전남대학교 CHONNAM NATIONAL UNIVERSITY | 정보화본부 INFORMATION SERVICE CENTER | 정보보호팀 INFORMATION SECURITY TEAM

2026년도

정보화사업 용역업체 보안관리 가이드

- 안전한 협력 체계 구축
- 보안 사고 및 정보 유출 예방
- 단계별 필수 준수사항 안내

Contents

1. 교육 개요
2. 최신 보안 동향
3. 용역사업 보안관리
4. 개인정보보호
5. 보안 위규 처리

I. 개요
교육 목적 및 추진 근거

보안 인식 제고

협력 체계 구축 및
공동 인식 강화

자료 유출 방지

해킹 및 관리 소홀로 인한
자료 유출 차단

침해사고 예방

미흡한 보안 관리로 인한
해킹 사고 예방

추진 근거 | 국가 및 교육부 정보보안 기본지침, 보안업무규정 등 관련 법규 준수

I. 개요
교육 목적 및 추진 근거

추진근거

- 국가 정보보안 기본지침 제16조(정보보안 교육), 제63조(용역사업보안관리)
- 보안업무규정 및 시행규칙(대통령 훈령)
- 교육부 정보보안 기본지침 제56조(용역사업 보안관리)

교육 내용

- 정기 보안교육으로 보안의식 향상
- 보안 사고 사례 전파 및 보안준수 사항 등 보안 경각심 제고

I. 개요
교육 목적 및 추진 근거

교육 목적

용역업체와 발주기관의 보안에 대한 공동 인식 제고 및 노력

(고도의 해킹이 아닌 **관리의 소홀**로 인한 자료유출 피해에 대한 대비)

최근 **업무 · 인터넷망이 분리되지 않은** 지자체를 대상으로

인터넷망과 연결되어 있거나 보안프로그램 미설치 등

보안관리가 미흡한 용역업체의 전산장비(PC · 서버)를 해킹하여

업무자료를 절취하는 침해사고가 지속 발생

2. 최신 보안 동향

Ⅱ. 정보보안동향 주요 침해 사례

2025년 SK텔레콤 유심 해킹 사건

위키백과, 우리 모두의 백과사전.

2025년 SK텔레콤 유심 해킹 사건은 2025년 4월 18일 대한민국의 정보이동통신사인 SK텔레콤 고객의 유심 정보를 해커가 유출한 사건이다.[1] SK텔레콤 전산망에서 해킹이 발생했지만 2025년 4월 29일 기준 현재까지 해커의 침입 경로와 정확한 피해 규모를 확인하지 못해 SK텔레콤에 대한 비판이 높아지고 있다.[1] 해당 해킹 사건 이후 SK텔레콤은 유심 보호 서비스 및 유심 무료 교체 등의 대책을 내놓았지만 유심 물량이 고객 숫자에 비해 많이 부족한 것으로 드러나 대처가 미흡하다고 평가받고 있다.[2] 은행을 비롯한 금융권은 SK텔레콤을 통한 신원 인증을 중단했고, SK텔레콤 고객들은 SK텔레콤의 미흡한 대처와 제대로 파악되지 않은 피해 규모에 국민청원에 이를 게시하고 집단 소송을 준비하고 있다.

2025년 SK텔레콤 유심 해킹 사건

사건 직후 인천국제공항에서 출국 전 유심 교체를 위해 줄을 서 있는 고객들

위치	대한민국
원인	조사중
최초 보고자	SK텔레콤

전개 [편집]

대한민국의 이동통신사인 SK텔레콤 (SKT)는 2025년 4월 19일 오후 11시 40분쯤 해커의 악성코드로 인해 유심 관련 일부 정보가 유출되었으며, 20일 한국인터넷진흥원에 사고를 신고했다고 밝혔다.[3] 해킹된 장비는 LTE(4G) 및 5G 고객들이 휴대전화로 SKT의 음성 통화 서비스를 이용할 때 SKT의 휴대전화가 맞는지 확인하는 서버인 것으로 전했다. 이로 인해 국제 이동국 식별 번호(IMSI), 단말기 고유식별번호(IMEI), 유심 인증키가 유출되었다. 국제 이동국 식별 번호(IMSI)이 유출되면 통신 신호를 도청하거나 스푸핑 등이 가능해지고, 단말기 고유식별번호(IMEI)가 유출되면 문자 및 통화 위장, 보이스피싱, 스미싱 표적 설정이 된다. 가장 중요한 '유심 인증키'가 유출되면 유심을 복제하는 것(심 클리닝)이 가능하여 타인이 유심 인증키가 유출된 사람의 명의로 대출을 하거나 그 사람의 계좌에서 돈을 가져가는 등의 금전적 피해가 발생하게 된다.[4] 해킹 공격으로 최대 9.7GB 분량의 정보가 외부 유출된 정황이 나왔다.[5]

Ⅱ. 정보보안동향 주요 침해 사례

2025년 11월, 쿠팡 회원들을 대상으로 중국인으로 추정되는 전직 내부 직원(이하 개발자 A)[A]에 의해 발생한 개인 정보 유출 사태. 약 3,370만 개에 달하는 회원의 성명, 주소, 연락처 등이 대량으로 유출된 것으로 확인되었다. 추후 쿠팡의 정부와의 합동조사[8]에 따르면, 쿠팡은 유출자를 특정하였고 고객 정보 유출에 사용된 모든 기기가 회수되었다고 발표하였다. 현재까지의 조사에 의하면 유출자는 약 3,000명의 제한된 고객정보[9]만 저장하였고, 현재는 이를 모두 삭제했다고 한다.

2026년 2월 5일 지난해 발생한 개인정보 유출 사고와 관련해 기존 조사 과정에서 16만 5000여 계정의 개인정보가 추가로 확인됐다. #

Ⅱ. 정보보안동향 주요 침해 사례

신한카드 가맹점주 19만명 개인정보 유출

등록기자: 송정배 [기자에게 문의하기]

신한카드에서 가맹점주 19만명의 휴대전화번호 등 개인정보가 유출됐다. 앞서 발생한 쿠팡의 대규모 개인정보 유출 사고와 마찬가지로 내부 직원에 의해 정보가 대거 빠져나갔다. 롯데카드 해킹 사고 이후 금융권 정보 보안에 대한 경각심이 커진 상황에서 신용카드 업계 가입자 1위인 신한카드까지 내부통제 소홀로 인한 유출 사고가 터지면서 정보보안에 대한 우려가 더욱 커지고 있다.

롯데카드 개인신용정보 유출 사고		
발생일		해킹 발생일: 2025년 8월 14일 ~ 8월 15일 해킹 신고일: 2025년 9월 1일 공식 발표일: 2025년 9월 18일
가해자		불명(조사 중)
피해 기업		롯데카드
피해자		롯데카드 이용자
유형		정보 유출
주요 원인		**해킹으로 인한 악성코드 감염**
피해규모	해킹 피해	악성 코드 2종, 웹쉘 5종[1] 발견 서버 3대 감염
피해규모	유출 정보	데이터 약 200GB 유출[2] 고객 온라인 결제 정보 및 암호화된 카드번호(222만 명) 고객 개인정보[3] 및 암호화된 카드번호(47만 명) 고객 카드번호, 비밀번호, 유효기간, CVC, 개인정보[4] (22만 명)
관할		

Ⅱ. 정보보안동향 주요 침해 사례

넷마블 개인정보 유출 사건	
발생일	해킹 발생일: 불명 공식 발표일: 2025년 11월 27일
피의자	불명
피해 기업	넷마블
피해자	**1차 발표** • **넷마블 이용자 약 611만 명** • 2015년 이전 PC방 가맹점 6만 6천여 개 사업주 • 넷마블 전현직 임직원 **2차 발표** • 넷마블 고객센터 문의 고객 • 넷마블 온라인 입사지원자 및 잡페어 부스 방문자 • 외부 B2B 사업 제안 담당자 등
유형	개인 정보 유출 사태
주요 원인	불명
관할	미정

[대성학력개발연구소] 개인정보 유출 관련 안내

먼저 저희 (주)대성학력개발연구소의 서비스를 신뢰하고 사랑해 주신 고객님께 심려 끼쳐드린 점 머리 숙여 사과드립니다.

당사는 고객님의 개인정보 보호를 위해 최우선으로 노력하여 왔으나,
당사가 파악한 바로는 성명불상의 권한 없는 제3자가 2025. 7. 18. 오후 2시~2시 30분경 사이 불상의 방법으로 무단으로 사내 시스템에 접속하여 개인정보파일에 접근한 것으로 추정됩니다.

유출로 의심되는 고객님의 개인정보 항목은
성명, 휴대전화번호, 이메일 주소, 아이디, 생년월일, 유선전화, 주소, 카카오ID, 네이버ID(총 9건)이며, 정보 주체에 따라 그 항목은 상이합니다. 당사는 유출 의심 정황 발견 즉시 피해를 최소화하기 위해 아래와 같은 조치를 완료하였습니다.

1. 외부에서 접속 가능한 접속 포트 전부 차단, 랜선 접속 모두 차단
2. 사내 시스템 접근 및 데이터 처리와 관련된 로그 분석
3. 윈도우 및 DB 로그인 계정정보 변경
4. 시스템 취약점 점검 및 보완 조치
5. 시스템 모니터링 강화 조치

Ⅱ. 정보보안동향 주요 침해 사례

국립대학병원 (2026.01)

- PACS 시스템 랜섬웨어 감염
- 전남대·강원대병원 진료 차질

전남대병원 랜섬웨어 공격…PACS 한때 '마비'

행정부서 PC 악성코드 '유입'…영상판독 일부 차질·개인정보 유출 '무(無)'

2026.01.27 11:53 댓글쓰기

전남대학교병원이 외부 랜섬웨어 공격으로 영상검사 시스템이 일시 마비되는 사태가 발생했다.

병원 측은 긴급 복구에 나서 하루 만에 시스템을 정상화했으나, 상대적으로 보안이 취약한 의원급 뿐만 아니라 지역 거점 국립대병원까지 사이버 공격 타깃이 되면서 의료계 전반의 보안 경각심이 요구된다.

강원대학교 병원 랜섬웨어 공격으로 한때 진료 차질..."현재 정상화"

2026. 1. 28. 13:18

댓글로 함께해요

[강원대병원 제공]

강원대학교병원이 랜섬웨어로 추정되는 사이버 공격을 받아 한때 진료에 차질을 빚었습니다.

병원 측에 따르면 지난 26일 오전 4시쯤 병원 전산망이 사이버 공격을 받았습니다,

공격자는 암호 해독을 대가로 수억 원 상당의 비트코인을 요구한 것으로 알려졌습니다.

이로 인해 MRI와 CT 등 의료영상 시스템 사용이 제한되며 진료에 불편이 발생했습니다.

Ⅱ. 정보보안동향 주요 침해 사례

'개인정보 침해 논란' 딥시크, 정책 변경…中 정보 보관 그대로

송고 2025-02-15 13:21

이상서 기자

+ 구독

키보드 패턴 등 민감정보 수집 삭제…유럽 이용자 보호 추가 약관 마련했으나 한국은 없어

개인정보위, 지난달 말 딥시크에 공식 질의…"아직 답변 안 와"

(서울=연합뉴스) 이상서 기자 = 민감정보를 포함한 과도한 개인정보 수집 논란을 빚어온 딥시크가 개인정보 처리방침을 일부 개정한 것으로 확인됐다.

이번 개정을 통해 유럽 국가의 개인정보 수집에 관한 별도의 약관을 마련했으나, 한국에 대한 언급은 없어 개인정보보호위원회 등 관계 기관의 적극적인 대처가 요구된다.

Ⅱ. 정보보안동향

핵심 시사점

기술적 취약점 방치
관리 및 모니터링 미흡
상시 점검 및 대응 체계 강화

대규모 고객 정보 유출 발생


3. 용역사업 보안관리

Ⅲ. 용역사업보안관리

용역사업 수행 시 단계별 점검사항

계약 및 착수

- 보안서약서 제출 (대표 및 전원)

인원·물리 보안

- 정기 보안 교육 이수
- 비인가 USB 금지
- 수행공간 보안 점검

자료·네트워크 보안

- 산출물 지정 서버 저장 (개인 전송 금지)
- 전산망 분리 및 접근 통제 (HIWARE 사용)

Ⅲ. 용역사업보안관리

보안관리 책임 및 비밀유지 의무 준수사항

다음 정보를 무단으로 누출할 경우, 관련 법규에 따라 즉각 '부정당업자' 제재를 받게 됩니다.

정보시스템 현황
시스템 구성 정보

사업 결과물
소스코드 및 산출물

접근 정보
계정 및 접근 권한

개인정보
모든 개인정보

Ⅲ. 용역사업 수행 시 준수사항

보안관리 및 책임

< 의 무 >

- 계약자는 **이용기관의 정보통신실 출입 시 이용기관의 시스템 담당자나 전남대학교가 요구하는 보안사항 및 점검내용**을 충실히 이행하여야 한다.
- 계약자는 유지보수 장소에 출입한 자의 신원에 대한 책임을 지고 **유지보수 활동을 통하여 취득한 기밀사항과 다음 각 호에 대하여 보안을 유지**하여야 한다.

< 관련 규정 및 처벌 내용 >

- 정보노출 적발 시 『국가를 당사자로 하는 계약에 관한 법률 시행규칙』 제17조에 근거
- 해당업체를 부정당업자로 등록 및 입찰 참가자격 제한 등 제재 조치할 수 있음.

Ⅲ. 용역사업 수행시 준수사항

(보안관리 및 책임)

<의무>

- 계약자는 당해 계약을 통하여 얻은 정보 또는 국가의 기밀 사항을 계약 이행의 전, 후를 막론하고 외부에 누설할 수 없다.
- 계약자는 업체 대표 및 유지보수 제반 업무를 처리하는 모든 인원에 대하여 보안서약서를 제출하여야 한다.
- 계약자는 시스템이나 전남대학교에서 직접, 간접으로 취득한 비밀을 제3자에게 누설하여서는 안되며 보안 사항의 누설로 인한 문제 발생시 계약자는 민,형사상 책임을 진다.

비밀유지 의무 준수사항

비밀유지 및 제재사항

용역사업 수행 시 제출된 보안서약서에 의해 용역사업 참여자는 대학이 정한 기밀 및 누출금지 대상 정보에 대해 일체 누설하거나 공개하여서는 아니되며, 이를 위반할 시, 관련법령 및 계약에 따라 법적 처벌을 받으며, 해당 용역수행 업체는 부정당업자 제재조치를 받게 됨.

<국가계약법 시행령 제76조(부정당업자의 입찰참가자격 제한) 제1항제3호나목에 해당하는자>

전자정부법 제2조제13호에 따른 정보시스템의 구축 및 유지보수 계약의 이행과정에서 알 알게 된 정보 중 각 중앙관서의 장 또는 계약담당공무원이 누출될 경우 국가에 위해가 발생할 판단하여 사전에 누출금지 정보로 지정하고 계약서에 명시한 정보를 무단으로 누출한 자

비밀유지 의무 준수사항 – 누출금지 대상정보

누출금지 주요 대상정보

- 전남대학교 정보시스템의 내,외부 IP주소 현황
- 세부 정보시스템 구성 현황 및 정보통신망 구성도
- 사용자 계정, 비밀번호 등 정보시스템 접근권한 정보
- 정보통신망 취약점 분석, 평가 결과물
- 정보시스템 용역사업 결과물 및 관련 프로그램 소스코드
- 누출 시 안보, 국익에 피해가 우려되는 중요 용역 사업일 경우 해당
- 보안시스템 및 정보보호시스템 도입 현황
- 정보보호제품 및 네트워크 장비 설정 정보
- 비공개 대상 정보로 분류된 기관의 내부문서, 대외비
- 개인정보보호법에 따른 개인정보 및 개인 영상 정보

용역사업 수행시 점검사항 – 인원 및 물리적 보안관리

점검 주요 내용

용역사업 참여인원 보안서약서 징구
(정보 누출 금지 및 친필 서명)

용역사업 수행 전 보안교육 실시
(비밀유지 의무 및 위반시 처벌 등)

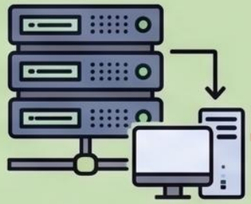
사업 수행 중 업체 인력 보안점검
(누출금지 정보 유출여부 등)

수행 공간 정기 보안점검 및 비인가 USB 사용 금지
(산출물 저장용 승인 후 사용)

용역사업 수행시 점검사항 – 자료에 대한 보안관리

자료 보안 점검 주요 내용

누출금지 대상정보 업체 제공 시 '자료관리 대장' 작성
(무단 복사 및 외부반출 금지, 완료 시 회수)



산출물은 전남대학교 파일 서버 또는 담당자 지정 PC에 저장

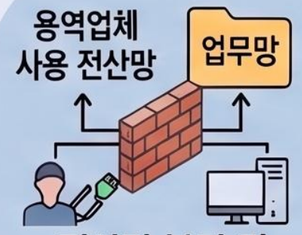
상주인원 비공개 자료 매일 퇴근 시 반납
(일반문서는 시건장치 보관함 보관)

자료 전송 시 자체 전자우편 이용 및 첨부자료 암호화
(대외비 이상 비밀 송수신 금지)

용역사업 수행시 점검사항 - 네트워크 및 시스템 접근 보안관리

네트워크 및 시스템 접근 점검 주요 내용

01



용역업체 사용 전산망은 해당 기관 업무망과 분리구성하고 업무상 필요한 서버에만 제한적 접근 허용

02

접근제어시스템(HIWARE) 사용자 계정(ID)은 계정 별 정보시스템 접근권한을 차등 부여하되 기관 내부문서 접근 금지

03

계정별로 부여된 접속권한은 불필요시 곧바로 해지. 업체 PC는 인터넷 금지하되, 사업 수행상 필요한 경우 통제 하에 제한적 허용
(P2P, 웹하드 등 인터넷 자료공유사이트 접속차단)

04

업체 사용 PC에 최신 백신 프로그램 설치, 비밀번호, 화면보호기 설정 등 주기적 PC점검 실시

기관 외부에서 기관 내부 시스템 개발 PC 및 기관 시스템에 원격 접속 금지

[개선된 보안 점검] 사업 완료시 필수 점검사항

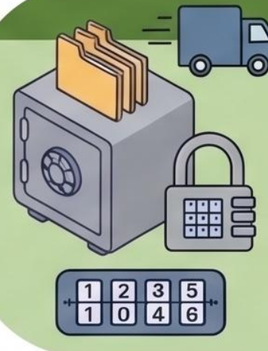
4단계 프로세스로 확인하는 보안 점검 내용

01

최종 산출물 대외비 관리

- 보안이 요구되는 자료는 대외비 이상으로 분류하여 엄격히 관리

02



제공 자료 및 산출물 전량 회수

- 제공된 모든 자료 및 용역 결과물 반납 완료
- 업체 복사본 또는 별도 보관 절대 금지

03

전자기록 완전 삭제 및 증빙

- 업체 소유 PC/서버 하드디스크, 휴대용 저장매체 완전 삭제 조치
- 완료보고서 제출 시 삭제 사진 등 증빙 자료 필수 첨부

04

관련자료 미보유 확약 및 서약

- 자료 회수 및 삭제 조치 후 업체 대표 명의 미보유 확약서 징구

보안서약서

- 보안서약서 추가 징구로 최종 보안성 강화

⚠ [최종 확인] 모든 점검사항 완료 후 사업 담당자의 승인 하에 사업 종결 처리

사업완료시 점검사항

1. (공문) 완료계

2. 사업완료보고서 : 구축 완료 내역, 향후 유지관리(조직도, 지원체계 등), 하자보수, 훈련계획 등

※ 반드시 포함) 발주기관 소유의 결과물 완전 삭제하였다는 포멧 사진 등

※ 반드시 포함) 개발사업의 경우, 취약점 점검 및 조치 사항

3. 대표 명의 확약서 및 보안서약서

4. 검사검수요청서

5. 그 외 제안요청서(과업지시서)에서 검수기관에서 요청한 사항 등

단계별 문서 정리

계약시
(At Contract Signing)

- 보안서약서
- 비밀유지서약서
- 개인정보처리위탁계약서(대상 시)

대표 참여인력

수행시
(During Execution)

계약시 기준

참여인력

종료시
(At Completion)

- 보안확약서(업체대표)
- 보안서약서(참여인력)

대표 참여인력

Ⅲ. 용역사업보안관리

사업 완료 시 점검사항 (외부 업체 대상)

- ✓ 자료 및 산출물 전량 반납
- ✓ 저장매체 데이터 완전 삭제 및 증빙
- ✓ 보안 문서 이관 및 대표자 보안확약서 제출


4. 개인정보보호
개인정보보호

Ⅳ. 개인정보보호

업무위탁과 제3자 제공의 명확한 구분

업무위탁 (수탁자: 용역업체)	제3자 제공 (제3자)
• 목적: 발주처 업무 대행 • 이익 귀속: 발주기관 • 관리/감독: 발주기관의 철저한 감독 • 정보주체 동의: 원칙적 불필요 (처리방침 공개)	• 목적: 제3자의 독자적 이익 • 이익 귀속: 제3자 • 관리/감독: 제공 후 제3자 자체 책임 • 정보주체 동의: 반드시 사전 동의 필요

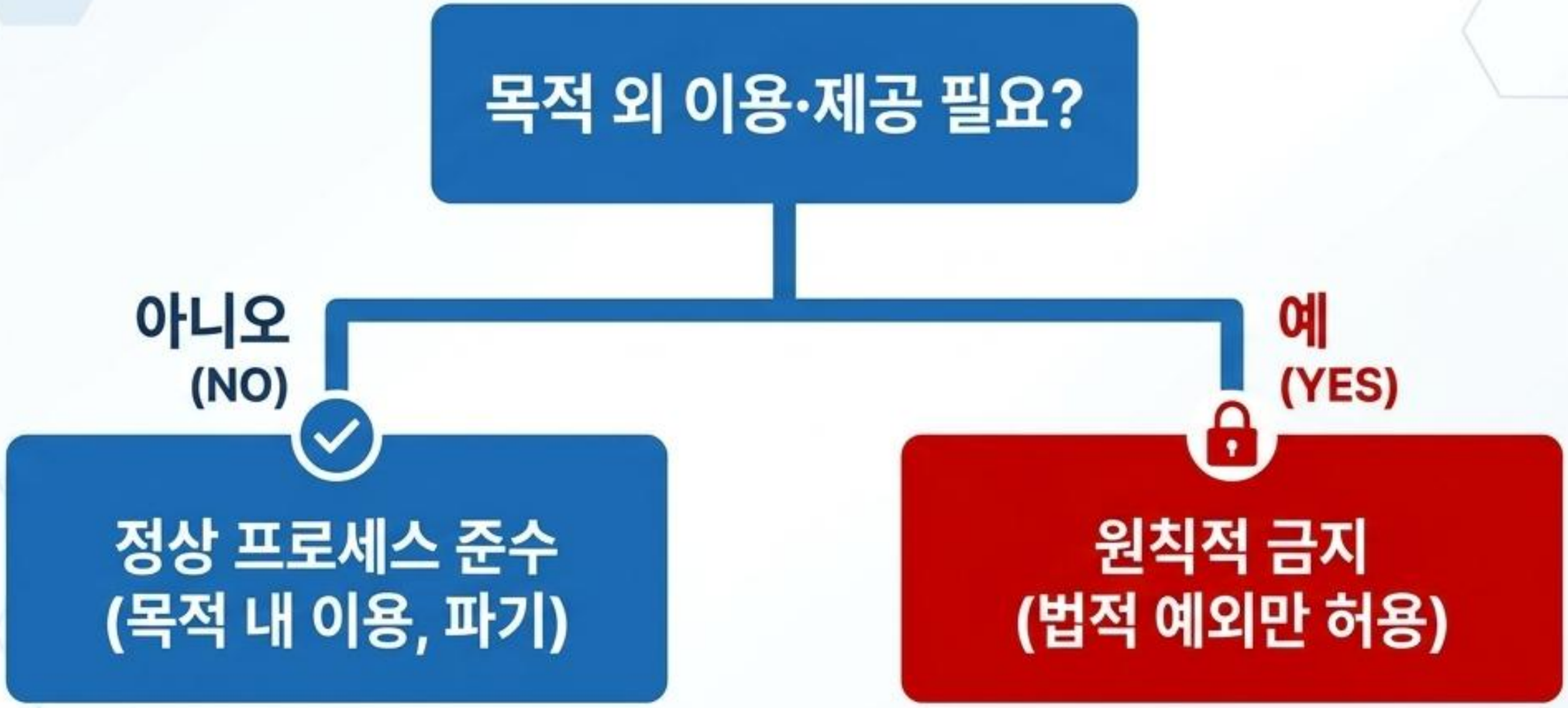
핵심: 용역업체는 '업무위탁(수탁자)'에 해당하며, 발주기관의 감독 하에 지정된 목적(사업수행)으로만 개인정보를 취급해야 합니다.

Ⅳ. 개인정보보호

업무 위탁과 제3자 제공의 구분

구 분	업 무 위 탁	제 3 자 제 공
관련조항	법 제26조	법 제17조, 제18조
예시	배송업무위탁, 전산관리 위탁	경찰에 수사자료제출
목적	위탁자의 이익을 위해 처리	제3자의 이익을 위해 처리
이전방법	위탁사실 공개	제공목적 등 고지 후 정보주체의 동의 획득
관리감독 책임	위탁자 책임	제공받는 자 책임
손해배상 책임	위탁자 책임(사용자책임)	제공받는 자 부담

IV. 개인정보보호: 목적 외 이용 금지



주의: 테스트 데이터 사용 등 목적 외 이용은 **형사 처벌 대상**입니다.

IV. 개인정보보호: 목적 외 이용 금지

목적 외 이용 · 제3자 제공 방법 및 제한

< 제공방법>

- 휴대용 저장매체(USB메모리, CD 등)는 사용 불가 원칙
  - 제공되는 중요한 개인정보는 암호화 조치
  - 반출된 보조기억매체는 요청 기관의 제공 자료 확인 조치 후 즉시회수하여 개인정보 파기
- 물리적 이전 : 개인정보가 담긴 출력물이나 책자 등으로 제공하고 이용목적을 달성한 후에는 안전한 방법(파쇄, 소각)으로 파기
- 네트워크를 통한 개인정보의 전송 : 전용선 또는 VPN 등 안전한 전송망 이용, 중요 개인정보에 대한 암호화 조치 후 전송

기타 방법에 의해 자료 제공이 필요한 경우는 안전성 확보 조치 등에 대해 개인정보 담당자와 협의를 거쳐 제공

5. 보안 위규 처리

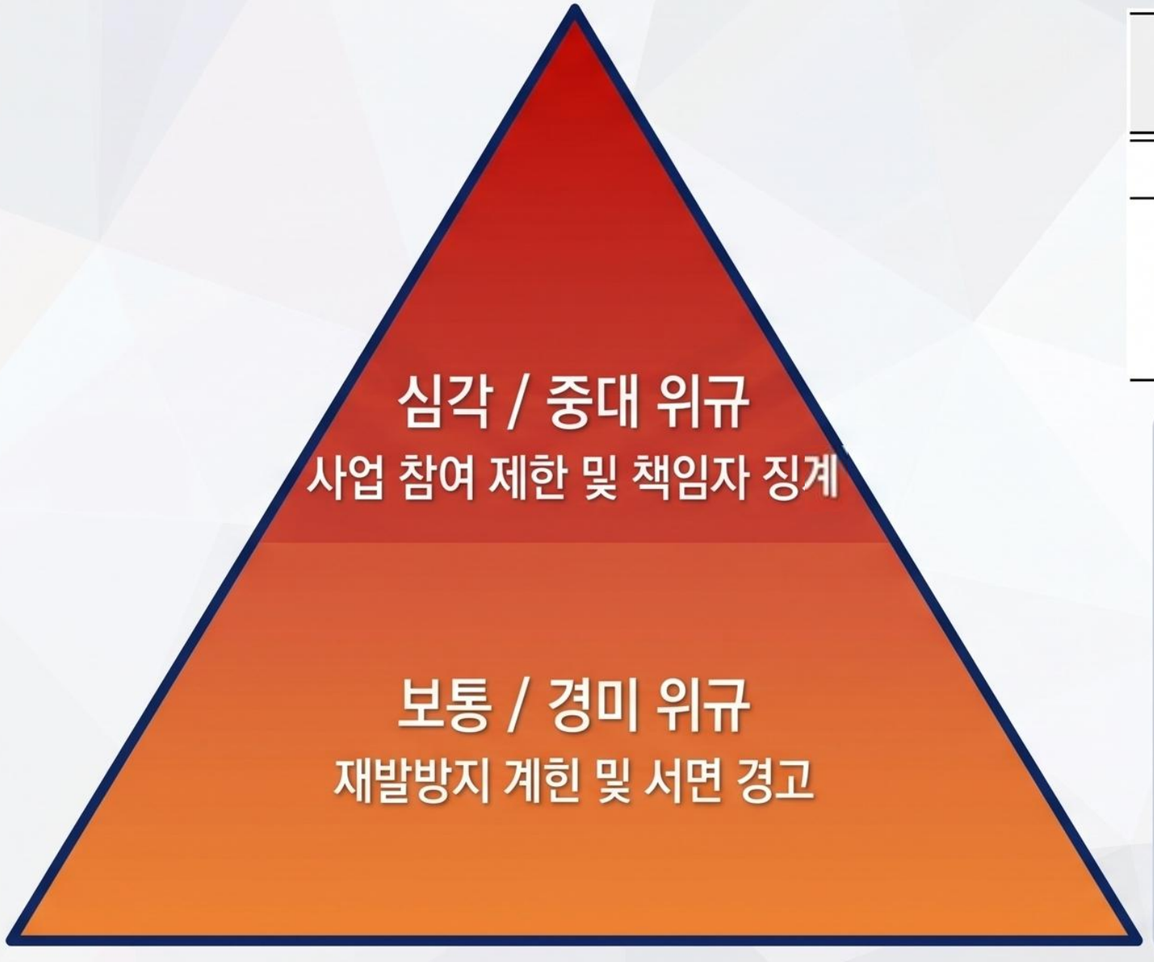
V. 사업자 보안위규 처리 관련

위규사항에 대한 처리 기준

구분	위 규 사 항	처 리 기 준
심각	1. 비밀 및 대외비 급 정보 유출 및 유출 시도 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	- 사업 참여 제한 (부정당업체 등록) - 위규자 및 직속 감독자 OO 등 중징계 - 재발 방지를 위한 조치계획 제출 - 위규자 대상 특별 보안교육 실시
중대	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 관리 소홀 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 사진 촬영 3. 전산정보 보호 대책 부실 가. 업무망 인터넷망 혼용사용, 보안 USB 사용 규정 위반 나. 웹하드·P2P등 인터넷 자료공유사이트를 활용하여 용역사업 관련 자료 수·발신 다. 개발·유지보수 시 원격작업 사용 라. 저장된 비공개 정보 비밀번호 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 OO 등 중징계 - 재발 방지를 위한 조치계획 제출 - 위규자 대상 특별 보안교육 실시

구분	위 규 사 항	처 리 기 준
보통	1. 기관 제공 중요정책·민감 자료 관리 소홀 가. 주요 현안 보고자료를 책상 위 등에 방치 나. 정책·현안자료를 휴지통·폐기함 등에 유기 또는 이면지 활용 다. 사무실 보안관리 부실 라. 캐비넷·서류함·책상 등을 개방한 채 퇴근 마. 출입키를 책상 위 등에 방치 2. 보호구역 관리 소홀 가. 통제·제한구역 출입문을 개방한 채 근무 나. 보호구역 내 비인가자 출입허용 등 통제 미실시 3. 전산정보 보호대책 부실 가. 휴대용 저장매체를 서랍·책상 위 등에 방치한 채 퇴근 나. 비인가 메신저 무단 사용 다. PC를 켜놓거나 보조기억매체(CD, USB 등)를 꽂아 놓고 퇴근 라. 부팅·화면보호 비밀번호 미부여 또는 "1111" 등 단순숫자 부여 마. PC 비밀번호를 모니터 옆 등 외부에 노출 바. 비인가 보조기억매체 무단 사용	- 위규자 및 직속 감독자 OO 등 중징계 - 위규자 및 직속 감독자 사유서/경위서 징구 - 위규자 대상 특별 보안교육 실시
경미	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. PC 내 보안성이 검증되지 않은 프로그램 사용 나. 보안관련 소프트웨어의 주기적 점검 위반	- 위규자 서면·구두 경고 등 문책 - 위규자 사유서/경위서 징구

Ⅴ. 사업자 보안위규 처리 관련 위규사항에 대한 처리 및 위약금 기준



위규사항에 대한 위약금 부과 기준

구분	위규 수준			
	A급	B급	C급	D급
위규	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금 비중	<예시 > 계약금액의 20%(또는 금액 _____원 이하) 및 부정당당자 동록	<예시 > 계약금액의 10% 이하 (또는 금액____원 이하)	<예시 > 계약금액의 5% 이하 (또는 금액____원 이하)	<예시 > 계약금액의 3% 이하 (또는 금액____원 이하)

- (위) 위규 수준별로 등급으로 차등 부과
- 보안 위약금은 다른 요인에 의해 상쇄, 삭감이 되지 않도록 부과
- 사업 종료 시 지출금액 조정을 통해 위약금 정산
- 보안규정을 위반하거나 누출금지 정보를 유출로 인해 손해 발생 시 용역업체에 민사상 손해배상 청구
- 보안 위반에 따른 위약금액, 제재조치 기준 등은 수요기관의 보안심사위원회에서 사안의 경중과 위반자의 고의성을 감안하여 확정

절대 주의 사항: 위약금은 별도 부과되며 감면 불가

감사합니다