비고
지정단위	세부시설	기종	수량	설치장소	
종합 관제 전력 시스템	서버	SUN V490	3	전산실	전력 Main Computer
	PC	HP 6400 WS	6	종합관제 등	관리용 콘솔
	DBMS	-	1	종합관제	DPS1DB
	소계		10		
종합 관제 신호 시스템	서버	HP DL580 G5	5	전산실	ATC 관리시스템 NMS 시스템
	보안장비	SECUI MF2-300	2	전산실	신호망 침입차단시스템
	PC	HP 6600 WS	9	종합관제 등	열차운행 제어 감시용 콘솔
		HP Z640	1	종합관제	
		Intel Xeon	2	종합관제	
	소계		19		
종합 관제 통신 시스템	서버	RP3440-2CPU	1	통신기계실	ADM 관리시스템
		HP DL385 G5	1	통신기계실	MUX 제어시스템
		iEi EC-1040GB	1	통신기계실	NTP 서버
	PC	HP DC7600	3	통신기계실 등	NMS 관리용 콘솔
		HP 6400 WS	1	종합관제	출입통제 관리용 콘솔
	소계		7		
종합 관제 전산 시스템	네트워크 장비	CISCO 3560G	1	전산실	라우터
		Piolink K1216	1	전산실	L4 스위치
	소계	소계	2		
기반시설(세부시설) 수			38		

※ '22년 대비 종합 관제 AFC 시스템 13개 시설물 제외(망분리 완료)

Ⅱ 추진 계획

1. 추진 목표

부산-김해경전철 주요정보통신기반시설 정보보호 수준 강화

인적 역량 강화	• 주요정보통신기반시설 침해사고대응 모의훈련을 통해 대응능력 점검 • 주요정보통신기반시설 업무종사자 대상 정보보호 교육을 통해 담당자 보안의식 제고
사전 예방 강화	• 주요정보통신기반시설 취약점 분석·평가를 통해 차년도 보호대책 수립 • 주요정보통신기반시설 취약점 조치 지원을 통해 잠재된 사이버위협 제거

2. 추진 전략

❍ 정보통신기반보호법시행령 제8조에 의거 보호대책을 8월 31일까지 관계중앙행정기관에 제출하기 위한 진단계획 수립 및 추진

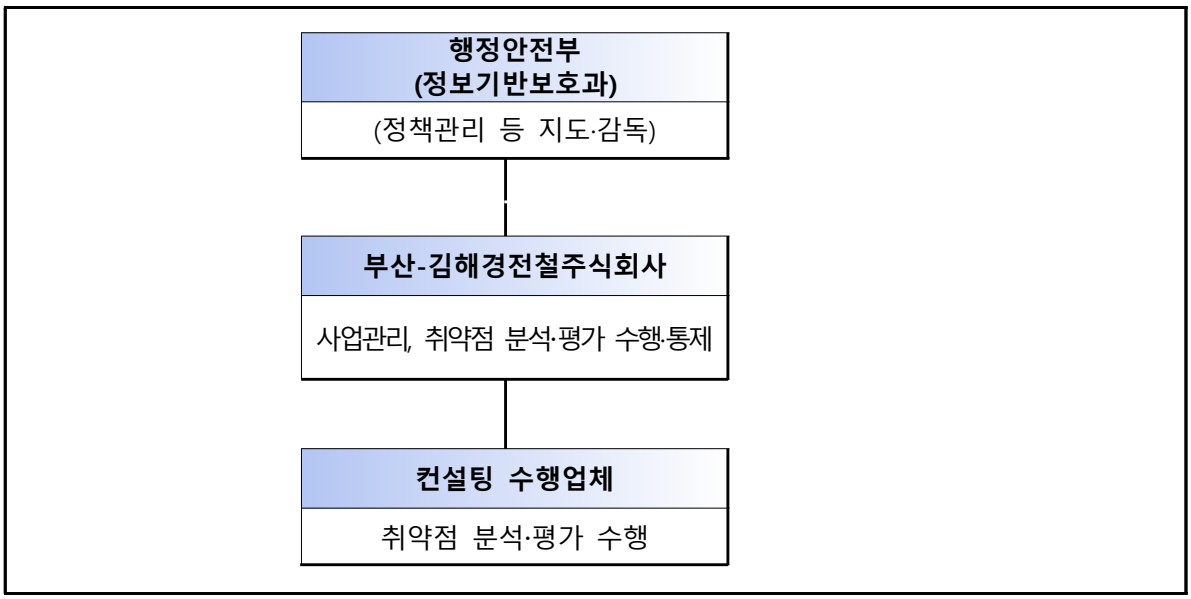
❍ 주요정보통신기반시설 특성 이해, 동일한 점검 기준 적용, 보안 준수사항 등 사전 교육실시를 통한 고품질의 보호대책 수립 기반 마련 및 사업 참여인력 보안의식 강화

❍ 주요정보통신기반시설 담당자의 요구사항을 반영하여 침해사고 대응 모의훈련 및 정보보호 교육계획 수립 및 추진

❍ 유관기관과 사전 긴밀한 협조를 통해 의사소통 강화 및 업무지연 방지

3. 추진 체계

❍ 추진 조직



❍ 추진조직별 역할

구 분	주요 역할
행정안전부 (정보기반보호과)	○ 행안부 소관 주요정보통신기반시설에 대한 정책 수립·관리 ○ 유관기관간 책임과 역할 정립 등 협조체계 유지 ○ 행안부 소관 주요정보통신기반시설 보호대책 및 관리계획 이행여부 확인·분석 등
부산-김해 경전철주식회사	○ 취약점 분석·평가 결과에 따른 개선방안 마련 및 조치 ○ 차년도 보호(관리)대책 수립 및 위험요소(취약점) 제거 등 이행
컨설팅 수행 업체	○ 전문인력 구성 및 담당자 지정·운영 ○ 취약점 분석·평가 수행 및 보호대책(안) 수립 지원 ○ 기반시설 관리기관 대상 침해사고대응 모의훈련 및 정보보호 교육 실시 ○ 취약점 분석·평가 결과에 따른 개선방안 마련 및 취약점 조치 지원 ○ 단기 취약점 조치사항 등에 대해 사후 이행점검 및 조치 지원

4. 추진 일정

❍ 주요업무 추진일정

구 분	'23.00월 및 '24.00월			
	1주차	2주차	3주차	4주차
취약점 분석평가 진단 및 조치				
모의해킹 및 침해사고 대응훈련				
정 보 보 호 교 육				
보호대책 작성 및 중장기계획 갱신				

※ 상기 항목과 추진 일정은 계약대상자와 협의에 따라 변경 가능

※ 1차 방문시 4주간 상주하여 취약점 분석·평가 진단 및 조치지원까지 완료를 원칙으로 하고, 부득이한 사유 발생 시 2차 방문 후 조치지원을 할 수 있다.

Ⅲ 사업 내용

1. 주요정보통신기반시설에 대한 취약점 분석·평가

❍ 취약점 분석

- 「주요정보통신기반시설 취약점 분석·평가 기준」에 따라 제어망에 대한 취약점 점검 수행
  · 상기 기준에 포함된 453개 전체 항목에 대해 점검하는 것을 원칙으로 함

❍ 취약점 평가

- 취약점 점검결과 항목별 위험도 산정 및 우선 조치대상 분류
- 위험도 산정 방법론은 수행사의 고유 방법론을 사용하되 관할 주무부처 및 한국인터넷진흥원(KISA)에서 권장하는 기준에서 벗어나지 않는 방법 적용
- 과학기술정보통신부에서 고시한 「주요정보통신기반시설 취약점 분석·평가 기준」에 따라 취약점 진단 실시
- 위험도 산정 과정 중, '위험수용'으로 분류하는 취약점에 대해서는 객관적인 사유를 반드시 확보 후 분류

※ 위험도 수치가 낮으므로 위험수용으로 분류하는 식의 단순 분류를 금하며, 시스템 미지원, 대체수단에 의한 조치 등 객관적인 사유를 확보해야 함

❍ 개선방안 도출

- 취약점 점검 및 평가 수행 후 발견된 문제점에 대한 세부 개선방안을 구체적으로 제시
- 일반적인 대안 제시가 아닌, 해당 기관의 현황 및 특성을 고려한 맞춤형 개선방안 제시로 실효성 제고
- 점검을 통해 발견된 취약점 중 즉시조치가 가능한 사항에 대해서는 진단기간 중 현장에서 개선조치

❍ 발견된 취약점에 대한 조치 현장지원

- 취약점 진단시 발견된 취약점에 대해서 담당자 협의후 현장 즉시

조치를 우선으로 하고, 부득이한 경우 위험수용여부를 결정한다.

❍ **취약점 조치 이행점검**

- 취약점조치 이행점검은 최대한 현장 즉시조치를 우선으로 하고, 조치가 어려울시 담당자 협의후 관리방향을 정한다.

2. `24년 및 `25년도 주요정보통신기반시설 보호대책 수립

❍ **차년도 보호대책 수립지원**

- 「`24년 및 `25년도 주요정보통신기반시설 보호대책 수립 지침」에 따라 해당 기반시설에 대한 보호대책(안) 마련 및 관리기관 최종 수립 지원
- 수립된 보호대책에 대한 내용을 해당 관리기관 담당자가 상세히 이해할 수 있도록 세부 설명 제공

❍ **기반시설 관련내규 및 세부지침 보완 제시**

- 기반시설 보호를 위한 관련내규(주요정보통신기반시설정보보호 내규, 보안업무규정) 및 세부지침 등을 보완할 수 있도록 제시

3. 모의해킹 실시

❍ **모의해킹 실시 후 취약점에 대한 보호조치 및 컨설팅 지원**

- 시스템 보안설정 변경 등 취약점 실제 개선조치를 지원하고 현장지원 결과보고서를 작성

4. 침해사고 대응 훈련 실시 및 훈련 미흡사항에 대한 보호조치 지원

❍ **침해사고 대응 훈련 시나리오 개발 및 수행**

- 시설별 침해사고 대응 훈련 계획 수립
- 사이버 침해 유형별 시나리오 개발, 상황발령, 신고 및 대응 절차 분석 등
- 훈련은 대상 기반시설별로 각각 수행해야 하며, 각 기반시설 현황을 심층 분석 후 개별 시나리오를 수립하여 진행해야 함

  ※ 훈련 대상은 취약점 분석·평가 지원 대상을 기본으로 하며 필요시 조정가능

5. 정보보호 교육 실시

❍ 정보보호 교육 수행

- 주요정보보호 담당자와 협의하여 교육대상(기반시설 업무종사자, 임직원 등), 교육내용, 일정 등 계획수립
- 교육 수행 후 수강자들을 대상으로 교육 평가(설문)
  · 교육 평가는 교육의 이해도, 교육 만족도로 나누어 평가
- 교육 평가를 분석하여 주요정보보호 담당자에게 교육결과 보고서 제출
  · 결과 보고서에 교육 개요, 내용, 증적(사진, 참석자 명단) 자료와 설문결과 및 분석내용을 포함하여 작성

Ⅳ 수행사항

1. 사업 수행조건

❍ 취약점 분석·평가 진단후 현장 조치에 중점을 두어야 하고, 종합점수에 있어서 전년도 조치률을 상회하여 발주자가 요구하는 조건을 충족하여야 한다

❍ [주요정보통신기반시설에 대한 취약점 분석·평가], [`23년 및 `24년도 주요정보통신기반시설 보호대책 수립]은 `23년 및 `24년도 8월까지 완료해야 함

❍ 「정보통신기반 보호법」제9조 제3항에 따라 취약점을 분석·평가할 수 있는 기관에 소속된 인력으로 최소 4인 이상으로 구성·운영해야 함

❍ [주요정보통신기반시설에 대한 취약점 분석·평가], [`23년 및 `24년도 주요정보통신기반시설 보호대책 수립]을 위해 3주 이상 상주하여 사업을 수행하는 것을 원칙으로 하며, 상주 기간은 발주자와 협의하여 최종 결정한다.

❍ 수행사 선정이 완료되는 대로 수행사는 사업 결과물의 품질 제고를 위해 투입인력에 대한 사전교육 등 제반 사항을 준비한다.

※ 투입인력에 대한 사전교육 등 제반사항 준비

❍ 본 지시서에 별도 명기된 사항이 없더라도 주요정보통신기반시설 보호관련 법.규정 등에서 요구하는 모든 사항을 포함하고 충족시켜야 함

❍ 사업 수행중에 발주자가 요구하는 규정개정 및 보안장비 확충 등 제반사항에 대한 조언을 구할시 충실히 자문에 임한다.

❍ 과제 수행을 위한 구체적인 인력 투입계획(투입인력의 실명 필수

표기)을 제안서에 명시해야 함

2. 일반 조건

❍ 수행사는 재무구조, 대외신인도, 신용도 등 회사의 경영 상태를 나타낼 수 있는 증빙자료를 제시하여야 함

❍ 수행사는 최근 3년간 본 사업과 관련한 분야에서 수행한 컨설팅 사업 실적 및 규모를 모두 제시하여야 함

- 수행사가 협력사를 활용하는 경우에는 해당 협력사에 대해서도 위 사항을 제시하되, 수행사와 구분하여 각 협력사별로 기재하여야 함

❍ 수행사는 회사의 조직 및 인력 현황을 제시하고 본 제안을 담당할 프로젝트 조직 및 투입인력, 조직별, 작업단위별 업무 분장내역을 제시하여야 함

❍ 세부적인 투입인력에 대해서는 발주자의 요청 기준을 벗어나지 않도록 하며, 수행사의 환경을 고려하여 일부 조정 가능함

❍ 전체 및 수행공정별 투입 인력에 대한 교육, 자격, 경력현황 등을 상세히 제시하여야 함

❍ 수행사는 업무수행범위 및 책임한계를 상세히 정의 하고 조직 운영 방안을 제시하여야 함

❍ 사업수행 총괄책임자(PM)는 『2020년 SW사업 대가산정 가이드(`20.06.15)』 기준으로 전임급 이상이어야 함

❍ 수행사가 제안한 전체 및 수행공정별 인력 투입계획에 따라 프로젝트 전 기간 동안 참여를 보장하여야 함

❍ 수행사는 발주자의 실정에 맞는 기술지원을 수립하고, 최신의 정보보호 전문소양 및 실무지식을 갖춘 인력을 지원해야 함

3. 하자 보수조건

❍ 본 사업의 하자 보증기간은 계약 종료일로부터 1년 까지로 하고, 보증기간동안 수행사는 결과물 분석.검토 관련 요청사항 등을 필수로 지원하여야 함

4. 산출물

❍ 사업추진과정에서 생산되는 제반 작업단위별 산출물의 종류, 주요 내용 작성 및 제출시기, 제출 부수, 제출 매체 등을 제시하여야 함

※ 컨설팅 결과를 효율적으로 관리하기 위하여, 발주자가 요청하는 형태의 산출물을 제공하여야 함

❍ 계약일로부터 사업종료일까지 사업수행계획서에 제시된 절차에 따른 진행사항 및 이슈사항 등 진도 보고(주간 및 월간)

※ 계획 대비 실적, 주요 내용 및 산출물, 인력투입 현황, 차주 계획 및 변동사항, 주요 의사결정 및 협조사항 등

❍ 사업 최종 결과보고서

- 사업 종료일 이전에 결과의 최종 산출물에 대한 내용 및 양식 등을 협의한 후 제안서, 계약서, 사업수행계획서 등 내용을 포함하여 제출

※ 보고서 산출물은 제본하여 2부 이상(CD포함) 제출하며, 산출물의 종류, 제출 방법 등은 발주자와 협의하여 조정할 수 있음(규격 : 인쇄용 한글문서 및 USB)

5. 품질보증 및 관리 계획

❍ 수행사는 품질보증 방법 및 절차, 품질목표수준, 품질보증 내용 및 보증 조직 등을 포함한 구체적인 품질보증 방안을 제시하여야 함

❍ 수행사는 본 사업의 공정관리, 품질관리, 진도관리, 보안관리 등 제반 관리를 보다 효과적으로 수행하기 위해서 사용할 프로젝트 관리도구의 활용방안을 제시하여야 함

❍ 수행사는 본 사업을 추진하는 과정에서 단계별, 작업단위별로 생산되는 산출물에 대하여 작업 일정계획 및 품질보증 계획과 연계하여 산출물의 제출시기, 제출내용 및 제출부수 등을 제시하여야 함

6. 기밀보안 및 비상대책

❍ 수행사는 사업수행기간 중 보안 관련법규를 준수하고 대외 보안 유지에 적극 협조하여야 함

❍ 수행사는 사업수행 기간 중 중요 데이터 등 정보유출에 대한 보안대책, 정보의 기밀성, 무결성, 가용성을 적정수준으로 구현하기 위한 방안에 대한 종합적인 정보보호 방안을 제시

❍ 수행사는 외부PC(노트북 등) 반입.반출 시 발주자가 요구하는 보안사항을 준수하여야 함

❍ 사업 수행과정에서 취득한 자료와 정보에 관하여 사업수행 중은 물론 사업 완료 후에도 이를 외부에 유출해서는 안되며, 사업종료 시 보안담당자의 입회하에 완전 폐기 또는 반납해야 함

7. 계약이행

❍ 수행사는 발주자의 서면에 의한 사전 동의 없이는 계약상의 어떠한 권리, 의무도 타인에게 양도 또는 이전할 수 없음

❍ 계약내용 중의 일부를 변경할 경우 반드시 쌍방간에 서면 합의가 있어야 함

❍ 계약 체결이후 또는 계약 이행이 완료된 후라 하더라도 계약상의 착오 또는 오류 등으로 인하여 수행사가 부당한 이득을 취한 사실이 발견되었을 경우 발주자는 과다 계상된 금액을 감액 또는 환급 청구할 수 있으며, 수행사는 이에 응하여야 함

❍ 계약 내용 중의 일부를 변경할 때는 반드시 발주자의 승인을 받아야 함

❍ 수행사는 인력투입계획에 따라 투입 요원의 이력 사항을 사업수행계획서에 포함하여 발주자에게 제출하여야 함

❍ 사업수행 책임자(PM) 및 전담 인력은 본 사업 수행 기간동안 특별한 사정이 없는 한 변경할 수 없음. 단, 불가피한 경우 발주자의 승인을 거쳐야 함

❍ 발주자는 투입된 요원이 정당한 업무지시를 이행하지 아니하는 등 업무수행에 적절하지 못하다고 판단될 경우 수행사에게 교체를 요구할 수 있음

8. 계약의 해제 및 해지

❍ 발주자는 수행사에게 다음 각 호에 해당하는 경우, 본 계약의 전부 또는 일부를 해제 또는 해지할 수 있음

- 발주자의 사전 승인 없이 계약서상의 어떠한 권리나 의무를 타인에게 양도, 전매한 경우
- 계약행위 미이행, 계약상 중대한 위반행위, 기술능력 부족 등 수행사의 귀책사유로 계약의 목적을 달성하지 못한 경우
- 투입인력의 태만이나 불성실로 인하여 발주자의 업무에 지장을 초래하여 계약의 해지 및 변경 등이 필요한 경우
- 정상적인 계약관리를 방해하는 불법·부정행위가 있는 경우
- 정보보호 및 보안 조건의 위반, 컨설팅중단 사유의 발생 등 불가피한 사정으로 인하여 계약을 해지할 필요가 있다고 발주자가 인정한 경우

❍ 발주자는 위항의 경우 이외에 불가피한 사정으로 인하여 계약을 해제 또는 해지할 필요가 있다고 인정될 경우에는 필요한 조치를 취할 수 있음

❍ 수행사의 귀책사유로 계약해지 시 부정당업자로 제재를 받을 수 있음

9. 검사/검수

❍ 최종 검사는 별도의 문서에 의하여 발주자의 검수 승인을 받은 일자에 완료된 것으로 함

10. 외주 컨설팅사업 보안특약

❍ 수행사는 발주자의 보안정책을 위반하였을 경우 [별표1]의 "용역 수행사 보안위반 처리 기준"에 따라 위반자 및 관리자를 조치하고 [별표2]의 "보안 위약금 부과 기준"에 따라 발주자가 부과한 보안 위약금을 납부한다.

❍ 수행사는 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 [별표3]의 "누출금지 대상정보"에 대한 보안관리계획을 사업 제안서에 기재하여야 하며, 해당 정보 누출 시 발주자는 국가를 당사자로 하는 계약에 관한 법률 시행령 제76조에 따라 수행사를 부정당업체로 등록한다

❍ 사업 수행과정에서 취득한 자료와 정보에 관하여 사업수행 중은 물론 사업 완료 후에도 이를 외부에 유출해서는 안 되며, 사업종료 시 정보 보안담당자의 입회하에 완전 폐기 또는 반납해야 한다.

[별표 1] 수행사 보안위반 처리기준

[별표 2] 보안 위약금 부과 기준

[별표 3] 누출금지 대상 정보

11. 기타사항

❍ 수행사는 본 과업지시서에서 요구한 조건의 수용이 어려울 경우 불가능한 사유 및 대체 방안을 제시할 수 있음

❍ 수행사는 본 사업 추진과 관련하여 수행사가 지원 가능한 기타사항에

대하여 제시한다.

- ❍ 수행사는 취약점 분석·평가를 위한 작업 장소를 발주자와 상호 협의하여 정함
- ❍ 취약점 진단, 모의해킹 등의 컨설팅 수행과정에서 수행사의 과실로 인하여 서비스 및 시스템 장애, 보안취약점 유발, 보안사고 발생, 개인정보 유출, 원본의 훼손, 금전적 손실 등이 발생한 경우에는 이에 상응하는 금전적 손해배상을 하여야 함. 다만, 수행사의 과실이나 손해액이 불분명한 경우에는 "장애평가위원회"를 개최하여 장애 원인 규명 및 귀책 여부 등 손해와 관련한 사항을 결정
- ❍ 계약과 관련하여 계약서상 어구해석에 이의가 있는 경우나 계약서에 명시하지 아니한 사항은 원칙적으로 발주자의 해석에 따름
- ❍ 위 조건 이외에 일반적인 작업조건은 발주자의 지침에 따르며, 이견이 있을 경우에는 발주자와 수행사의 책임자급이 협의.조정할 수 있음

[별표 1]

용역 수행사 보안위반 처리 기준

구 분	위 반 사 항	처 리 기 준
심 각	1. 비밀 및 대외비 급 정보 유출 및 유출시도 가. 정보시스템에 대한 구조, 데이터베이스 등의 정보 나. 개인정보·신상정보 목록 다. 비공개 항공사진·공간정보 등 비공개 정보 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 (부정당업체 등록) ○ 위반자 및 직속 감독자 등 중징계 및 교체 ○ 재발 방지를 위한 조치계획 제출 ○ 위반자 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 컨설팅사업 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)	○ 위반자 및 직속감독자 등 중징계 및 교체 ○ 재발 방지를 위한 조치계획 제출 ○ 위반자 대상 특별 보안교육 실시

구 분	위 반 사 항	처 리 기 준
보 통	1. 기관 제공 중요정책·민감 자료 관리 소홀 가. 주요 현안·보고자료를 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	○ 위반자 및 직속 감독자 등 경징계 ○ 위반자 및 직속 감독자 경위서 제출(제출처: 발주자) ○ 위반자 대상 특별 보안교육 실시
경 미	1. 업무 관련서류 관리 소홀 가. 진행중인 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	○ 위반자 서면·구두 경고 등 문책 ○ 위반자 경위서 제출(제출처: 발주자)

[별표 2]

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 비중	부정당업자 등록	계약금액의 5%	계약금액의 3%	계약금액의 1%

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

[별표 3]

누출금지 대상 정보

1. 기관 소유 정보시스템의 내·외부 IP주소 현황

2. 세부 제어시스템 구성현황 및 제어망구성도

3. 사용자계정 및 패스워드 등 제어시스템 접근권한 정보

4. 제어망 취약점 분석·평가 결과물

5. 컨설팅사업 결과물 및 프로그램 소스코드

6. 국가용 보안시스템 및 제어시스템 도입현황

7. 망연계장비 및 라우터·스위치 등 네트워크장비 설정 정보

8. '공공기관의 정보공개에 관한 법률' 제9조 1항에 따라 비공개 대상정보로 분류된 기관의 내부문서

9. '개인정보 보호법' 제2조 1호의 개인정보

10. 발주자 '보안업무규정' 제28조의 대외비문서의 관리

11. 그 밖의 발주자가 공개가 불가하다고 판단한 자료