2026년
분임보안담당자
정보보안 교육

교육 일자: 2026년 6월 26일

교육 부서: 전남대학교 정보화본부

CONTENTS

01. 분임보안담당자 법적 지정 근거 및 의무

규정 제3조에 의거, 당해 직위 임용과 동시에 분임보안담당관 임무 자동 부여

지정 대상 명시 (규정 제3조 제2항)

본부 각과의 과장 및 각 대학/소속기관의 행정실(팀)장(또는 서무책임자)은 임용과 동시에 당연직 분임보안담당관으로 지정됨.

법적 의무 수행 (규정 제3조 제4항)

보안담당관(총무과장)의 지휘·감독을 받아 소속 부서 내 보안 점검, 보안 감사 대비 및 보안사고 발생 시 즉시 보고 절차 수행.

부서 총괄 책임

보안 전문성 유무와 상관없이 소속 부서원 전체의 보안 관리 상태를 상시 지도·감독해야 할 행정적 연대 책임 보유

- **사전 예방**
  - 상시 보안 점검 및 위규 적발
- **감사 대비**
  - 상급기관 보안 감사 수감 철저
- **사고 보고**
  - 징후 발견 즉시 비상 핫라인 보고

02. 보안서약서 징구 대상 및 정보화사업 보안성 검토 의무

수탁업체 용역 계약, 정보화사업 착수 전 보안 서약 및 보안성 검토 필수

직원 관리
(규정 제9조 및 제9조의2)

- 비밀업무 취급 임시직원 고용 시 계약서 내 민·형사상 책임 명시 및 **보안서약서 즉시 징구.**
- 재직 중 보안 교육 실시 및 퇴직 시 누설 방지 **보안서약서 추가 작성 의무.**

정보화사업 보안성 검토 의뢰
(규정 제37조)

기획 단계 (공고 전) → 계약 → 사업 수행 → 종료

조달청 용역 및 자체 계약을 통한 정보화사업(서버 구매, 네트워크 구축, 홈페이지 등) 수행 시 반드시 '사업 계획 단계(공고 전)'에 보안성 검토 공문 의뢰 필수.

- 사업수행 전 참여 용역 인력 전원에 대한 **개별 보안서약서 집행.**
- 사업 종료 후 개발 산출물 로컬 보존 여부 대조 및 **완전 소거** 확인할 것.

03. 부서 내 주요 침해사고 유형 및 초동 차단 요령

의심 메일 열람 및 미인가 불법 다운로드 시 즉시 네트워크 물리 격리 수행

주요 침해사고 경고

사례 1. 공공기관 사칭 타겟형 피싱 메일

교육부, 대학본부 혹은 상급기관을 사칭한 포털 비밀번호 변경 요청, 급여 명세서 등의 유도 링크 클릭 및 악성 첨부파일 실행으로 교직원 계정 유출.

사례 2. 미인가 프로그램 및 불법 다운로드

인터넷 우회 소프트웨어(VPN), 정품 인증 크랙(Crack), 불법 다운로드 파일 실행 시 랜섬웨어 감염 및 전사 행정망 내 백도어 침투 통로 제공.

사고 인지 시 초동 격리 행동 지침

- 감염 의심 즉시 PC 전원을 유지한 상태에서 랜선 물리적 분리(Wi-Fi 수동 차단) 조치할 것.
- 시스템 무단 포맷 및 재부팅 절대 엄금 (침해사고 로그 증적 보존 목적).

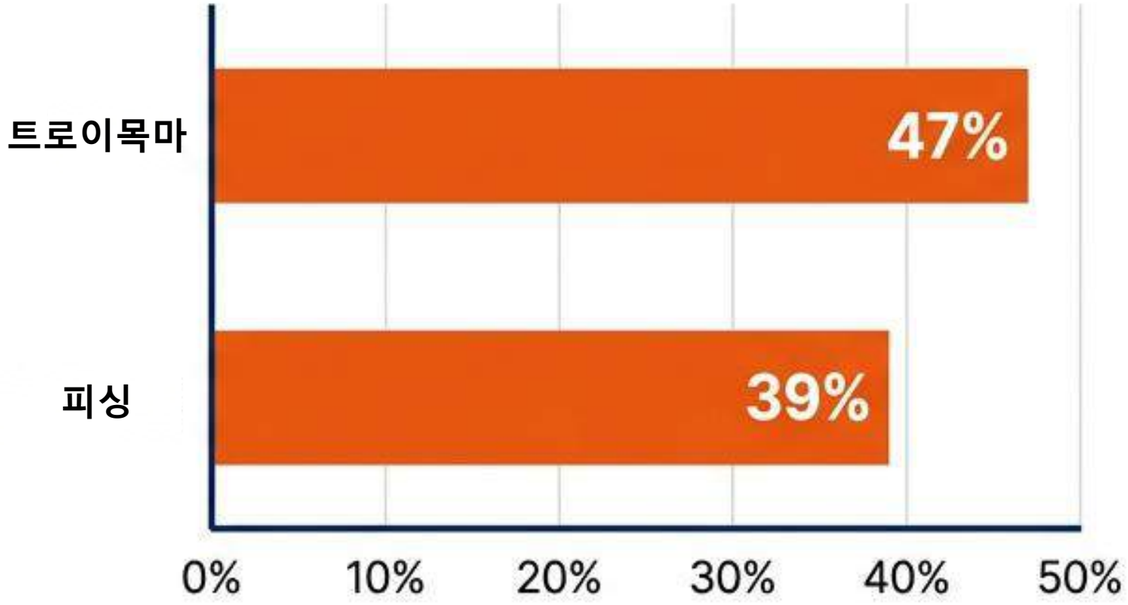
즉시 정보보안으로 사고 일시 및 증상 유선 신고 요망.

2026년 핵심 사이버 위협 동향

1. AI 기반 보안 위협의 부상 (출처: Samsung SDS)

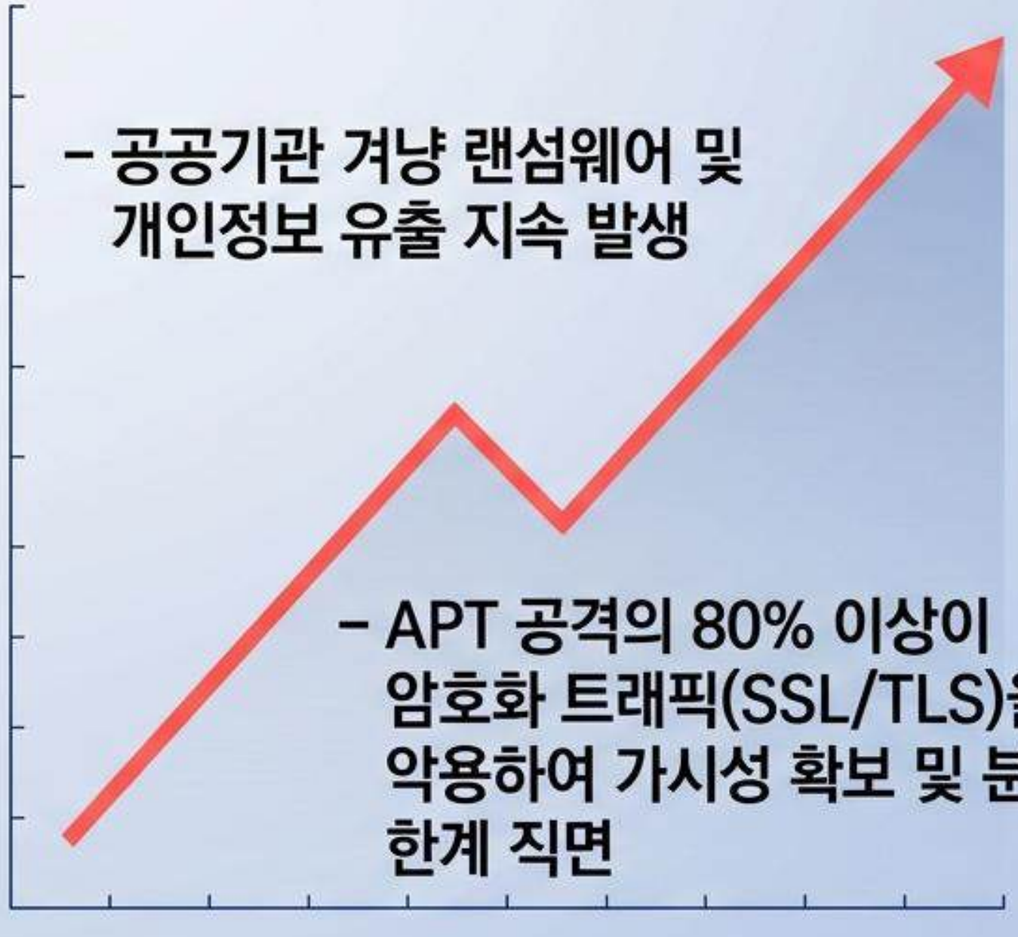
- **현황:** 2026년 주요 보안 위협 1위 (81.2% 차지).
- **분석:** 생성형 AI 악용 및 AI Agent의 과도한 권한 위임으로 인한 민감 데이터 유출 위험 고조.
- **영향:** AI 모델 변조 및 자율적 불법 명령 수행에 의한 내부 시스템 침해 우려.

2. 피싱 이메일 및 악성코드 고도화 (출처: ASEC)



- **현황:** 이메일 첨부파일 위협 중 Trojan(47%), Phishing(39%)이 압도적 다수 차지.
- **분석:** 통일부 등 공공기관 및 주요 기업을 사칭한 HTML 스크립트(가짜 로그인 페이지) 유포 급증.
- **영향:** ZIP(25%), PDF(17%) 등 정상 파일로 위장하여 실무자의 오인 클릭 유도 및 랜섬웨어 감염.

최근 위협 동향



분임보안담당관의 2대 핵심 임무 (정보보안 기본지침 제10조)

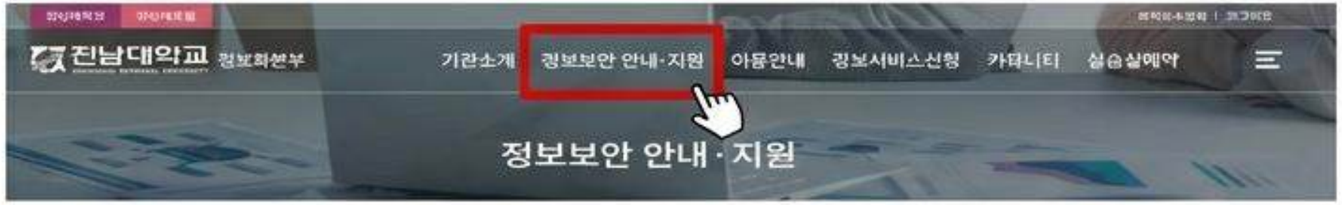
- 부서 내 일반·정보보안 및 개인정보보호 이행사항 총괄 및 준수
- 건물 내 정보통신(ICT) 인프라 및 물리적 시설(MDF룸 등) 관리 강화

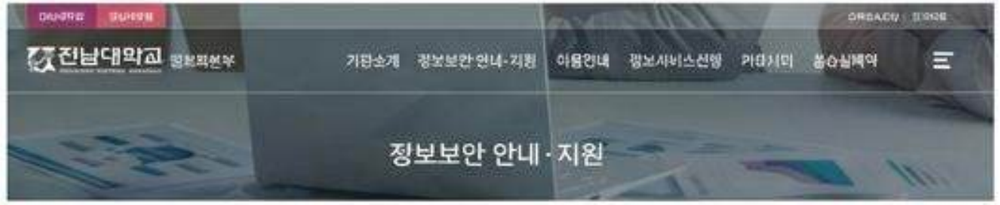
부서 내 관리 책임이 있는 정보자산(서버, PC 등) 목록 최신화 및 관리대장 현행화 실시

분임보안담당관(담당자) 핵심 임무 및 역할

정보보안 통합 안내 서비스 접속 경로 및 핵심 구성

정보화본부 홈페이지: 메인화면 ⇨「정보보안 안내·지원」 메뉴 클릭





전남대 포털: 홈페이지 최하단
⇨「정보보호 실천수칙」 바로가기 링크

대표 홈페이지: 홈페이지 최하단
⇨「정보보호 실천수칙」 바로가기 링크

[일상 보안]

- 정보보호 실천수칙
- 생성형 AI 활용 가이드
- 보안 공지 및 뉴스레터

[자산/시스템 보안]

- 시스템 보안성 검토
- 저장매체 관리 및 폐기

[행정/비상 지원]

- 업무 서식 다운로드
- 필수 S/W 매뉴얼
- 사이버위기 경보 안내

환경 변화에 따른 보안 콘텐츠 및 서식 상시 현행화 중

[일상 보안] 반드시 준수해야 할 10대 실천 수칙

PC 및 시스템 보호		데이터 및 네트워크 보호	
	**1. 백신 S/W 설치** (실시간 감시 활성화)	**6. 공유폴더 사용 최소화** (불가피할 경우 비밀번호 필수 설정)	
	**2. 의심스러운 전자우편 열람 금지** (출처 불분명 메일 즉시 삭제)	**7. 프로그램 신뢰성 확인** (인증서/서명 확인 후 설치)	
	**3. OS 보안 기능 활용** (자동 업데이트 및 방화벽 활성화)	**8. 중요 정보 안전한 저장** (PC 내 중요 문서 암호화)	
	**4. 안전한 비밀번호 설정** (영문/숫자/특수문자 조합, 주기적 변경)	**9. 정품 S/W 사용** (불법·비인가 S/W 금지)	
[필수]	**5. PC 접근 통제 강화** (부팅/로그인 및 화면보호기 비밀번호 설정 필수)	**10. 중요 자료 안전한 전송** (이메일 첨부파일 전송 시 비밀번호 설정)	

[주의/필수] 감사 대비 핵심 점검 사항
자리 이석 시 화면보호기(비밀번호 포함) 작동 누락은 자체 점검 시 가장 많이 지적되는 항목이므로, 즉각적인 단축키(Win+L) 사용 습관화 요망.

[일상 보안] 생성형 AI(ChatGPT 등) 안전 활용 가이드

- **목적**: AI 사용 중 발생할 수 있는 대학 내 중요 정보 및 개인정보 유출 원천 차단
- **필수 조치**: 각 AI 서비스 설정에서 '학습 데이터로 사용(Data Training)' 옵션 반드시 비활성화할 것

✓ 올바른 활용 (권장)	⊗ 위험한 활용 (절대 금지)
• **자료 요약**: 공공 데이터나 일반 논문 요약	→ • [주의] 개인정보가 포함된 명단 번역 및 요약
• **코드 작성**: 공개된 알고리즘 샘플 코드 생성	→ • [주의] 대학 내부 시스템 소스코드 업로드 및 분석
• **문서 작성**: 일반적인 안내문 초안 작성	→ • [주의] 비공개 내부 기안문 교정 및 수정

[주의/필수] 학생·교직원의 개인정보(성명, 학번 등) 및 행정 내부 문서 입력 절대 금지.
(부득이한 경우 고유 식별 정보는 'OOO' 등으로 비식별화 처리 후 입력함)

[자산/시스템 보안] 정보화 사업 보안성 검토 절차

신규 정보시스템 구축 및 사업 추진 시, 필수적으로 거쳐야 하는 3단계 보안성 검토 절차임.

[STEP 01] 계획 수립 (사업부서)

- 사업 진행 전 자체 보안 대책 수립
- 제출 서류: 신청서, 사업계획서, 제안요청서, 망 구성도 등

[STEP 02] 보안성 검토 (정보화본부)

- 관리적/기술적 보안 요소 검토 (암호화, 망 분리 등)
- 결과 통보: 적정, 조건부 적정, 부적정

[STEP 03] 사업 진행 (사업부서)

- 검토 결과 반영 및 이행 점검
- 완료 후 이행점검 확인 및 결과 보고서 제출

`[주의/필수]` 용역업체 권한 관리 (주요 감사 지적 사항)

시스템 개발을 위한 외부 용역업체 접근 권한은 사전 승인을 득해야 하며, 사업 완료 즉시 접근 권한을 회수해야 함.
(권한 회수 지연 시 외부 감사의 핵심 지적 대상이 됨)

[자산 보안] 신규 저장매체 등록 및 사용 승인 절차

인가되지 않은 USB, 외장하드 연결로 인한 악성코드 감염 및 자료 유출 방지 절차.

[STEP 01]

매체 연결:
PC 포트에
저장매체 삽입

[STEP 02]

승인 신청: PC FILTETER
팝업 또는 메인화면의
'사용매체 승인 신청' 클릭

[STEP 03]

목적 입력:
매체 식별 정보 및 상세
사용 목적 입력 후 요청

[STEP 04]

관리자 승인:
관리자(정보화본부) 승인
및 정책 업데이트 후
읽기/쓰기 가능

휴대용 저장매체 준수사항

- **일반용:** 행정전자서명 인증서 등 일반 자료 보관 시 사용 (개인 서랍/캐비닛 보관)
- **비밀용:** 비밀등급별 전용 매체 마련 및 이중 캐비닛/금고 보관 필수

개인 PC에 외부 매체 연결 시 반드시 사내 보안 솔루션(PC FILTER)을 통한 사전 승인을 통해야만 정상 작동

[자산 보안] 불용 저장매체 안전 파기 5단계

내용연수 경과, 고장 등으로 외부 반출·폐기되는 모든 저장매체(PC, 노트북, USB 등)의 데이터 완전 삭제 절차.

- **[STEP 01] 선별:** 정기 재물조사 등을 통해 불용 처리할 기기 선별
- **[STEP 02] 신청:** '불용 전산장비 저장매체 삭제 및 파기 요청서' 작성 후 공문 제출
- **[STEP 03] 접수:** 불용 전산장비를 정보화본부(내 PC병원)로 직접 제출
- **[STEP 04] 파기:** 물리적 파쇄 또는 데이터 완전 삭제 진행
- **[STEP 05] 완료:** 파기 완료된 장비를 최종 불용(매각/폐기) 처리

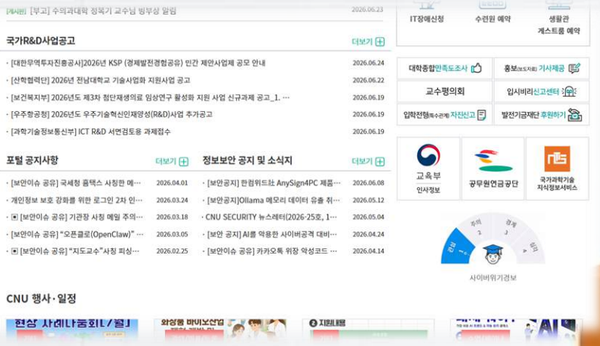
⚠ [주의/필수] '파기 확인서' 보관 의무

STEP 04 완료 후, 정보화본부로부터 반드시 '파기 확인서(공문)'를 발급받아 보관해야 함.

물리적 파기 증빙 누락은 정기 보안 감사 시 중대한 규정 위반으로 처리됨.

[비상 대응] 사이버위기 경보 단계별 행동 요령

사이버 공격의 수준에 따른 4단계 경보 발령 체계 및 실무 조치 사항.



단계: 심각
발령 기준: 전국적 대규모 피해 발생, 시스템 대규모 마비
조직 내 행동 요령: 대응 역량 총동원 (전사적 복구 및 차단 조치 실행)

단계: 경계
발령 기준: 복수 정보통신망 장애, 다수 기관 피해 발생
조직 내 행동 요령: 즉각 대응 태세 돌입 (비상 연락망 가동 및 모니터링 강화)

단계: 주의
발령 기준: 일부 정보통신망 장애, 국가위기로 발전 가능성
조직 내 행동 요령: 협조 체제 가동 (정보보호팀 및 유관부서 정보 공유)

단계: 관심
발령 기준: 해외 피해 확산 우려, 위기 발생 가능성 증가
조직 내 행동 요령: 위기 징후 감시 강화 (평시 대비 태세 점검)

사고 발생 시 즉각 조치
침해 사고나 정보 유출이 의심되는 즉시 PC 랜선(네트워크)을 분리하고, 정보화본부 정보보호팀으로 신속히 신고하여 확산을 차단할 것.

[행정 지원] 필수 서식 통합 제공 및 공통 보안 S/W 운영

1. 정보보안 업무 서식 통합 다운로드 (포털 게시판)

시스템 접근, 망 연결 등 행정 처리에 필요한 최신 양식을 일괄 제공함.

- ☑ 접근제어시스템 사용자 등록·변경·삭제 신청서
- ☑ 침입차단시스템(방화벽) 정책 신청서
- 보안서약서 (양식)
- ☑ 원격 접속 사용 신청서 (양식)

2. 3대 필수 공통 보안 S/W 및 정기 점검

AhnLab V3
실시간 악성코드 감시 및 자동 업데이트 활성화

PC FILTER
개인정보 포함 문서 탐지 및 USB 매체 통제

내PC보안점검
사용자 스스로 PC 취약점 점검 및 조치

매월 세 번째 수요일(사이버 보안 진단의 날)에 '내PC보안점검' 프로그램을 실행하여 도출된 취약점을 즉시 조치할 것.
(최초 설치 시 인사 데이터 동기화에 10~30분 소요 가능)

현위치: 감사 주요 지적 사항

퇴사자/계약 종료자 시스템 접근 권한 회수 누락

외부 용역 인력의 보안 서약서 징구 및 서명 누락

사전 협의 없는 임의의 방화벽 포트 개방 요청

핵심 달성 목표

절차 숙지: 시스템별 명확한 권한 신청 및 승인 프로세스 내재화

서류 완비: 용역 투입 전 필수 보안 서약 및 신청 서류 100% 구비

즉각 조치: 인력 변동 발생 시 즉각적인 권한 회수 체계 구축

보안 양식 4종 핵심 비교

양식명	사용 목적 및 대상	필수 서명권자	제출 방식 및 유효기간
원격 접속 신청서	외부망에서 내부망(학내 IP/서버) 접근 시	✅ 신청자, 확인자	전자공문 발송 (최대 2년)
보안 서약서	외부 용역 사업 투입 업체 및 인력	✅ 업체대표, 참여인력 전원	부서 자체 보관 및 감사 시 제출
방화벽 정책 신청서	특정 IP/Port 접근 허용 필요 시	✅ 신청자, 분임보안담당관	전자공문 발송 (최대 2년)
접근제어시스템 신청서	서버 직접 로그인 및 권한 필요 시	✅ 신청자, 분임보안담당관	전자공문 발송 (최대 2년)

1. 원격 접속(VPN) 사용 신청 가이드

원격 접속 사용 신청서

신청자(책임자)			포털 ID		
소 속			직 위(급)		
신청 구분	□등록 □변경 □연장 □삭제				
구 분	IP	포트	운영체제/호스트명	장비위치	
대상 장비	192.0.0.0.1	포트	운영체제/호스트명	장비위치	
	192.0.0.3	포트	운영체제/호스트명	장비위치	
	...	...	...	...	
신청 사유	*사유 작성*				
신청 기간	*2026. 1. 1. ~ 2028. 12. 31. (최대 1년, 미연장시 유효기간 이후 자동 차단)*				
사용자추가	ID(포털 ID)	성명	신분	휴대전화	이메일
추가 , 삭제			*신구원, 학생, 외부인 등*		

해당 시스템을 업무 목적에 한하여 사용하고, 업무상 취득한 정보를 비밀로 유지할 것을 서약하며, 이를 위반할 경우 관계 법령 및 내부 규정에 따른 책임을 부담함에 동의합니다.

년 월 일

신청자 : 소속 직위(급) 성명 (인)

확인자 : 소속 직위(급) 성명 (인)

정보화본부장 귀하

기본 원칙

- 외부망에서 접속 시 반드시 **SSL VPN 사용 필수**
- **최대 신청 가능 기간** : 1년 (기한 만료 시 자동 차단)

[주의/필수] 계정 발급 및 우회 금지

- **우회 금지** : FTP(21), SSH(22), HTTP(80) 등 알려진 포트(Well-known Port)는 기본 차단되므로, 필요 시 포트 번호 변경하여 운영할 것

[주의/필수] [감사 타겟] 미사용 계정 차단

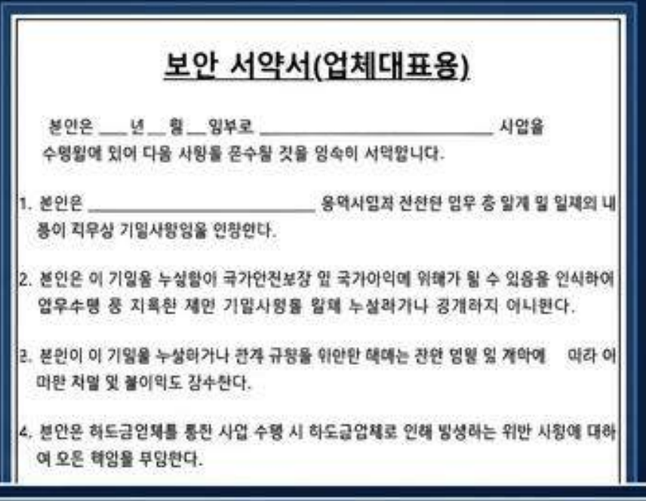
- 신청 기간 내라도 **3개월 이상 미사용 시** 즉시 자동 차단됨
- 보안 사고 발생 시 책임은 신청자 본인에게 귀속됨

2. 외부 용역 보안 서약서 징구

이원화 징구 체계

[패널 1: 업체대표용]

사업 착수 시 대표자 명의로 1부 징구
핵심 조항: 사업 기간 중 발생한 모든 기밀 누설에 대한 법적 책임 감수



보안 서약서(업체대표용)

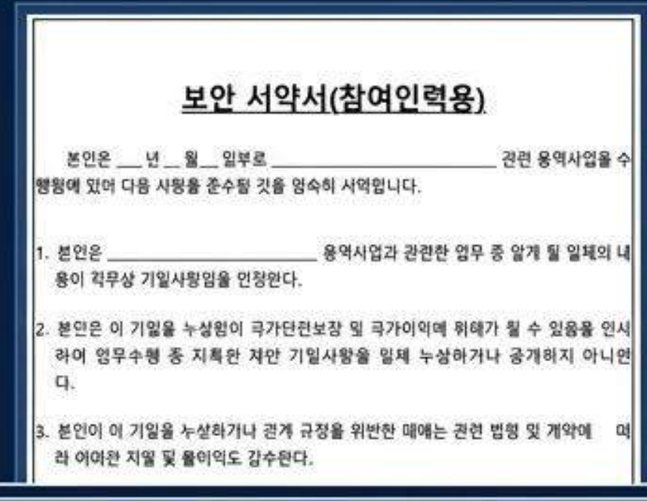
본인은 ___년 __월 __일부로 _____ 사업을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 _____ 용역사업적 전반적 업무 중 알게 될 일체의 내용이 직무상 기밀사항임을 인정한다.
2. 본인은 이 기밀을 누설함이 국가안전보장 및 국가이익에 위해가 될 수 있음을 인식하여 업무수행 중 지득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.
3. 본인이 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 이에 따른 처벌 및 불이익도 감수한다.
4. 본인은 하도급업체를 통한 사업 수행 시 하도급업체로 인해 발생하는 위반 사항에 대하여 모든 책임을 부담한다.

VS

[패널 2: 참여인력용]

사업에 투입되는 개별 인력 전원 징구
핵심 조항: 직무상 알게 된 일체의 내용에 대한 기밀 유지 의무



보안 서약서(참여인력용)

본인은 ___년 __월__일부로 _____ 관련 용역사업을 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 _____ 용역사업과 관련한 업무 중 알게 될 일체의 내용이 직무상 기밀사항임을 인정한다.
2. 본인은 이 기밀을 누설함이 국가안전보장 및 국가이익에 위해가 될 수 있음을 인식하여 업무수행 중 지득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.
3. 본인이 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 법령 및 계약에 따라 이에 따른 처벌 및 불이익도 감수한다.

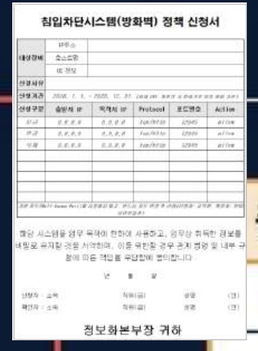
[주의/필수] [감사 타겟]
하도급 책임 및 서명 누락

- **하도급 연대 책임:** 업체대표는 하도급 업체를 통한 사업 수행 시, 하도급 업체의 위반 사항에 대해서도 모든 책임을 부담함 (대표용 서약서 제4조)
- **서명 누락 방지:** 자필 서명 또는 공인 전자서명 여부 교차 검증 필수 (타이핑 이름 불가)

3. 침입차단시스템(방화벽) 정책 신청

방화벽 개방 4단계 프로세스

사전 협의	신청서 작성	보안담당자 확인	공문 발송
신청 전 정보화본부 담당자와 타당성 및 포트 협의 (임의 신청 불가)	시스템 IP, Protocol, Port 번호 명확히 기재 (최대 2년)	부서별 정보보안담당관 (확인자) 결재 및 서명 필수	최종 서명 완료본을 첨부하여 정보화본부로 전자공문 접수


침입차단시스템(방화벽) 정책 신청서

정보화본부장 귀하

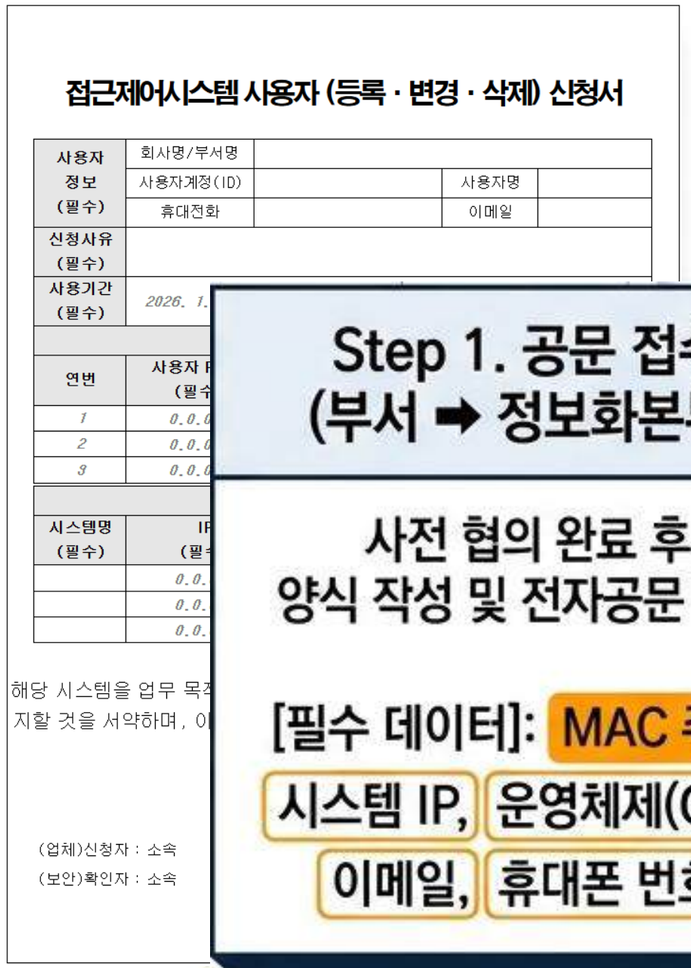
[주의/필수] 보안 준수 사항

- Well-known 포트 사용 지양: FTP, SSH, TELNET 등 기본 포트 사용은 보안상 엄격히 제한됨
- 반드시 시스템 포트 변경 후 신청할 것

출발지 IP	목적지 IP	Protocol	포트번호
0.0.0.0	0.0.0.0	tcp/http	12345
0.0.0.0	0.0.0.0	tcp/http	12345
0.0.0.0	0.0.0.0	tcp/http	12345
0.0.0.0	0.0.0.0	tcp/http	12345

4. 접근제어시스템 사용자 등록 및 관리

사용자 계정 발급 절차



접근제어시스템 사용자 (등록 · 변경 · 삭제) 신청서

사용자 정보 (필수)	회사명/부서명			
	사용자계정(ID)		사용자명	
	휴대전화		이메일	
신청사유 (필수)				
사용기간 (필수)	2026. 1.			

연번	사용자 I (필수
1	0.0.0
2	0.0.0
3	0.0.0

시스템명 (필수)	IP (필
	0.0.
	0.0.
	0.0.

해당 시스템을 업무 목적
지할 것을 서약하며, 이

(업체)신청자 : 소속
(보안)확인자 : 소속

Step 1. 공문 접수 (부서 ➡ 정보화본부)

사전 협의 완료 후
양식 작성 및 전자공문 발송

[필수 데이터]: MAC 주소, 시스템 IP, 운영체제(OS), 이메일, 휴대폰 번호

Step 2. 계정 생성 (정보화본부)

사용자 디렉토리 및 계정 생성

임시 비밀번호 발급 처리

Step 3. 결과 통보 및 접속 (정보화본부 ➡ 사용자)

담당자 이메일로 접속 매뉴얼
및 하이웨어 주소 통보

⚠ [주의/필수]: 최초 접속 시 반드시 즉각적인 비밀번호 변경 수행할 것

04. 정보화사업 서버 위탁 및 원격접근제어(하이웨어) 통제 의무

서버 위탁 및 원격 접속 통제

자체 서버 구축 금지 (서버 위탁 의무)

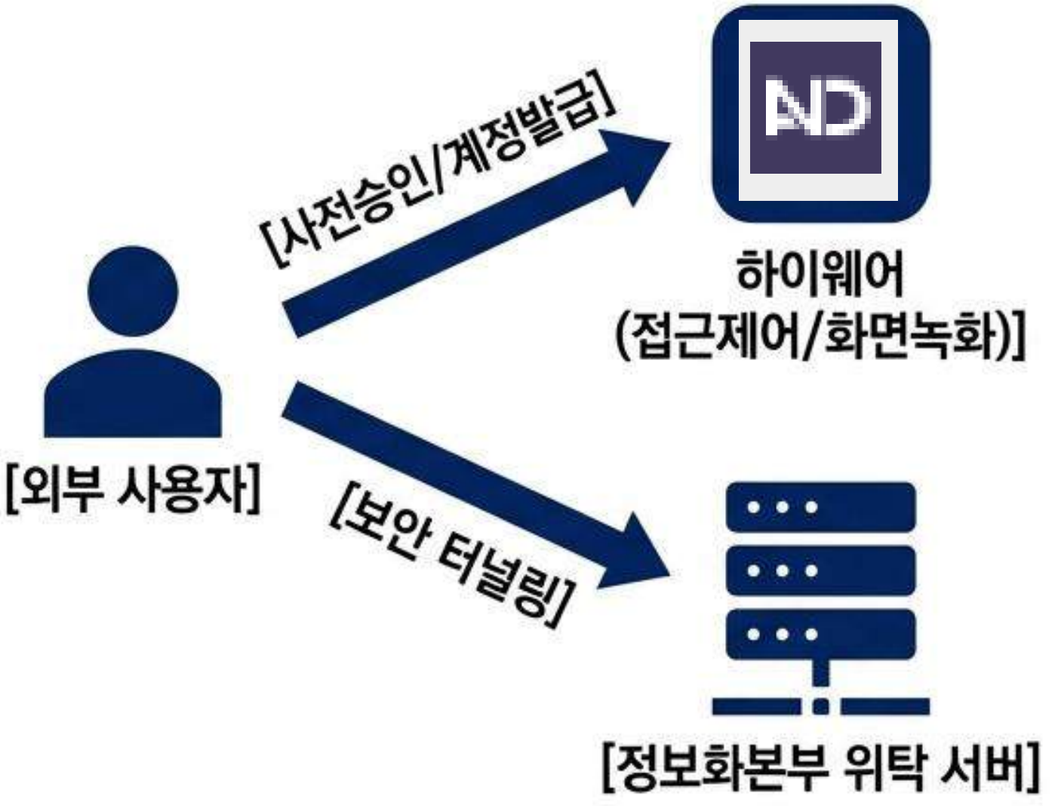
부서 내 서버 설치 불가.
모든 서버는 정보화본부 위탁 관리.

원격 접속은 공식 시스템 이용 (HIWARE)

사설 원격 프로그램 사용 금지.
승인된 HIWARE만 이용.

접속 기록 관리 및 권한 회수

모든 접속 내역 녹화 및 보관.
작업 완료 후 계정 즉시 회수.



최우선 점검 대상: 감사 단골 지적사항 Top 3

1. 퇴사/인력 변경 시 권한 회수 지연

[감사 지적] 용역 종료 또는 담당자 변경 후에도 방화벽/VPN 접근 권한 유지

변동 발생 당일, 즉각적인 삭제 공문 발송 및 계정 회수 처리

2. 서약서 및 신청서 서명(인) 누락

[감사 지적] 프린트된 이름만 있고 자필 서명이나 직인이 없는 서류 다수 발견

문서 취합 즉시 하단 '신청자' 및 '확인자' 서명란 1차 육안 검수

3. 목적 외 사용 및 기간 연장 미처리

[감사 지적] 신청 유효기간(1~2년) 만료 후 연장 신청 없이 불법 접속 시도

유효기간 만료 1개월 전 담당자 알림 설정 및 선제적 연장/삭제 판단

일상 보안 : 사이버 보안 진단의 날

- 일정: 매월 세 번째 주 수요일 시행
- 목표: 부서별 점검 이행률 80% 이상 필수 달성

1. 안내 및 독려
점검 당일 오전,

2. 점검 실행
내PC보안점검(알약 내PC지키미 등)
실행 및 취약점 100% 자동/수동 조치

3. 필수 SW 확인
의무 보안 SW(V3, PC-Filter 등)
정상 동작 및 최신 패치 여부 점검

[주의/필수] 점검결과 2개월 연속 이행률 80% 미만 시 별도 통보 및 집중 관리 대상 지정됨 /
[향후계획] 교수 및 연구용 PC, 비상주 인력 PC도 예외 없이 점검 대상에 포함 필수

[Action Item] 매월 셋째 주 수요일 오전, 전 부서원 대상 PC보안점검 실행 예약 메일 설정 및 미이행자 독려

[조치 사항] 매월 '사이버 보안 진단의 날' 이행 규정

시행 개요:
매월 세 번째 주 수요일 실시
(전 기관 이행률
80% 이상 달성 필수)

● [필수 사항] 내PC지키미 실행

점검 스케줄에 맞춰 전 직원 대상 PC 취약점 자동 점검 시행.

● [필수 사항] 취약점 즉시 조치

진단 결과 취약 항목 발견 시 [자동 조치] 및 [수동 조치 안내]를 통해 즉각 보안 상태 '안전'으로 전환.

● [금지 사항]
점검 우회 절대 금지

미조치 단말기에 대해서는 [최상위 고정] 창 알림 및 [네트워크 차단] 등 등 강제 통제 정책이 적용됨.

● [협조 사항] 결과 보고

분임보안담당자는 부서원 진단 완료 여부 확인 후 미비점 보완 지시 및 최종 조치 결과 제출 바람.

[현황 및 문제점] 실무 현장 보안 취약점 진단

[기술적 취약점] 단말기 및 네트워크 보안 관리 미흡

- 사설 IP 임의 할당 및 단말기 최신 보안 패치(OS, 백신) 미적용 사례 발생.
- 인가되지 않은 S/W(P2P, 상용 메신저 등) 사용으로 인한 악성코드 감염 노출.

[관리적 취약점] 매체 및 인프라 통제 사각지대

- 미등록 휴대용 저장매체(USB)의 무분별한 반출·입 및 등급별(비밀/일반) 혼용 사례 적발.
- 정보화 사업 추진 시 사전 보안성 검토 누락 및 정보시스템 관리대장 현행화 미흡.

[인적 취약점] 사용자 보안 의식 결여

- 의심스러운 출처의 이메일 열람 및 악성 첨부파일 무단 실행으로 인한 내부 정보 유출 위험.
- 퇴직 및 인사이동 시 정보시스템(PC 등) 접근 권한 미회수 및 인계인수 누락.

사이버 침해사고 발생 시 비상 대응 절차

[1단계] 사고 인지 및 초동 조치 (즉시)

- [필수 사항]: 피해 확산 방지를 위해 랜섬웨어 등 감염 의심 PC의 네트워크 선(LAN)을 물리적으로 즉시 분리할 것.
- [금지 사항]: 원인 규명 및 증거 보전을 위해 임의로 전원을 끄거나 자료를 삭제, 포맷하는 행위 절대 금지.

[2단계] 즉각 신고 (24시간 이내)

분임보안담당관 및 사이버안전센터로 피해 상황(발생 일시, 증상, 피해 범위) 유선 및 이메일 긴급 신고.

[3단계] 사고 조사 협조

정보보안담당관의 지시에 따라 로그(Log) 기록 제출 및 악성코드 제거 (백신 치료) 작업 수행.

[4단계] 사후 복구 및 재발 방지

사고 조사 결과에 따른 취약점 패치 적용 및 해당 부서원 대상 특별 보안 교육 이행.

위기 대응 - 침해사고 발생 시 골든 타임 초동 조치

제1원칙: 임의 조작(전원 끄기, 재부팅, 포맷) 절대 금지

1. **물리적 차단:** 피해 PC/서버의 랜선(네트워크 케이블) 즉시 분리
(논리적 방화벽 차단에 의존하지 않음)

2. **현장 보존:** 피해 시스템 전원 유지, 화면 캡처, 시스템 로그 등
증거 훼손 원천 차단

3. **즉시 신고:** 내부 정보보호팀(CERT) 및 교육부
사이버안전센터(ECSC)에 24시간 이내 신고 통보

[주의/필수] 악성코드/랜섬웨어 감염 시 당황하여 PC 전원을 끄거나 강제 재부팅하면 메모리에 남은 핵심 해킹 증거가 즉각 소멸되어 역추적 및 원인 분석 불가

부서원들에게 '랜섬웨어 의심 시 전원을 끄지 말고 랜선만 물리적으로 뽑을 것'을 전파

위기 대응 비교 - 악성코드 vs 네트워크 공격(DDoS)

	[악성코드 / 랜섬웨어 감염]	[DDoS 등 트래픽 공격 / 해킹]
주요 증상	내부 파일 암호화 확장자 변경, PC 시스템 속도 급격한 저하	웹페이지 접속 불가, 네트워크 트래픽 폭주로 인한 서비스 마비
핵심 조치 목표	내부 확산 차단 및 해킹 증거 보존	상위 기관 협조를 통한 악성 트래픽 차단 및 우회
담당관 즉시 행동	**랜선 물리적 분리 → 전원 유지(현장 보존) → 즉시 신고**	**시스템 연계 상태 파악 → 보안장비 로그 보존 → 즉시 신고(차단 요청)**

[주의/필수] 개인정보가 포함된 자료의 유출이 확인된 경우, 인터넷 차단 등 확산 방지 조치 후 관련 법령(개인정보보호법)에 따른 추가 신고 절차 필수 진행

단말기(PC) 및 업무망 보안 통제 체계

🔵 [필수 사항] 이행 지침	🔴 [금지 사항] 위규 지침
✔ - 장비(CMOS), 자료(문서 암호화), 사용자(로그온)별 비밀번호 상이하게 설정 및 분기별 정기 변경.	✖ - 메신저, P2P, 웹하드 등 인가되지 않은 외부 프로그램 설치 및 공유 폴더 사용 원천 금지.
✔ - 10분 이상 이석 시 비밀번호가 적용된 화면보호기 즉시 가동.	✖ - 출처가 불분명하거나 서명되지 않은 Active-X 무단 다운로드 및 실행 절대 금지.
✔ - 운영체제(OS), 백신 프로그램 및 주요 응용프로그램(Acrobat, 한글 등) 최신 보안 패치 유지.	✖ - 외부 업체의 원격 접속을 통한 정보시스템 유지보수 작업 엄격히 금지 (예외 시 별도 승인 및 보안 통제 적용).
✔ - 부득이한 개인 소유 PC 반입 시 사전 승인 득 및 최신 백신 점검 필수.	

일상 보안 : 인적/물리적 보안 통제

[시스템 접근 통제]

- 全 구성원 시스템 2차 인증(MFA) 적용
- 주기적 비밀번호(9자리 이상) 변경 준수

[단말기 통제]

- 업무상 불필요한 공유 폴더 사용 전면 금지
- 자리 이석 시 화면보호기 (10분) 작동 설정
- 개인 소유 PC 업무망 임의 연결 금지

[물리적 통제]

- 정보통신 핵심 시설(MDF룸 등) 상시 시건 장치 확인
- 외부인 출입 시 출입기록부 작성 의무화

[주의/필수] 인사이동(전출) 및 퇴사자 발생 시 즉각적인 정보시스템 접근 권한 회수 누락은 최다 감사 지적 사항임

최근 1개월 내 전출/퇴직자 계정 삭제 및 권한 회수 여부 전수 확인

휴대용 저장매체(USB) 엄격 통제 절차

기본 원칙: 부서 내 모든 USB는 정보보안담당관 승인 하에 등록 후 사용 (미등록 매체 사용 절대 금지).

🔵 [필수 사항] 등급별 분리 관리

🔴 비밀용	🔵 일반용	⚠ 공인인증서용
- 비밀관리기록부 등재 - 전면에 비밀등급/관리번호 부착 표기 - 이중캐비닛(금고) 보관 필수	- 일반자료만 보관 - '부서명-일반-연번' 체계로 라벨링 - 시건장치 내 보관	- 사적 소지는 허용됨 - 기관의 업무 자료 보관 절대 금지

[금지 사항] 혼용 보관 및 무단 반출 금지: 하나의 USB에 다른 등급의 비밀 혼합 보관을 금지하며, 외부 반출입 시 반드시 관리대장에 기록할 것.

[필수 사항] 안전한 폐기: 불용 처리 또는 용도 전환 시 복구 불가능한 완전 삭제(포맷 3회 이상) 절차 이행 후 승인 폐기 바람.

피싱 이메일 방어 및 모의 훈련 지침

최신 피싱 수법: 통일부 사칭(플랫폼 업그레이드 유도), 배송업체 사칭, 견적서 위장 첨부파일(HTML, ZIP, PDF) 유포.

실무 행동 지침

- [금지 사항] 의심 메일 열람 금지: 발신자가 불분명하거나 제목이 의심스러운 전자우편(상용 메일 등)은 절대 열람하지 말고 즉시 삭제할 것.
- [주의 조치] 첨부파일 검사: 문서 파일 다운로드 전 반드시 최신 백신으로 악성코드 은닉 여부 정밀 검사 수행.
- [필수 사항] 즉각 신고: 해킹메일로 의심되거나 로그인 정보 유출이 우려되는 경우 즉시 정보보안담당관실 및 사이버안전센터로 신고 바람.
- [필수 사항] 훈련 적극 참여: 악성메일 대응 해킹 모의훈련 시행 시 부서원의 적극적 참여 독려 및 초동 조치 절차 숙지 요망.

AI 서비스 활용 보안 가이드라인

배경: ChatGPT 등 외부 생성형 AI 도입 확산 및 Shadow AI 리스크에 따른 사내 민감 정보 유출 방지.

[필수 사항] AI Guardrail 적용

- 사내 승인 및 보안이 검증된 AI 도구(예: Brity Copilot 등)만 제한적으로 사용할 것.
- 정보 입력 및 응답 산출물을 실시간 모니터링하여 개인정보 및 기관 비밀 데이터 유출 원천 차단.

[주의 조치] AI Agent 권한 통제

- AI에게 결제, 시스템 설정 변경 등 민감한 명령 수행 위임 시 반드시 인간의 승인(Human-in-the-loop) 과정을 거칠 것.

[금지 사항] 무단 학습 데이터 입력 금지

- 비인가 퍼블릭 AI에 기관의 공문서, 보안 지침, 소스코드, 개인정보 등을 질문 형태로 입력하는 행위 엄단.

보안 감사 및 위규자 제재 규정

정기 및 수시 보안 점검 수검

- **내용:** 정보통신 인프라 자산, PC 단말기 보안, 개인정보파일 안전 조치 등 정보보안 전반에 대체 실사 및 현장 감사 시행.
- **협조:** 분임보안담당자는 점검반의 현장 실사 방문 및 로그 기록 요구 시 적극 협조 바람.

정보보안 위규 처리 기준 (징계 심의)

[경고/주의 조치] 미등록 USB 단순 소지, 미등록 USB 단순 소지, 화면보호기 미설정, 비밀번호 주기 미변경 등 관리 소홀.

[중징계 대상] 비밀 자료 외부 무단 유출, 인가되지 않은 비인가 통신망(무선AP) 임의 설치, 고의적 보안시스템 무력화 행위.

후속 조치: 적발 시 정보보안사고 조사를 통해 위규 경중에 따라 자체 처분 실시 및 상급 기관(국정원 등) 통보 조치됨.

1. 착수 전 | 2. 수행 중 | 3. 완료 시

용역사업 보안 통제 – [1단계] 사업 착수 전

보안성 검토:
사업 계획 단계(공고 전) 보안성 검토 요청 및 결과를 과업지시서에 반영

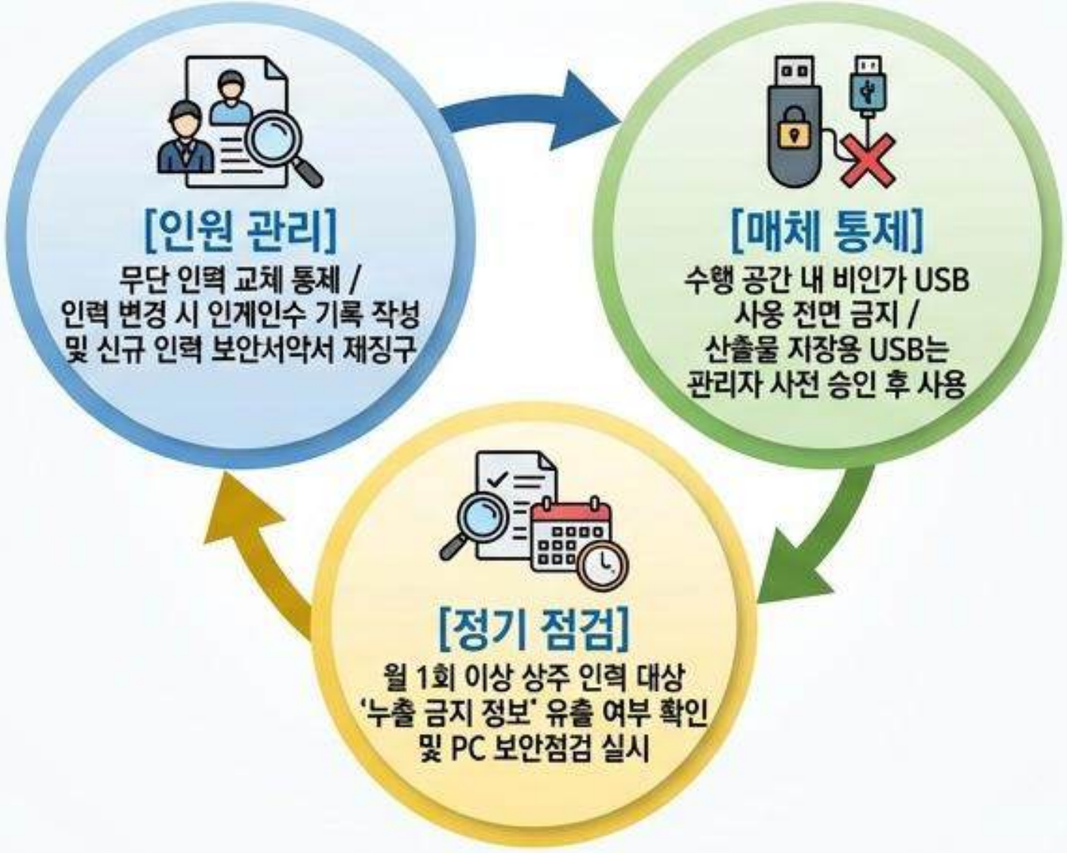
보안서약서 징구:
용역사업 참여 인원 전체에 대한 보안서약서 수령

보안교육 실시:
투입 전 정보 유출 금지, 비밀유지 의무 및 위반 시 처벌 내용 자체 교육 진행

[주의/필수] 보안서약서는 반드시 친필 서명으로 징구할 것. (워드 타이핑, 단순 도장 날인 대체 절대 불가) / 용역업체 대표 명의의 서약서 별도 징구 필수

부서 내 진행 예정인 사업의 보안서약서 양식이 최신 규정에 맞는지 확인하고, 투입 인력 명단과 서약서를 1:1 대조하여 서명 누락자 파악

용역사업 보안 통제 - [2단계] 사업 수행 중



[주의/필수] 사업 기간 중 무단 인력 교체 여부 점검 미흡 시 제재 조치 가능 / 인가된 USB 외 무단 매체 연결 시 정보보호시스템 로그 기록에 즉각 적발됨

현재 상주 중인 용역 인력이 반입한 노트북의 USB 포트 봉인 상태 및 비인가 무선공유기(AP) 사용 여부 현장 점검

1. 착수 전 | 2. 수행 중 | 3. 완료 시

용역사업 보안 통제 - [3단계] 사업 완료 시

자료 완전 삭제: 발주기관 소유의 결과물 및 제공 자료를 업체 노트북에서 완전 삭제 처리

계정 회수: 부여된 정보시스템(DB, 서버 등) 접근 권한 및 외부 VPN 계정 전면 회수

서류 징구: 대표 명의 보안확약서 및 용역 산출물 검사검수요청서 수령

[주의/필수] 완전 삭제 증빙용으로 하드디스크 포맷 결과 사진 등 시각적 증빙 반드시 결과보고서에 포함 / 취약점 점검 및 조치 결과서 수령 필수 / 자료 미삭제 적발 시 입찰 참가자격 제한 등 강력 제재

최근 종료된 사업 중 산출물 완전 포맷 증빙 사진이나 대표 명의 확약서가 누락된 건이 없는지 문서고 점검

보안 감사 생존(Survival) 체크리스트 : 빈출 지적 사항 Top 5

빈출 지적 사항

- ☑ [인사] 인력 퇴직 및 전출 시 정보시스템(포털, 그룹웨어) 및 물리적 출입 권한 회수 지연 (즉시 회수 요망)
- ☑ [용역] 용역사업 참여 인원 보안서약서 서명 누락 또는 대리 서명 (친필 서명 필수)
- ☑ [용역] 사업 완료 시 산출물 및 데이터 완전 삭제 증빙(포맷 결과 화면 캡처 등) 누락
- ☑ [운영] 부서 내 공용 폴더 사용 및 비인가 무선공유기(AP) 임의 설치 (사설 IP/무선랜 보안 통제 위반)
- ☑ [일상] '사이버 보안 진단의 날' 대상 PC 점검 미수행 (연구용 PC 및 비상주 인력 PC 점검 누락)

위 5가지 항목 을 인쇄하여 부서 내 게시판에 부착하고 월 1회 자가 진단 실시

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)

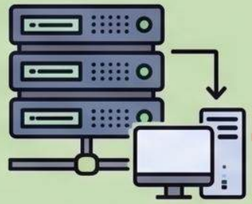
사업 수행 중 업체 인력 보안점검
(누출금지 정보 유출여부 등)

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

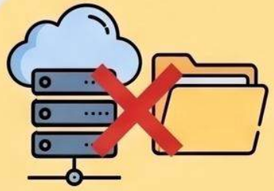
용역사업 수행시 점검사항 – 자료에 대한 보안관리

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

전산망 분리 및
제한적 접근

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

02

차등적 접근
권한 부여

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

03

인터넷 접속
차단 및 통제

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

주기적 PC 보안 점검

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

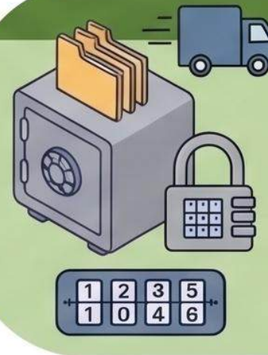
4단계 프로세스로 확인하는 보안 점검 내용

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 추가 징구로 최종 보안성 강화

보안서약서

[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

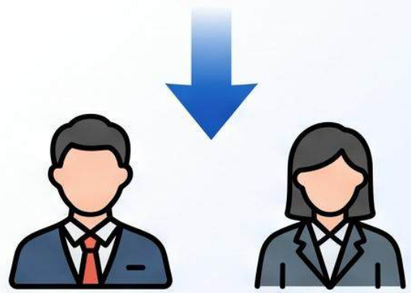
4. 검사검수요청서

5. 그 외 제안요청서(과업지시서)에서 검수기관에서 요청한 사항 등

단계별 문서 정리

계약시
(At Contract Signing)

- 보안서약서
- 비밀유지서약서
- 개인정보처리위탁계약서(대상 시)



대표 참여인력

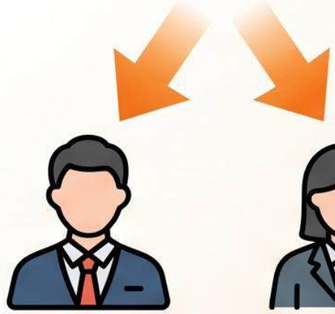
수행시
(During Execution)

계약시 기준

참여인력

종료시
(At Completion)

- 보안확약서(업체대표)
- 보안서약서(참여인력)



대표 참여인력

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]

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. #

신한카드 가맹점주 19만명 개인정보 유출

등록기자: 송경배 [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		

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

'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.

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.

핵심 시사점

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

대규모 고객 정보 유출 발생

분임보안담당자 실무 수칙 체크리스트

Check 1

최근 1개월 내 전출/퇴직자
시스템 계정 삭제 및
출입 권한 회수 여부
전수 확인

Check 2

부서 내 진행 중인
용역업체 인력의
보안서약서 '친필 서명'
누락 여부 대조 확인

Check 3

'랜섬웨어 의심 시
PC 끄지 말고 랜선 뽑기'
행동 수칙
부서원 전체 이메일 전파

보안은 두꺼운 매뉴얼이 아닌, '내일 아침의 행동'에서 시작됩니다.
담당관님의 신속한 조치가 우리 기관을 보호합니다.

분임보안담당자 실무 수칙 체크리스트

- ✓ [매월 3주 차 수요일] 사이버 보안 진단의 날 '내PC지키미' 부서원 100% 실행 완수 여부 점검.
- ✓ [상시 점검] 부서 내 전 PC 백신 최신화 유지 및 단말기 비밀번호 정기 변경 여부 확인.
- ✓ [매체 통제] 부서 내 지급된 모든 USB 매체 등록 대장 현행화 및 시건장치 보관 점검.
- ✓ [인사이동 시] 퇴직/전보자의 정보시스템 접근 권한 즉시 삭제 및 정보 자산 인계인수 철저.
- ✓ [사고 발생 시] 랜섬웨어/악성코드 의심 즉시 랜선을 뽑고 정보보안담당관실로 신고.

정보보안의 시작은 실무 현장의 철저한 규정 준수로부터 비롯됩니다.
담당자 여러분의 적극적인 협조를 바랍니다.