’25년
정보보호 및
개인정보 관리체계(ISMS-P)
운영 가이드

개정판

SK 쉴더스 | ICT취약점진단팀

목 차

주요 개정사항

1. 개인정보보호법 및 관련 법령 개정사항 반영

- 현행 개인정보보호법[시행 2025. 10. 2] 기준 등 정보보호 및 개인정보보호 관리체계(ISMS-P) 관련 법령 개정사항 반영

법령	주요 개정사항(2024~2025)
개인정보보호법	- 개인정보 처리 목적·항목·보유기간 명시 및 최소 수집 원칙 준수 - 개인정보 전송 요구권 신설 및 세부 처리절차 고시 - 가명정보 결합, 이용·제공 절차 엄격화 - 국내대리인 지정 의무 - 개인정보관리 전문기관 지정기준 강화 - 인터넷망의 차단조치 개정 등
정보통신망법	- 불법 스팸 대응 제도 개선(수신거부 절차 간소화 등) - 연계정보 안전조치 - 본인확인기관의 물리적·기술적·관리적 조치
전자금융거래법	- 선불전자지급수단 이용자 보호 강화 - 클라우드 컴퓨팅 서비스 이용 기준 개선 - 전자금융감독규정 규제 체계 변경
신용정보보호법	- 신용정보 범위 확대(불공정거래·피싱 방지 정보 포함) - 예비허가제 도입 근거 신설 - 데이터전문기관 업무·결합 보고 의무 강화 - 마이데이터 서비스 개인정보 활용 동의 절차
기타 법령	- 민감정보(의료·건강) 별도 동의 및 보관·파기 절차 엄격화

※ 2024~2025년 정보보호 및 개인정보관련 법령 개정사항

2. 항목별 가이드 개정

- 방송통신위원회, 개인정보보호위원회, 한국인터넷진흥원 등 유관기관의 최신 가이드 반영
- 정보보호정책서 예시, 보안조치 방안 등 항목별 가이드라인 작성

※ 참고자료 :

1. 개인정보 처리 통합 안내서(개인정보보호위원회. 2025.7)
2. 연계정보 처리 및 안전조치 등에 관한 안내서(방송통신위원회, 한국인터넷진흥원. 2025.6)
3. 개인정보 전송요구권 제도 안내서(개인정보보호위원회. 2025.04)
4. 개인정보보호책임자(CPO) 핸드북(개인정보보호위원회, 한국개인정보보호책임자 협의회. 2024.11)
5. 개인정보의 안전성 확보조치 기준 안내서(개인정보보호위원회,한국인터넷진흥원. 2025.11)
6. 기타 '정보보호 및 개인정보보호 관리체계' 관련 기준 및 최신 가이드 반영

I. 정보보호 및 개인정보보호 관리체계(ISMS-P) 진단 항목

영역	분야	항목
1. 관리체계 수립 및 운영 (16개)	1.1 관리체계 기반 마련	1.1.1 경영진의 참여
		1.1.2 최고책임자의 지정
		1.1.3 조직 구성
		1.1.4 범위 설정
		1.1.5 정책 수립
		1.1.6 자원 할당
	1.2 위험 관리	1.2.1 정보자산 식별
		1.2.2 현황 및 흐름분석
		1.2.3 위험 평가
		1.2.4 보호대책 선정
	1.3 관리체계 운영	1.3.1 보호대책 구현
		1.3.2 보호대책 공유
		1.3.3 운영현황 관리
	1.4 관리체계 점검 및 개선	1.4.1 법적 요구사항 준수 검토
		1.4.2 관리체계 점검
		1.4.3 관리체계 개선
2. 보호대책 요구사항 (64개)	2.1 정책, 조직, 자산 관리	2.1.1 정책의 유지관리
		2.1.2 조직의 유지관리
		2.1.3 정보자산 관리
	2.2 인적 보안	2.2.1 주요 직무자 지정 및 관리
		2.2.2 직무 분리
		2.2.3 보안 서약
		2.2.4 인식제고 및 교육훈련
		2.2.5 퇴직 및 직무변경 관리
		2.2.6 보안 위반 시 조치
	2.3 외부자 보안	2.3.1 외부자 현황 관리
		2.3.2 외부자 계약 시 보안
		2.3.3 외부자 보안 이행 관리
		2.3.4 외부자 계약 변경 및 만료 시 보안
	2.4 물리 보안	2.4.1 보호구역 지정
		2.4.2 출입통제
		2.4.3 정보시스템 보호
		2.4.4 보호설비 운영
		2.4.5 보호구역 내 작업

2. 보호대책 요구사항 (64개)	**2.4 물리 보안**	2.4.6 반출입 기기 통제
		2.4.7 업무환경 보안
	2.5 인증 및 권한관리	2.5.1 사용자 계정 관리
		2.5.2 사용자 식별
		2.5.3 사용자 인증
		2.5.4 비밀번호 관리
		2.5.5 특수 계정 및 권한관리
		2.5.6 접근권한 검토
	2.6 접근통제	2.6.1 네트워크 접근
		2.6.2 정보시스템 접근
		2.6.3 응용프로그램 접근
		2.6.4 데이터베이스 접근
		2.6.5 무선 네트워크 접근
		2.6.6 원격접근 통제
		2.6.7 인터넷 접속 통제
	2.7 암호화 적용	2.7.1 암호정책 적용
		2.7.2 암호키 관리
	2.8 정보시스템 도입 및 개발 보안	2.8.1 보안 요구사항 정의
		2.8.2 보안 요구사항 검토 및 시험
		2.8.3 시험과 운영 환경 분리
		2.8.4 시험 데이터 보안
		2.8.5 소스 프로그램 관리
		2.8.6 운영환경 이관
	2.9 시스템 및 서비스 운영관리	2.9.1 변경관리
		2.9.2 성능 및 장애관리
		2.9.3 백업 및 복구관리
		2.9.4 로그 및 접속기록 관리
		2.9.5 로그 및 접속기록 점검
		2.9.6 시간 동기화
		2.9.7 정보자산의 재사용 및 폐기
	2.10 시스템 및 서비스 보안관리	2.10.1 보안시스템 운영
		2.10.2 클라우드 보안
		2.10.3 공개서버 보안
		2.10.4 전자거래 및 핀테크 보안
		2.10.5 정보전송 보안
		2.10.6 업무용 단말기기 보안
		2.10.7 보조저장매체 관리

2. 보호대책 요구사항 (64개)	**2.10 시스템 및 서비스 보안관리**	2.10.8 패치관리
		2.10.9 악성코드 통제
	2.11 사고 예방 및 대응	2.11.1 사고 예방 및 대응체계 구축
		2.11.2 취약점 점검 및 조치
		2.11.3 이상행위 분석 및 모니터링
		2.11.4 사고 대응 훈련 및 개선
		2.11.5 사고 대응 및 복구
	2.12 재해 복구	2.12.1 재해·재난 대비 안전조치
		2.12.2 재해 복구 시험 및 개선
3. 개인정보 처리 단계별 요구사항 (21개)	**3.1 개인정보 수집 시 보호조치**	3.1.1 개인정보 수집·이용
		3.1.2 개인정보 수집 제한
		3.1.3 주민등록번호 처리 제한
		3.1.4 민감정보 및 고유식별정보의 처리 제한
		3.1.5 개인정보 간접수집
		3.1.6 영상정보처리기기 설치·운영
		3.1.7 마케팅 목적의 개인정보 수집·이용
	3.2 개인정보 보유 및 이용 시 보호조치	3.2.1 개인정보 현황관리
		3.2.2 개인정보 품질보장
		3.2.3 이용자 단말기 접근 보호
		3.2.4 개인정보 목적 외 이용 및 제공
		3.2.5 가명정보 처리
	3.3 개인정보 제공 시 보호조치	3.3.1 개인정보 제3자 제공
		3.3.2 개인정보 처리 업무 위탁
		3.3.3 영업의 양도 등에 따른 개인정보 이전
		3.3.4 개인정보 국외이전
	3.4 개인정보 파기 시 보호조치	3.4.1 개인정보 파기
		3.4.2 처리목적 달성 후 보유 시 조치
	3.5 정보주체 권리보호	3.5.1 개인정보 처리방침 공개
		3.5.2 정보주체 권리보장
		3.5.3 정보주체에 대한 통지

II. 개인정보 처리 단계별 요구사항

1. 관리체계 수립 및 운영

1.1 관리체계 기반 마련

1.1.1 경영진의 참여

세부분야	1.1.1 경영진의 참여
인증 기준	최고경영자는 정보보호 및 개인정보보호 관리체계의 수립과 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여 운영하여야 한다.
주요 확인사항	• 정보보호 및 개인정보보호 관리체계의 수립 및 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 등의 책임과 역할을 문서화하고 있는가? • 경영진이 정보보호 및 개인정보보호 활동에 관한 의사결정에 적극적으로 참여할 수 있는 보고, 검토 및 승인 절차를 수립·이행하고 있는가?
기준 요약도	
운영 방안	**◇ 정보보호 및 개인정보보호 관리체계의 수립 및 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 등의 책임과 역할을 문서화하고 있는가?** **(예시) 정보보호 및 개인정보보호 정책 또는 시행문서에 관련 내용 명시** 「**정보보호정책서**」 제 ○○조 (정보보호 조직 구성 및 운영)

① 최고경영자(CEO)는 전사 정보보호의 체계적이고 원활한 이행을 위한 조직을 구성·운영하고 정보보호 최고책임자(CISO)를 인사발령 등의 공식적인 지정절차를 거쳐 지정하여야 한다.

② 최고경영자(CEO)는 전사 정보보호 업무를 원활히 수행하기 위해 조직의 규모 및 자산의 중요도에 따라 필요인력, 예산 등을 분석하여 정보보호 실무조직을 구성하여야 한다.

③ 정보보호 실무조직은 정보보호 관리자, 정보보호 담당자, 개인정보보호 책임자, 개인정보보호 관리자 및 개인정보보호 담당자로 구성할 수 있다.

「**정보보호정책서**」 제 ○○조 (정보보호위원회 구성 및 운영)

① 정보보호위원회는 전사 정보보호 관련 정책 방향을 심의 및 의결한다

② 정보보호위원회는 정보보호최고책임자(CISO)가 위원장을 역임하여 영역별 정보보호 담당자로 정보보호위원회를 구성하고 운영한다

◇ 경영진이 정보보호 및 개인정보보호 활동에 관한 의사결정에 적극적으로 참여할 수 있는 보고, 검토 및 승인 절차를 수립·이행하고 있는가?

(예시) 정보보호 활동, 의사결정 절차, 대상, 주기 등 결정

「**정보보호 조직 관리지침**」 제 ○○조 (정보보호 최고책임자)

① 정보보호 최고책임자(CISO)는 정보보호 업무를 총괄하며, 각 호에 대한 사항을 검토, 운영한다.

1. 정보보호 관리체계 계획 수립에 관한 업무
2. 정보보호 정책 지침 제·개정 업무
3. 취약점 분석·평가 및 침해사고 예방 지원 업무
4. 침해사고 대응 및 복구 업무
5. 정보보호의 날 운영 업무
6. 정보보호에 필요한 예산 및 설비 등 자산 확보에 관한 업무
7. 그 밖에 정보보호를 위해 필요한 업무

「**정보보호 조직 관리지침**」 제 ○○조 (정보보호위원회)

① 정보보호위원회는 정보보호 최고책임자(CISO)를 위원장으로 하며, 개인정보보호책임자를 비롯한 정보보호와 관련된 각 부서의 장을 위원으로 구성한다.

② 간사의 역할은 정보보호관리자가 수행한다.

③ 정보보호위원회는 다음의 역할을 수행한다.

1. 정보보호정책 및 지침의 제·개정에 대한 심의·승인

	2. 정보보호 예산 심의·승인 3. 정보보호 활동 계획의 심의·승인 4. 정보보호 위반자 심의·처리에 관한 사항 5. 기타 정보보호최고책임자가 필요하다고 인정하는 사항

1.1.2 최고 책임자의 지정

세부분야	1.1.2 최고 책임자의 지정
인증 기준	최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보보호 업무를 총괄하는 개인정보보호책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.
주요 확인사항	• 최고경영자는 정보보호 및 개인정보보호 처리에 관한 업무를 총괄하여 책임질 최고책임자를 공식적으로 지정하고 있는가? • 정보보호 최고책임자 및 개인정보보호책임자는 예산, 인력 등 자원을 할당할 수 있는 임원급으로 지정되어 있으며, 관련 법령에 따른 자격요건을 충족하고 있는가?
기준 요약도	
운영 방안	**◇ 최고경영자는 정보보호 및 개인정보보호 처리에 관한 업무를 총괄하여 책임질 최고책임자를 공식적으로 지정하고 있는가?** **정보보호 최고책임자(CISO)와 개인정보보호책임자(CPO) 직무** ① 정보보호 최고책임자(CISO) 역할 1. 정보보호 관리체계의 수립 및 관리·운영 2. 정보보호 취약점 분석·평가 및 개선 3. 침해사고의 예방 및 대응 4. 사전 정보보호 대책 마련 및 보안조치 설계·구현 등 5. 정보보호 사전 보안성 검토 6. 중요정보의 암호화 및 보안서버 적합성 검토 7. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행 ② 개인정보보호책임자(CPO) 1. 개인정보 보호 계획의 수립 및 시행 2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선

3. 개인정보 처리 관련 불만 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독
7. 개인정보처리방침의 수립·변경 및 시행
8. 개인정보 보호 관련 자료 관리
9. 목적이 달성되거나 보유기간이 지난 개인정보 파기

정보보호 최고책임자(CISO) 임명

① 정보보호 최고책임자 및 개인정보 보호책임자를 인사발령 등의 절차를 통하여 공식적으로 지정.


SK 실더스
안녕을 지키는 기술
참고자료

ON	소 속	직능	직급	성명	발령내용	발령구분	발령일자	비고
1	정보보호그룹	기업정보보안	임원	김 ○ ○	명) 정보보호최고책임자 (CISO)	전보	2023-01-01	

해당 예시는 참고자료로 실제 문서가 아닙니다. SK 실더스

※ 인사발령 내용 (이해를 돕기 위한 예시)

◇ 정보보호 최고책임자 및 개인정보보호책임자는 예산, 인력 등 자원을 할당할 수 있는 임원급으로 지정되어 있으며, 관련 법령에 따른 자격요건을 충족하고 있는가?

정보보호 최고책임자 지정·신고 의무대상

「**정보통신망법**」 제45조의 3 (정보보호 최고책임자의 지정 등)

① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 한다. **다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 신고하지 아니할 수 있다.**

「**정보통신망법 시행령**」 제36조의 7 (정보보호 최고책임자의 지정 및 겸직금지 등)

① 법 제45조의3제1항 본문에서 "대통령령으로 정하는 기준에 해당하는 임직원"이란

다음 각 호의 구분에 따른 사람을 말한다

1. 다음 각 목의 어느 하나에 해당하는 정보통신서비스 제공자: 사업주 또는 대표자

가. 자본금이 1억 이하인 자

나. 중소기업법 제2조제2항에 따른 소기업

다. 중소기업법 제2조제2항에 따른 중기업, 다음의 어느 하나에 해당하지 않는 자

1)「전기통신사업법」에 따른 전기통신사업자

2) 법 제47조제2항에 따라 정보보호 관리체계 인증을 받아야 하는 자

3)「개인정보 보호법」제30조제2항에 따라 개인정보 처리방침을 공개해야 하는 개인정보처리자

4)「전자상거래 등에서의 소비자보호에 관한 법률」제12조에 따라 신고를 해야 하는 통신판매업자

※ 출처: 정보보호 최고책임자 지정 신고제도 안내서 (과학기술정보통신부•KISA)

정보보호 최고책임자 신고 의무대상자 분류 별 지정 기준

① 대규모 기업(겸직 제한 의무대상): 직전 연도 말 자산총액 5조 이상이거나,

② 인증 의무대상 중 자산총액 5천억 이상

③ 중기업 이상: 대규모 기업 외 정보통신 서비스 제공자

④ 소기업 등 (신고 의무 제외)

※ 출처: 정보보호 최고책임자 지정 신고제도 안내서 (과학기술정보통신부•KISA)

정보보호 최고책임자 자격요건

① 일반 자격요건: (중기업 이상 신고 의무대상자)

1. 정보보호 또는 정보기술분야 석사 이상
2. 정보보호 또는 정보기술분야 학사 3년 이상 경력
3. 정보보호 또는 정보기술분야 전문학사 5년 이상 경력
4. 정보보호 또는 정보기술분야 10년 이상 경력

② 특별 자격요건: (대규모 기업 겸직제한 의무대상자)

1. 정보보호 업무 경력 4년 이상
2. 정보보호 또는 정보기술분야 5년 이상 경력 중 2년은 정보보호 분야 업무 경력

개인정보보호책임자 지정

「**개인정보보호법**」 제31조 (개인정보 보호책임자의 지정 등)

① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다. 다만, 종업원 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 개인정보처리자의 경우에는 지정하지 아니할 수 있다.

② 제1항 단서에 따라 개인정보 보호책임자를 지정하지 아니하는 경우에는 개인정보처리자의 사업주 또는 대표자가 개인정보 보호책임자가 된다

개인정보보호책임자 자격요건 충족 의무대상

「**개인정보보호법 시행령**」 제32조(개인정보 보호책임자의 업무 및 지정요건 등)

④ 다음 각 호의 어느 하나에 해당하는 개인정보처리자(공공기관의 경우에는 제2조제2호부터 제5호까지에 해당하는 경우로 한정한다)는 제3항 각 호의 구분에 따른 사람 중 별표 1에서 정하는 요건을 갖춘 사람을 개인정보 보호책임자로 지정해야 한다.

1. 연간 매출액 등이 1,500억원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자(제2조제5호에 따른 각급 학교 및 「의료법」 제3조에 따른 의료기관은 제외한다)

가. 5만명 이상의 정보주체에 관하여 민감정보 또는 고유식별정보를 처리하는 자

나. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자

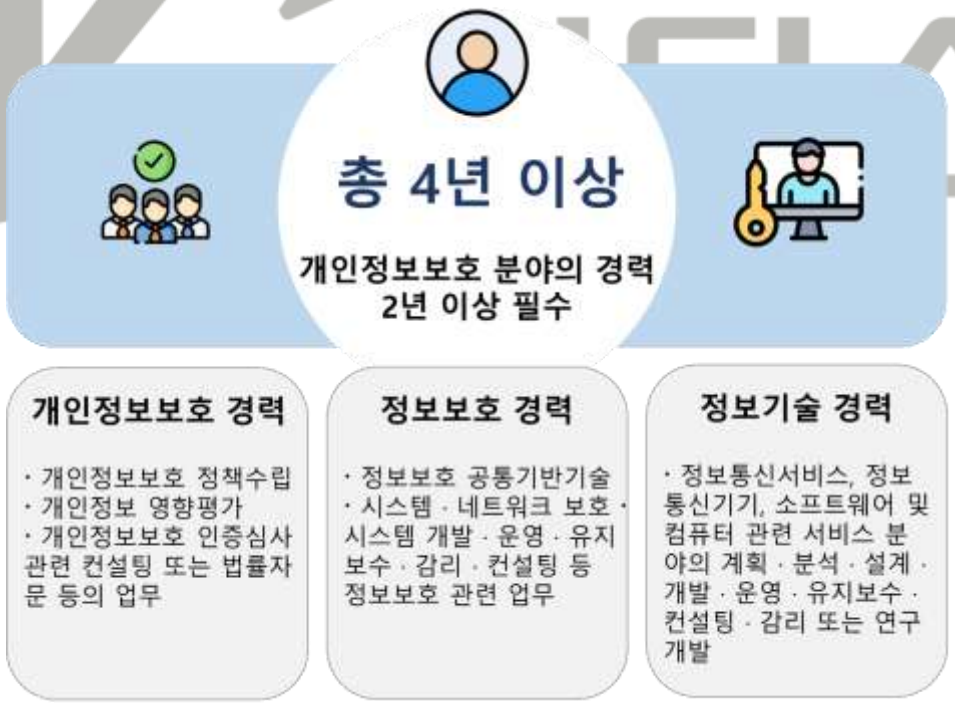
2. 직전 연도 12월 31일 기준으로 재학생 수(대학원 재학생 수를 포함한다)가 2만명 이상인 「고등교육법」 제2조에 따른 학교

3. 「의료법」 제3조의4에 따른 상급종합병원

4. 공공시스템운영기관

개인정보보호책임자 자격요건(대상 해당 시)

① 개인정보보호책임자로 지정되는 사람은 개인정보 보호 경력, 정보보호 경력, 정보기술 경력을 합하여 총 4년 이상 보유하고, 그 중 **개인정보 보호 경력을 최소 2년 이상 보유**해야 한다.



※ 개인정보보호책임자 자격요건 (이해를 돕기 위한 예시)

	※ 관련 분야의 학위를 취득한 경우, 다음과 같이 경력으로 인정받을 수 있음 ① 박사 학위: 2년 경력 인정 ② 석사 학위: 1년 경력 인정 ③ 학사 학위: 6개월 경력 인정 여러 학위를 가지고 있더라도, 이 중 **하나만 경력으로 선택하여 인정**받을 수 있음

1.1.3 조직 구성

세부분야	1.1.3 조직 구성
인증 기준	최고경영자는 정보보호와 개인정보보호의 효과적 구현을 위한 실무조직, 조직 전반의 정보보호와 개인정보보호 관련 주요 사항을 검토 및 의결할 수 있는 위원회, 전사적 보호활동을 위한 부서별 정보보호와 개인정보보호담당자로 구성된 협의체를 구성하여 운영하여야 한다.
주요 확인사항	• 정보보호 최고책임자 및 개인정보보호책임자의 업무를 지원하고 조직의 정보보호 및 개인정보보호 활동을 체계적으로 이행하기 위하여 전문성을 갖춘 실무조직을 구성하여 운영하고 있는가? • 조직 전반에 걸친 중요한 정보보호 및 개인정보보호 관련사항에 대하여 검토, 승인 및 의사결정을 할 수 있는 위원회를 구성하여 운영하고 있는가? • 전사적 정보보호 및 개인정보보호 활동을 위하여 정보보호 및 개인정보보호 관련 담당자 및 부서별 담당자로 구성된 실무 협의체를 구성하여 운영하고 있는가?
기준 요약도	
운영	

방안	◇ 정보보호 최고책임자 및 개인정보보호책임자의 업무를 지원하고 조직의 정보보호 및 개인정보보호 활동을 체계적으로 이행하기 위하여 전문성을 갖춘 실무조직을 구성하여 운영하고 있는가?

(예시) 정보보호 조직구성 문서화

「**정보보호 조직 관리지침**」 제 ○○조 (정보보호 전담조직)

① 정보보호 최고책임자는 정보보호 관련 업무를 기획하고 시행하기 위한 세부계획을 수립하고 각종 보안통제 사항을 관리하는 정보보호팀을 구성한다

1. 정보보호팀은 자산에 대한 위협 및 위험분석, 주기적인 모니터링을 통해 평상시의 정보보호 관리를 수행한다.

2. 정보보호팀은 조직 임직원의 정보보호에 대한 인식 및 기술 수준을 제고하기 위해 교육계획을 수립하고 시행한다

... 이하 생략

② 개인정보의 안전한 관리를 수행하기 위해 개인정보보호팀을 구성한다.

1. 최고경영자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보보호책임자를 지정하여야 한다.

2. 개인정보보호책임자는 개인정보보호법 제31조의 의무를 수행하여야 한다.

③ 정보통신망의 침해사고 등 사이버 침해로부터의 예방, 대응, 분석 및 복구 등의 활동을 수행하기 위하여 침해사고대응팀을 구성한다.

1. 비상시 조직으로서 침해사고를 비롯한 정보보호 사고가 발생할 경우, 신속하고 효과적인 사고처리 및 복구를 위해 주요 정보보호관리자를 중심으로 침해사고 대응팀을 구성하여 운영한다.

... 이하 생략

※ 출처: 정보보호 및 개인정보보호 관리체계 인증신청 양식 (KISA)

◇ 조직 전반에 걸친 중요한 정보보호 및 개인정보보호 관련사항에 대하여 검토, 승인 및 의사결정을 할 수 있는 위원회를 구성하여 운영하고 있는가?

(예시) 정보보호위원회 구성 문서화

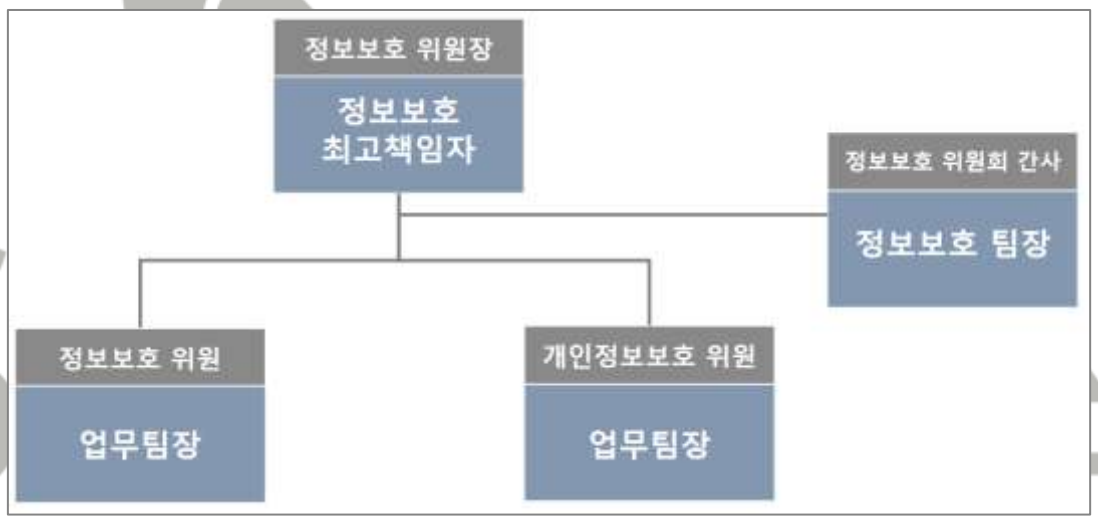
「**정보보호 조직 관리지침**」 제 ○○조 (정보보호위원회)

① 정보보호위원회는 정보보호최고책임자를 위원장으로 하며, 개인정보보호책임자를 비롯한 정보보호와 관련된 각 부서의 장을 위원으로 구성한다.

② 간사의 역할은 정보보호관리자가 수행한다.

③ 정보보호위원회는 다음의 역할을 수행한다.

1. 정보보호정책 및 지침의 제·개정에 대한 심의·승인
2. 정보보호 예산 심의·승인
3. 정보보호 활동 계획의 심의·승인
4. 기타 정보보호최고책임자가 필요하다고 인정하는 사항



※ 정보보호 위원회 조직도 (이해를 돕기 위한 예시)

정보보호위원회 회의록	
회의명	2025. 제 OO차 정보보호위원회 회의
회의일시	2025.OO.OO 13:00 ~ 16:00
참석자	OOO, OOO, OOO
심의안건	정보보호정책 및 지침 제·개정

심의내용	개인정보 보호법 및 유관 법 및 시행규칙의 개정에 따라, 관련 개정내용의 정보보호정책서 내 반영 필요성 및 반영여부 결정 1. 개인정보보호법 제31조의2(국내대리인의 지정) 관련 - 국내대리인 지정요건(동법 제31조의2 2항)에 따라, 국내대리인 지정 및 관련 관리·감독 수행			
심의결과	원안 가결 1. 국내대리인 지정 및 관리·감독			
서명	OOO	OOO	OOO	OOO

※ 정보보호위원회 회의록 (이해를 돕기 위한 예시)

◇ 전사적 정보보호 및 개인정보보호 활동을 위하여 정보보호 및 개인정보보호 관련 담당자 및 부서별 담당자로 구성된 실무 협의체를 구성하여 운영하고 있는가?

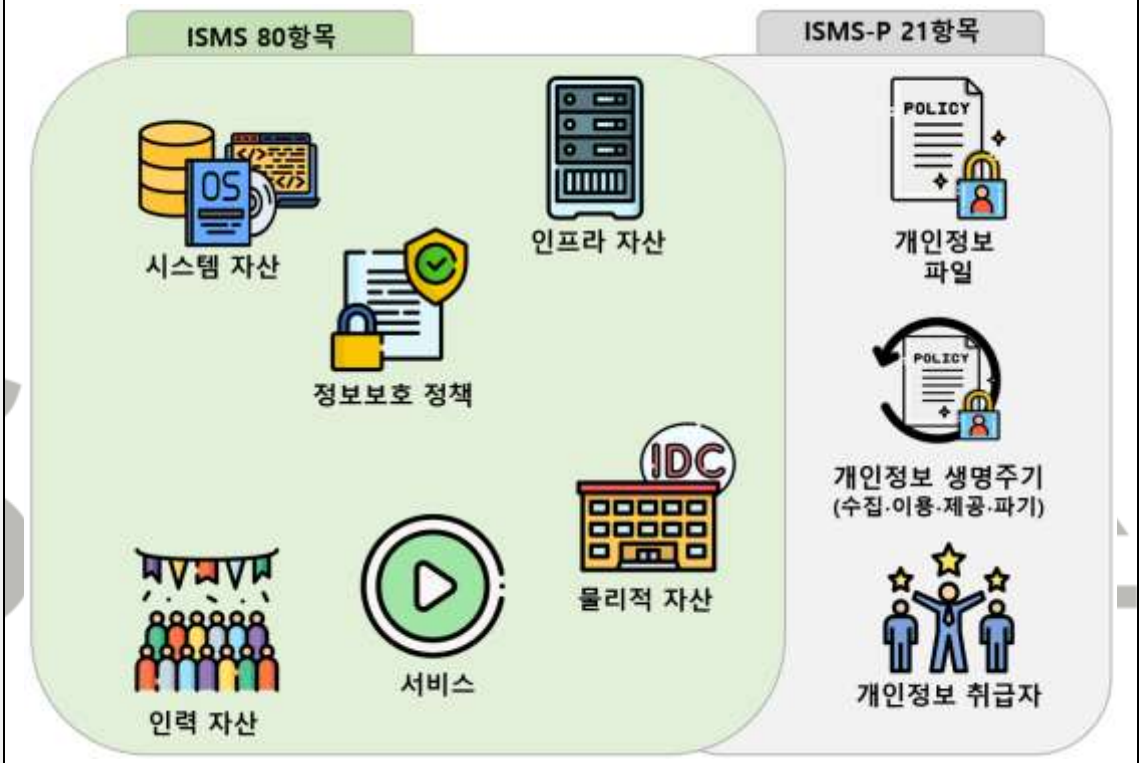
(예시) 정보보호 실무 협의체 구성 문서화

「**정보보호 조직 관리지침**」 제 ○○조 (정보보호 실무 협의체)

① 정보보호 실무 협의체는 정보보호위원회의 심의·의결사항에 따른 실무적인 검토, 세부 이행방안 수립, 원활한 정보보호 관리활동의 조정 등의 업무를 수행한다.

② 정보보호 실무 협의체는 연 1회 이상 개최하되, 특별한 사유 발생 시 비정기적으로 회의를 소집할 수 있다.

1.1.4 범위 설정

세부분야	1.1.4 범위 설정
인증 기준	조직의 핵심 서비스와 개인정보 처리 현황 등을 고려하여 관리체계 범위를 설정하고, 관련된 서비스를 비롯하여 개인정보 처리 업무와 조직, 자산, 물리적 위치 등을 문서화하여야 한다.
주요 확인사항	• 조직의 핵심 서비스 및 개인정보 처리에 영향을 줄 수 있는 핵심자산을 포함하도록 관리체계 범위를 설정하고 있는가? • 정의된 범위 내에 예외사항이 있을 경우 명확한 사유 및 관련자 협의·책임자 승인 등 관련 근거를 기록·관리하고 있는가? • 정보보호 및 개인정보보호 관리체계 범위를 명확히 확인할 수 있도록 관련된 내용(주요 서비스 및 업무 현황, 정보시스템 목록, 문서 목록 등)이 포함된 문서를 작성하여 관리하고 있는가?
기준 요약도	
운영 방안	**◇ 조직의 핵심 서비스 및 개인정보 처리에 영향을 줄 수 있는 핵심자산을 포함하도록 관리체계 범위를 설정하고 있는가?** **자산 범위 설정 시 고려사항** ① ISMS 및 ISMS-P 인증범위 기준 1. ISMS : **정보통신서비스를 기준**으로 관련된 정보시스템, 장소, 조직 및 인력을 포함 2. ISMS-P : ISMS 인증범위에 더하여 해당 서비스에서 처리되는 **개인정보의 흐름**에 따라 해당 개인정보를 처리하는 정보시스템, 조직 및 인력, 물리적 장소 등을 모두 포함

② ISMS 인증범위 설정 고려사항

1. 인증 의무대상자는 신청기관의 정보통신서비스를 모두 포함하여 설정
2. 백오피스 시스템은 인증범위에 포함
3. 정보통신서비스와 직접적인 관련성이 낮은 ERP, DW, 그룹웨어 등 기업 내부 시스템과 영업/마케팅 조직은 일반적으로 인증범위에서 제외 가능

③ ISMS-P 인증범위 설정 고려사항

1. **ISMS-P 인증은 의무사항이 아니므로, 자율적으로 인증을 받고자 하는 서비스를 지정**
2. 인증 받고자 하는 서비스의 범위는 이용자 중심의 대외 서비스만 포함할 것인지 임직원이 이용하는 내부 서비스까지 포함할 것인지에 대해서 고려
3. 다만, ISMS 인증 의무대상자가 ISMS-P 인증으로 대체하고자 하는 경우 ISMS-P 인증범위에는 ISMS 인증범위를 반드시 모두 포함

④ 그 외 고려사항

1. 클라우드서비스를 이용하여 서비스를 제공하는 경우, 클라우드 서비스 유형(IaaS, PaaS, SaaS) 등에 따른 책임 범위에 따라 신청기관이 직접 관리 가능한 영역에 대하여 인증범위에 포함
2. 영리를 목적으로 하지 않더라도 정보통신망을 통해 정보를 제공하거나 정보의 제공을 매개하는 서비스는 모두 인증범위에 포함
3. 기타 시스템 유형 별 인증범위 고려사항(인증 대상 서비스와 직접적으로 관련된 네트워크 장비 범위포함, 내부업무 처리 목적의 그룹웨어 범위제외 등) 반영

자산 범위 설정 예시

① ISMS 인증범위

「**네트워크 및 보안 시스템**」 라우터, 스위치, 방화벽 IPS/IDS, 웹방화벽 등

「**서버 존**」 서버, 데이터베이스, 보안시스템

「**정보통신서비스 관리시스템**」 관리시스템(back office), 모니터링 시스템 등

「**개발 환경**」 개발 및 테스트 서버, 테스트 데이터베이스 등

「**업무 환경**」 인증범위 내 인력, IT 운영자, 정보통신 관리자, 개발자 등의 단말

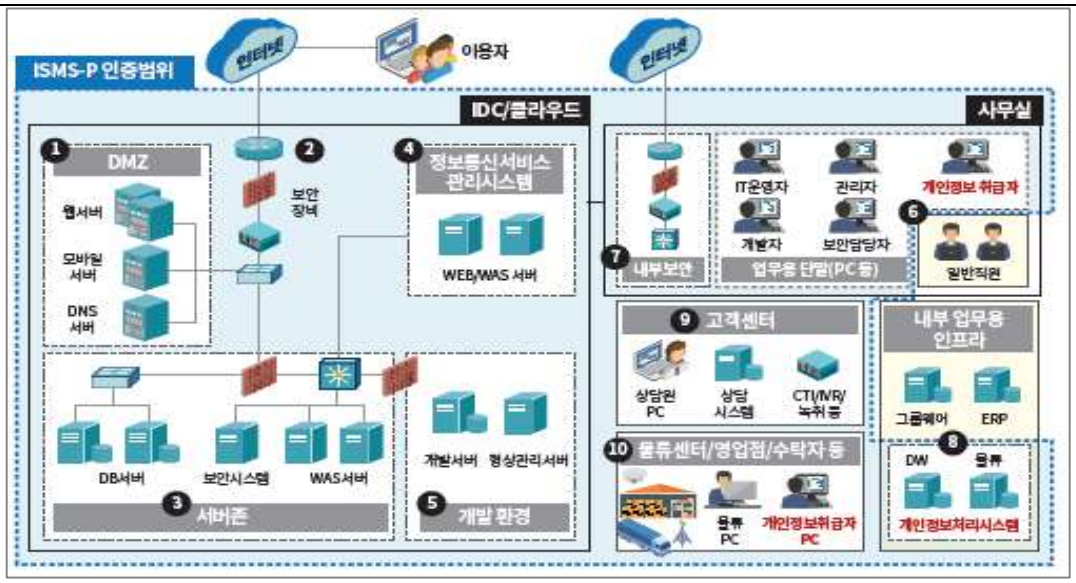
「**내부용 네트워크 및 보안 시스템**」 라우터, 스위치, DRM, DLP, PMS 등

「**내부 업무용 인프라**」 그룹웨어, ERP 등

② ISMS + P 추가 인증범위

「**고객센터**」 상담원, 팩스시스템, 녹취시스템 등

「**물류 센터**」 영업점·개인정보 수탁사 등: 대리점, POS, 업무용 단말 등



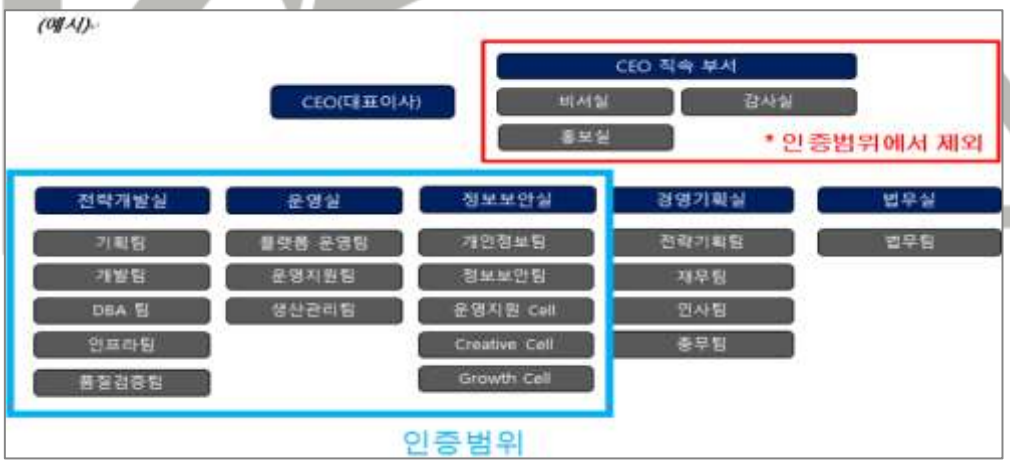
※ 출처: 정보보호 및 개인정보보호 관리체계 인증제도 안내서(KISA, 2024.07)

◇ 정의된 범위 내에 예외사항이 있을 경우 명확한 사유 및 관련자 협의 · 책임자 승인 등 관련 근거를 기록·관리하고 있는가?

(예시)범위 내 예외 사항

① 정보보호 및 개인정보보호의 업무 범위를 벗어난 조직 제외

1. 비서실, 감사실, 홍보실 등 서비스 제공을 위한 업무 조직이 아닌 경우.



※ 출처: 정보보호 및 개인정보보호 관리체계 인증신청 양식 (KISA)

2. 인증범위 제외 조직 목록 및 사유 작성

부서명	대상 제외 사유	규모
비서실	고객정보 미취급	O명
홍보실	고객정보 미취급	O명
감사실	고객정보 미취급	O명

② 정보보호 및 개인정보보호의 업무 범위를 벗어난 자산 제외

1. ERP, 그룹웨어 등 서비스 제공을 위한 자산이 아닌 경우도 동일

시스템	대상 제외 사유	규모
ERP서버	고객정보 미취급	O식
그룹웨어	고객정보 미취급	O식

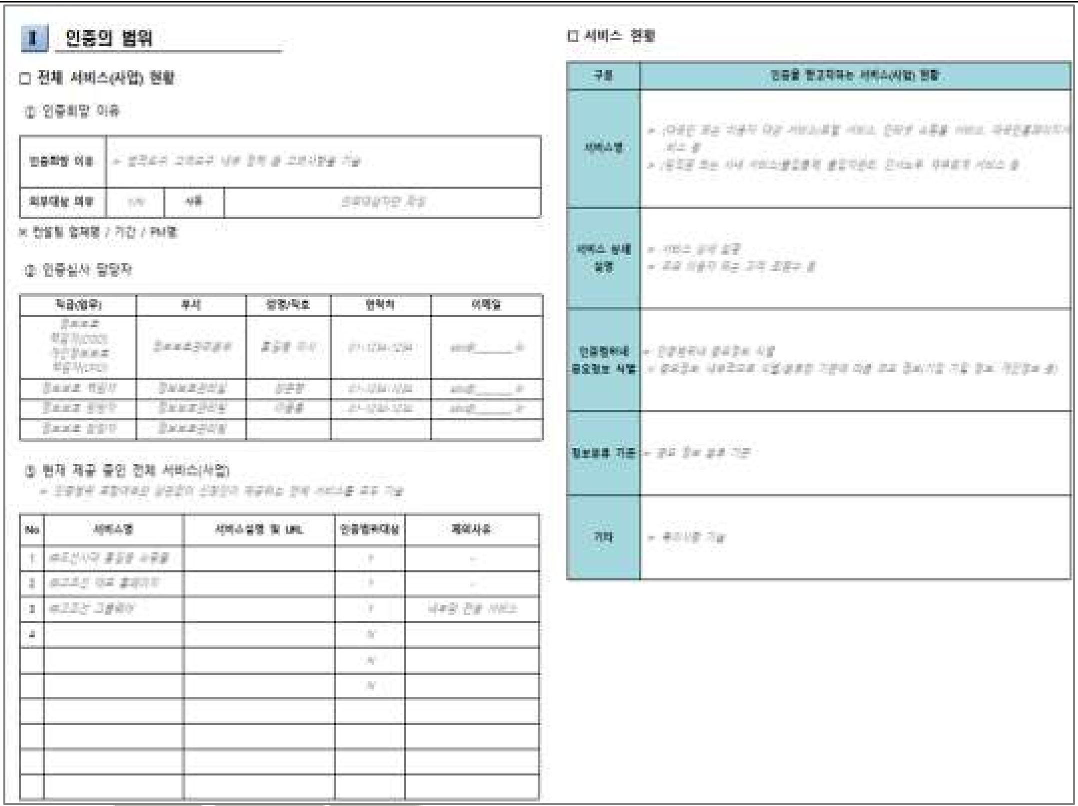
③ 인증범위에서 제외되는 서비스, 정보시스템 등에 대해서는 내부 협의 및 책임자 승인을 거친 후 그 사유 및 근거에 대하여 기록하여 관리

◇ 정보보호 및 개인정보보호 관리체계 범위를 명확히 확인할 수 있도록 관련된 내용(주요 서비스 및 업무 현황, 정보시스템 목록, 문서 목록 등)이 포함된 문서를 작성하여 관리하고 있는가?

정보보호 및 개인정보보호 관리체계 범위 문서화

① 정보보호 및 개인정보보호 관리체계 인증 시 범위 산정 문서로 예시 대체

1. 주요 서비스 및 업무 현황(개인정보 처리 업무 현황 포함)
2. 서비스 제공과 관련된 조직 현황(조직도 등)
3. 정보보호 및 개인정보보호 조직 현황
4. 주요 설비 목록
5. 정보시스템 목록 및 네트워크 구성도
6. 정보자산, 개인정보 관련 자산식별 기준 및 자산현황
7. 정보보호 및 개인정보보호 시스템 목록
7. 서비스(시스템) 구성도 및 개인정보(수집, 이용, 제공, 저장, 관리, 파기) 처리
8. 문서 목록(예: 정책, 지침, 매뉴얼, 운영명세서 등)
9. 정보보호 및 개인정보보호 관리체계 수립 방법 및 절차, 관련 법적 준거성 검토, 내부감사
10. 고객센터, IDC, IT 개발 및 운영 등 외주(위탁)업체 현황 등



※ 출처: 정보보호 및 개인정보보호 관리체계 인증신청 양식 (KISA)

1.1.5 정책 수립

<table>
<tr><th>세부분야</th><th>1.1.5 정책 수립</th></tr>
<tr><td>인증
기준</td><td>정보보호와 개인정보보호 정책 및 시행문서를 수립·작성하며, 이때 조직의 정보보호와 개인정보보호 방침 및 방향을 명확하게 제시하여야 한다. 또한 정책과 시행문서는 경영진의 승인을 받고, 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 조직이 수행하는 모든 정보보호 및 개인정보보호 활동의 근거를 포함하는 최상위 수준의 정보보호 및 개인정보보호 정책을 수립하고 있는가?
• 정보보호 및 개인정보보호 정책의 시행을 위하여 필요한 세부적인 방법, 절차, 주기 등을 규정한 지침, 절차, 매뉴얼 등을 수립하고 있는가?
• 정보보호 및 개인정보보호 정책·시행문서의 제·개정 시 최고경영자 또는 최고경영자로부터 권한을 위임받은 자의 승인을 받고 있는가?
• 정보보호 및 개인정보보호 정책·시행문서의 최신본을 관련 임직원에게 이해하기 쉬운 형태로 제공하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 조직이 수행하는 모든 정보보호 및 개인정보보호 활동의 근거를 포함하는 최상위 수준의 정보보호 및 개인정보보호 정책을 수립하고 있는가?

정보보호 및 개인정보보호 정책 수립
① 정보보호 정책서: 조직의 정보자산을 보호하고, 정보보안을 달성하기 위한 기본적인</td></tr>
</table>

목표와 방향, 원칙을 설정하는 최상위 문서

② 지침 : 정보보호 정책에 따라, 특정 영역·분야 별 세부사항에 대해 규정

③ 가이드라인/매뉴얼 : 실행방식 및 절차의 권고적 사항

※ 정보보호정책 수립 (이해를 돕기 위한 예시)

※ 참고사항 : 개인정보의 안전성 확보조치 기준(2025.10.31)

① '12. 출력·복사시 안전조치에 관한 사항', '13. 개인정보의 파기에 관한 사항'을 내부 관리계획 수립대상에 포함

◇ 정보보호 및 개인정보보호 정책의 시행을 위하여 필요한 세부적인 방법, 절차, 주기 등을 규정한 지침, 절차, 매뉴얼 등을 수립하고 있는가?

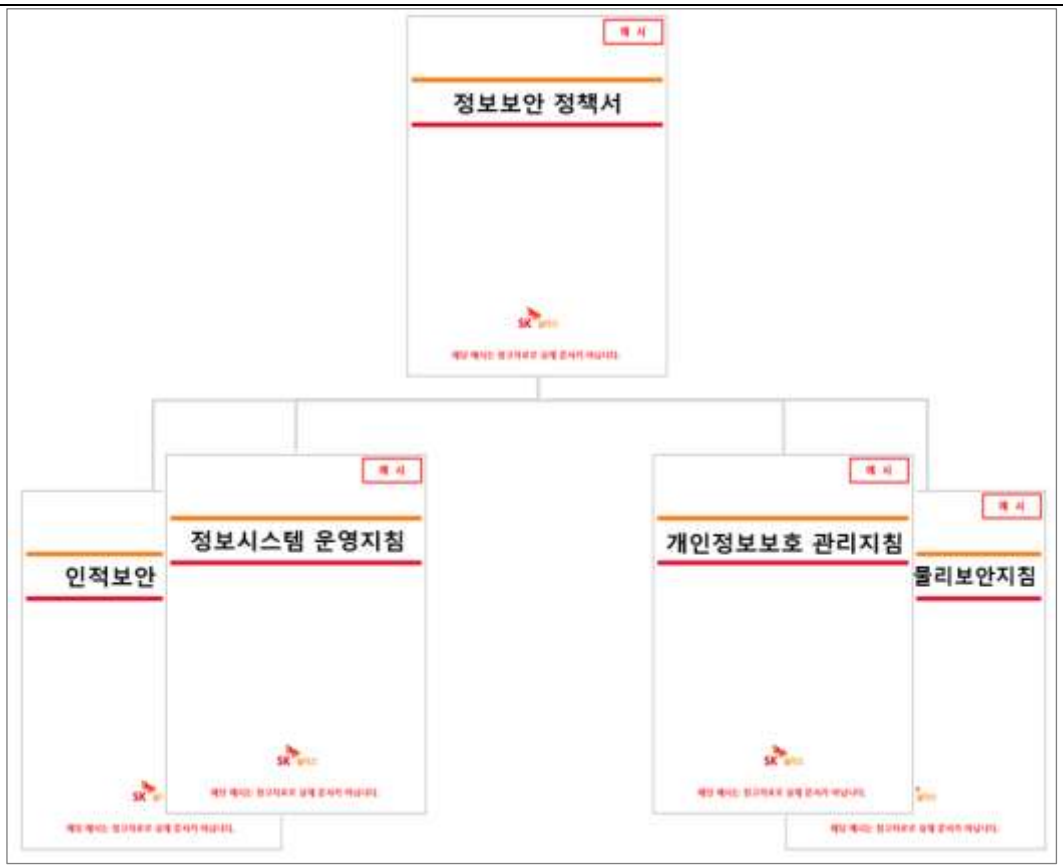
세부적인 방법 및 절차, 주기 등 하위 실행 문서 작성

① 정보보호 관리지침: 정보보호 조직, 교육, 감사, 임직원 보안, 위·수탁 계약 등 규정

② 서버운영 보안지침: 서버 보안성 검토, 취약점 점검, 패스워드 정책, 접근권한 검토 규정

③ 임직원 보안지침: 계정 및 패스워드, PC지급 및 사용, 인터넷, 이메일 사용 등

④ 그 외 세부 사항에 대한 지침 작성



※ 내부 지침서 수립 (이해를 돕기 위한 예시)

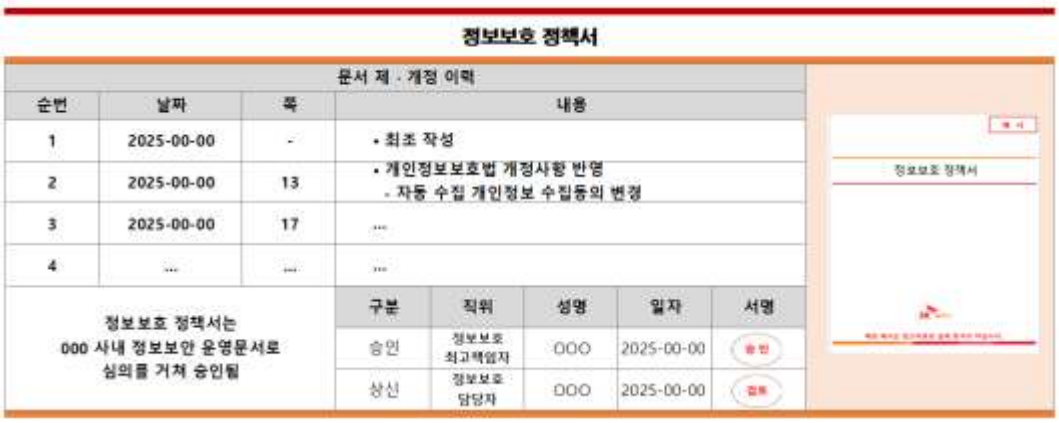
◇ 정보보호 및 개인정보보호 정책·시행문서의 제·개정 시 최고경영자 또는 최고경영자로부터 권한을 위임받은 자의 승인을 받고 있는가?

경영진 정보보호 활동 참여

「정보보호 조직 관리지침」 제 ○○조 (정보보호위원회)

① 정보보호위원회는 다음의 역할을 수행한다.

1. 정보보호정책 및 지침의 제·개정에 대한 심의·승인
2. 정보보호 예산 심의·승인
3. 정보보호 활동 계획의 심의·승인
4. 기타 정보보호최고책임자가 필요하다고 인정하는 사항



정보보호 정책서

문서 제 · 개정 이력

순번	날짜	쪽	내용
1	2025-00-00	-	• 최초 작성
2	2025-00-00	13	• 개인정보보호법 개정사항 반영 - 자동 수집 개인정보 수집동의 변경
3	2025-00-00	17	…
4	…	…	…

정보보호 정책서는
000 사내 정보보안 운영문서로
심의를 거쳐 승인됨

구분	직위	성명	일자	서명
승인	정보보호 최고책임자	OOO	2025-00-00	
상신	정보보호 담당자	OOO	2025-00-00	

※ 경영진의 정책 승인(이해를 돕기 위한 예시)

◇ 정보보호 및 개인정보보호 정책·시행문서의 최신본을 관련 임직원에게 이해하기 쉬운 형태로 제공하고 있는가?

(예시) 정보보호 및 개인정보보호 정책 내부 직원 공유·전파

① 임직원이 접근하기 쉬운 방법으로 지침 및 가이드 제공

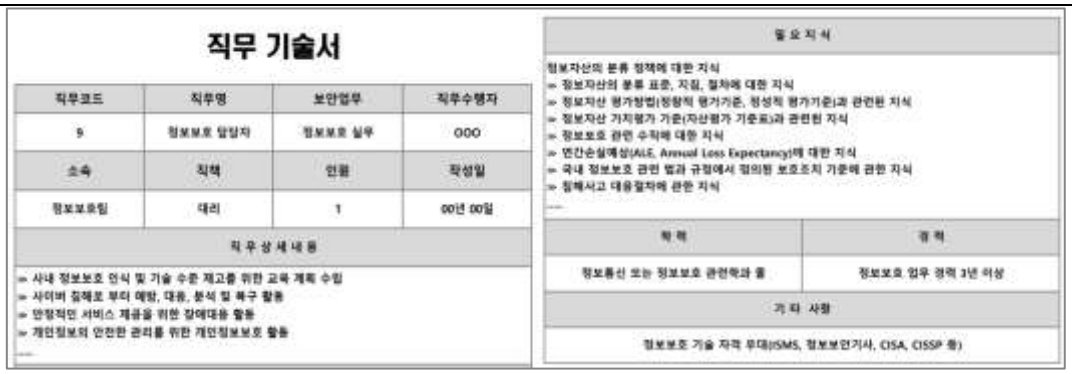
공지사항

No.	첨부	구분	제목	부서
808		[정보보호]	[안내] 2025년 정보보호 시행문서 일부 개정 안내	개인정보팀
789		[정보보호]	[안내] 2025년 전사 정보보호 시행문서 2차 개정 안내	개인정보팀
725		[정보보호]	[안내] 2025년 전사 정보보호 시행문서 개정 안내 (2)	개인정보팀
346		[정보보호]	[안내] 2023년 사내 정보보호 정책 문서 일부 개정 안내	개인정보보호팀
315		[정보보호]	[안내] 2023년 사내 정보보호 정책 문서 개정 안내	개인정보보호팀

※ 출처 : SK쉴더스 정보보호 시행문서 개정 안내 공지(SK쉴더스)

1.1.6 자원 할당

세부분야	1.1.6 자원 할당
인증기준	최고경영자는 정보보호와 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고, 관리체계의 효과적 구현과 지속적 운영을 위한 예산 및 자원을 할당하여야 한다.
주요 확인사항	• 정보보호 및 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고 있는가? • 정보보호 및 개인정보보호 관리체계의 효과적 구현과 지속적 운영을 위하여 필요한 자원을 평가하여 필요한 예산과 인력을 지원하고 있는가? • 연도별 정보보호 및 개인정보보호 업무 세부추진 계획을 수립·시행하고, 그 추진결과에 대한 심사분석·평가를 실시하고 있는가?
기준 요약도	
운영 방안	**◇ 정보보호 및 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고 있는가?** **정보보호 전문성을 갖춘 인력 확보** ① 전문 지식 및 관련 자격 보유 ② 정보보호 및 개인정보보호 관련 실무 경력 보유 ③ 정보보호 및 개인정보보호 관련 직무교육 이수 등



직무 기술서

직무코드	직무명	보안업무	직무수행자
9	정보보호 담당자	정보보호 실무	OOO
소속	직책	인원	작성일
정보보호팀	대리	1	00년 00월

직 무 상 세 내 용

- 사내 정보보호 인식 및 기술 수준 제고를 위한 교육 계획 수립
- 사이버 침해로 부터 예방, 대응, 분석 및 복구 활동
- 안정적인 서비스 제공을 위한 장애대응 활동
- 개인정보의 안전한 관리를 위한 개인정보보호 활동

필 요 지 식

정보자산의 분류 정책에 대한 지식
- 정보자산의 분류 표준, 지침, 절차에 대한 지식
- 정보자산 평가방법(정량적 평가기준, 정성적 평가기준)과 관련된 지식
- 정보자산 가치평가 기준(자산평가 기준표)과 관련된 지식
- 정보보호 관련 수치에 대한 지식
- 연간손실예상(ALE, Annual Loss Expectancy)에 대한 지식
- 국내 정보보호 관련 법과 규정에서 정의된 보호조치 기준에 관한 지식
- 침해사고 대응절차에 관한 지식

학 력	경 력
정보통신 또는 정보보호 관련학과 졸	정보보호 업무 경력 3년 이상

기 타 사 항

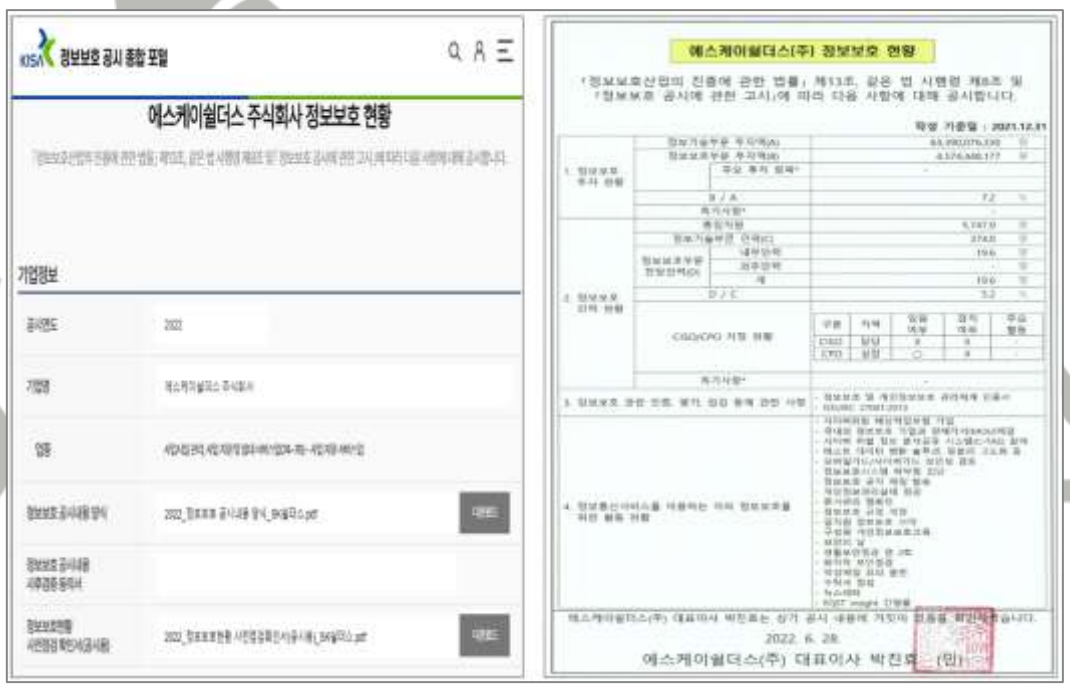
정보보호 기술 자격 우대(ISMS, 정보보안기사, CISA, CISSP 등)

※ 직무기술서 (이해를 돕기 위한 예시)

◇ 정보보호 및 개인정보보호 관리체계의 효과적 구현과 지속적 운영을 위하여 필요한 자원을 평가하여 필요한 예산과 인력을 지원하고 있는가?

정보보호 및 개인정보보호 관리체계 지속 지원

① 예산과 자원을 평가하여 예산 및 인력운영 계획 수립 및 승인 필요



※ 출처: 에스케이쉴더스 주식회사 정보보호 현황 (정보보호 공시 종합 포털)

◇ 연도별 정보보호 및 개인정보보호 업무 세부추진 계획을 수립·시행하고, 그 추진결과에 대한 심사분석 · 평가를 실시하고 있는가?

세부추진 계획 수립 및 추진결과 심사분석 · 평가

「**정보보호 조직 관리지침**」 제 ○○조 (정보보호 활동계획 수립 및 심사)

① 해당 연도의 정보보호 및 개인정보보호 업무를 효과적으로 수행하기 위한 연도별

정보보호 및 개인정보보호 업무 세부추진 계획을 수립하고 경영진 보고 및 시행

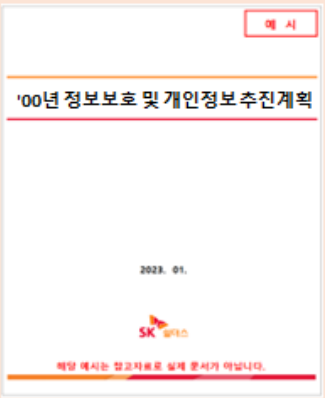
1. 해당연도의 추진계획과 전년도 추진결과에 대한 분석 및 평가 필요

② 세부추진 계획에 따른 추진결과를 심사분석 및 평가하여 경영진에게 보고

00년 정보보호 및 개인정보 추진계획

순번	내용
1	개요
2	OO년(전년도) 추진실적
3	정보보호 및 개인정보 운영 현황
4	OO년 세부 추진계획
5	기타 사항

구분	직위	성명	일자	서명
승인	정보보호 최고책임자	OOO	OOOO-OO-OO	승인
상신	정보보호 담당자	OOO	OOOO-OO-OO	-



※ 정보보호 및 개인정보 추진계획 심사분석 · 평가(이해를 돕기 위한 예시)

1.2 위험관리

1.2.1 정보자산 식별

세부분야	1.2.1 정보자산 식별
인증 기준	조직의 업무특성에 따라 정보자산 분류 기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.
주요 확인사항	• 정보자산의 분류 기준을 수립하고 정보보호 및 개인정보보호 관리체계 범위 내의 모든 자산을 식별하여 목록으로 관리하고 있는가? • 식별된 정보자산에 대하여 법적 요구사항 및 업무에 미치는 영향 등을 고려하여 중요도를 결정하고 보안등급을 부여하고 있는가? • 정기적으로 정보자산 현황을 조사하여 정보자산 목록을 최신으로 유지하고 있는가?
기준 요약도	
운영 방안	◇ 정보자산의 분류 기준을 수립하고 정보보호 및 개인정보보호 관리체계 범위 내의 모든 자산을 식별하여 목록으로 관리하고 있는가? 정보자산 분류 및 식별

「**정보자산 관리지침**」 제 ○○조 (정보자산 식별)

① 운영되는 모든 정보자산을 식별하고 관리하여야 한다.

② 식별된 정보자산은 별첨 "정보자산 관리대장"으로 목록화 하여 관리하고, 해당 목록은 최신의 자산상태를 반영하여야 한다

③ 주기적(반기 별 1회)으로 정보자산 현황을 조사하여 정보자산 목록을 최신으로 유지하여야 한다.

④ 정보자산은 다음 각 호와 같이 분류하고 최신화 관리해야 한다.

1. 정보(전자문서, 종이문서)
2. 서버, 스토리지
3, 네트워크, 정보보안 시스템
4. 응용프로그램(소프트웨어)
5. 업무용 단말기(노트북, 태블릿, 모바일 등)
6. 보조기억매체(USB, 외장형 하드디스크)
7. 물리적 시설(출입통제 설비, 항온항습기, UPS, 소화설비, 냉·난방 설비, 발전기 등)
8. 기타 서비스 운영에 필요한 정보자산(클라우드 서비스 등)

정보자산 관리대장

정보보호업임자	정보보호최고책임자

구분			호스트명	자산명	IP주소	자산위치	장비 상세내역					관리번호	관리부서	관리자	자산 가치평가		
							CPU	메모리	HDD	OS	모델명				기밀성	무결성	가용성
무형자산	정보																
	응용프로그램		APP01	CRM 시스템	192.168.1.10	서버실 2층	Intel Xeon E5-2690 v3	32GB	1TB SSD	Windows Server 2019	Microsoft Dynamics 365	APP01	IT 부서	김철수	3	3	3
유형자산	서버	DNS	DNS01	DNS 서버	192.168.1.100	서버실 1층	Intel Xeon E5-2630 v4	Intel Xeon E5-2630 v4	600GB SAS	Ubuntu 20.04	Dell PowerEdge R640	APP01	IT 부서	박영수	3	3	3
		DHCP															
		DB															
		공개서버															
		관리용서버															
		응용서버															
		로그서버															
		기타															
	네트워크	라우터															
		스위치															
		기타															
	정보보호 시스템	F/W															
		IDS/IPS															
		웹방화벽															
		VPN															
	업무용 단말기																

구분	모델명	자산위치	장비 상세내역	관리번호	관리부서	관리자	자산 가치평가		
							기밀성	무결성	가용성
항전기									
항온항습기									
소방시설									
UPS									

※ 정보자산 관리대장 (이해를 돕기 위한 예시)

◇ 식별된 정보자산에 대하여 법적 요구사항 및 업무에 미치는 영향 등을 고려하여 중요도를 결정하고 보안등급을 부여하고 있는가?

정보자산 목록 및 중요도 산정

「**정보자산 관리지침**」 제 ○○조 (정보자산 중요도 평가)

① 정보자산의 중요도 평가 기준을 수립하여 평가 기준에 따라 정보자산의 중요도를 산정한다.

② 정보자산은 기밀성, 무결성, 가용성을 기준으로 1등급, 2등급, 3등급으로 분류한다.

정보자산 중요도 산정기준

가용성(Availability)	중요도	상세 기준
심각	3	• 치명적인 영향을 초래할 수 있는 경우 (예시)
주의	2	• 업무활동에 상당한 영향을 끼칠 수 있는 경우 (예시)
경미	1	• 손실에 대한 영향이 크지 않은경우 (예시)
기밀성(Cofidentiality)	중요도	상세 기준
심각	3	• 치명적인 영향을 초래할 수 있는 경우 (예시)
주의	2	• 업무활동에 상당한 영향을 끼칠 수 있는 경우 (예시)
경미	1	• 손실에 대한 영향이 크지 않은경우 (예시)
무결성(Integrity)	중요도	상세 기준
심각	3	• 치명적인 영향을 초래할 수 있는 경우 (예시)
주의	2	• 업무활동에 상당한 영향을 끼칠 수 있는 경우 (예시)
경미	1	• 손실에 대한 영향이 크지 않은경우 (예시)

정보자산 중요도 평가 기준

보안 등급(중요도) = 가용성(A) + 기밀성(C) + 무결성(I)

자산 등급	등급 분류 가준	자산 가치
1등급	8 ~ 9 점	상 (High)
2등급	5 ~ 7 점	중 (Medium)
3등급	3 ~ 4 점	하 (Low)

※ 정보자산 중요도 산정기준 (이해를 돕기 위한 예시)

◇ 정기적으로 정보자산 현황을 조사하여 정보자산 목록을 최신으로 유지하고 있는가?

정보자산 현황 조사 및 목록 최신화

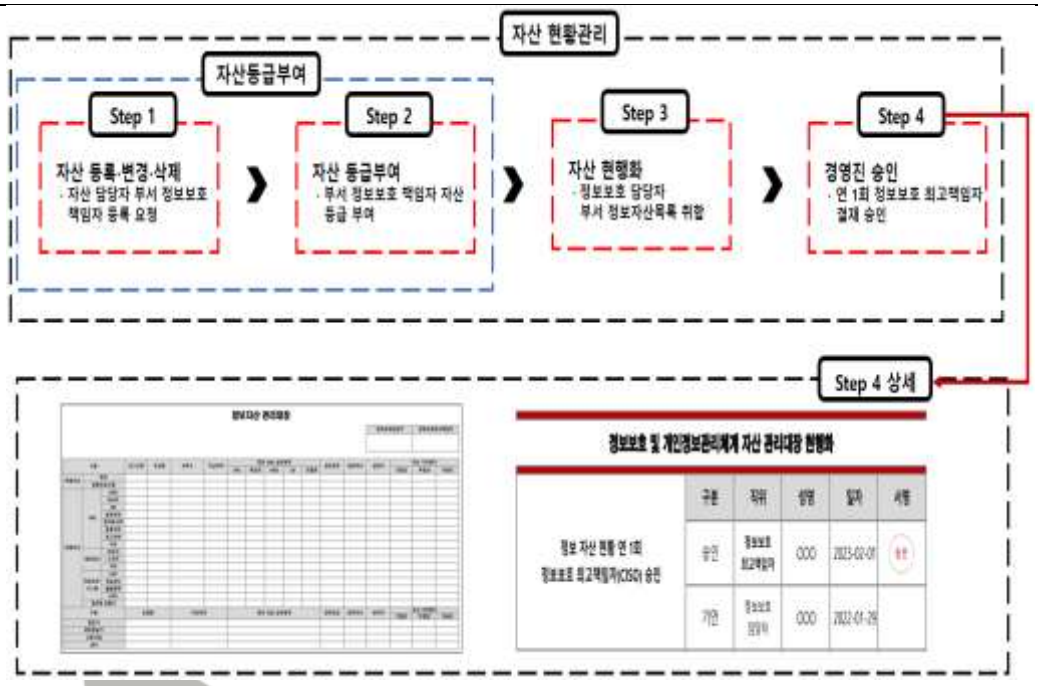
「**정보자산 관리지침**」 제 ○○조 (정보자산 등록)

① 자산 등록·변경·삭제는 정보 소유자가 필요 시 부서 정보보호 책임자의 허가를 득하고 부서 자산목록에 직접 등록한다.

② 부서 정보보호 책임자는 등록된 자산의 보안 등급에 따라 자산코드를 부여하여야 한다.

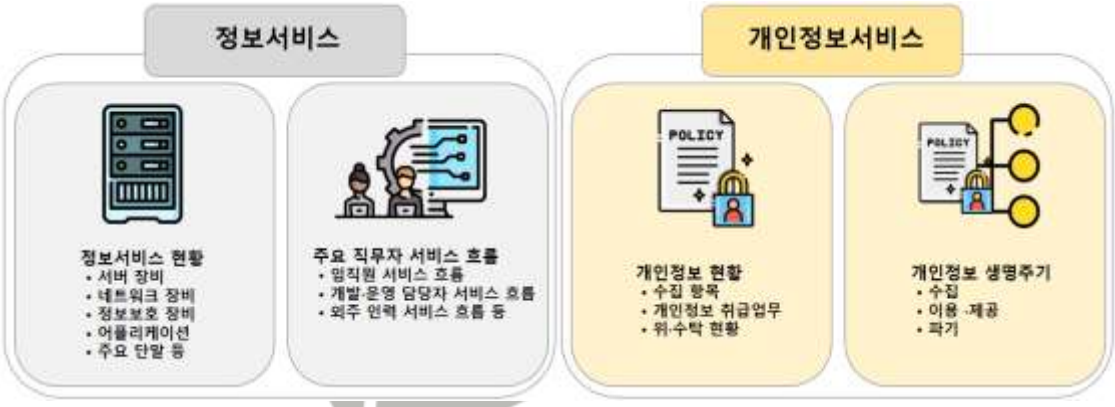
③ 정보보호담당자는 분기별 각 부서의 자산목록을 검토, 취합, 현행화한다.

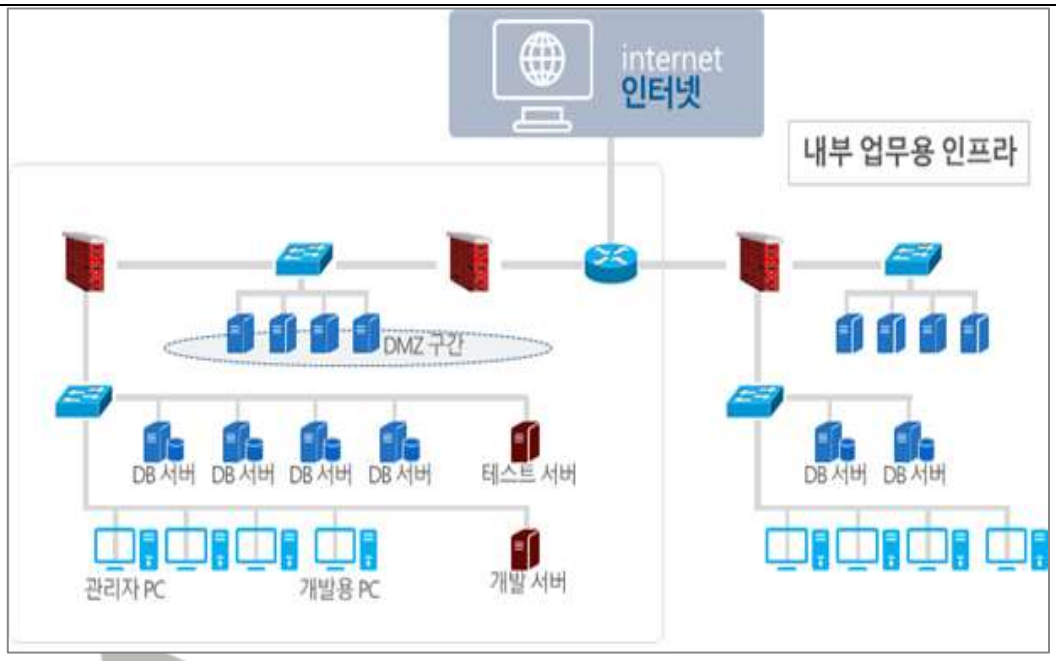
④ 정보보호담당자는 연 1회 이상 자산현황을 실사하여야 하며, 그 결과를 정보보호 최고책임자에게 보고해야 한다.



※ 정보자산 현행화 절차 (이해를 돕기 위한 예시)

1.2.2 현황 및 흐름분석

세부분야	1.2.2 현황 및 흐름분석
인증기준	관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.
주요 확인사항	• 관리체계 전 영역에 대한 정보서비스 현황을 식별하고 업무 절차와 흐름을 파악하여 문서화하고 있는가? • 관리체계 범위 내 개인정보 처리 현황을 식별하고 개인정보의 흐름을 파악하여 개인정보 흐름도 등으로 문서화하고 있는가? • 서비스 및 업무, 정보자산 등의 변화에 따른 업무절차 및 개인정보 흐름을 주기적으로 검토하여 흐름도 등 관련 문서의 최신성을 유지하고 있는가?
기준 요약도	
운영 방안	**◇ 관리체계 전 영역에 대한 정보서비스 현황을 식별하고 업무 절차와 흐름을 파악하여 문서화하고 있는가?** **정보시스템 흐름 파악** ① 관리체계 범위 내 모든 정보서비스 현황 1. DB 서버, 웹서버, 로그 모니터링 시스템 등 2. 네트워크 장비(예. 라우터, 스위치 등) 3. 정보보호 관련 장비 (예. 방화벽, 침입 탐지 시스템, 침입 방지 시스템 등) 4. DMZ 구역, VPN 구간 등



※ 출처: 정보보호 및 개인정보보호 관리체계 인증신청 양식 (KISA)

② 정보서비스별 업무 절차 및 흐름 파악

1. 정보서비스 및 개인정보처리에 관한 현황 및 흐름분석

③ 업무 절차 및 흐름에 대한 문서화

※ 출처: 정보보호 및 개인정보보호 관리체계 인증신청 양식 (KISA)

◇ 관리체계 범위 내 개인정보 처리 현황을 식별하고 개인정보의 흐름을 파악하여 개인정보 흐름도 등으로 문서화하고 있는가?

(예시) 개인정보 생명주기(Life Cycle)에 따른 흐름도 작성

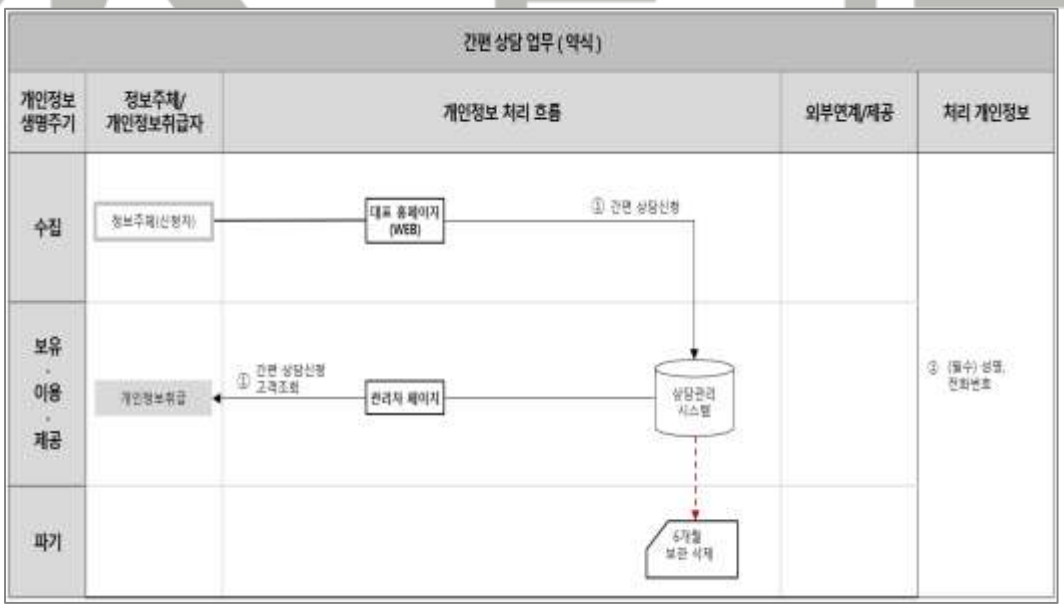
① 전문상담 예약(이름, 연락처 수집)

개인정보 흐름표

번호	업무	수집항목	수집경로	수집주기	수집부터	보관기간
1	전문상담예약	이름 / 연락처	대표 홈페이지	상시	고객상담팀	상담 신청 후 6개월 보관/이용 후 파기

※ 개인정보 흐름표 (이해를 돕기 위한 예시)

② "간편 상담" 업무 개인정보 흐름도



※ 개인정보 흐름도 (이해를 돕기 위한 예시)

개인정보 흐름 분석 단계별 세부절차

① 개인정보 처리 업무 현황분석

② 개인정보 흐름표 작성

③ 개인정보 흐름도 작성

④ 정보시스템 구성도 작성

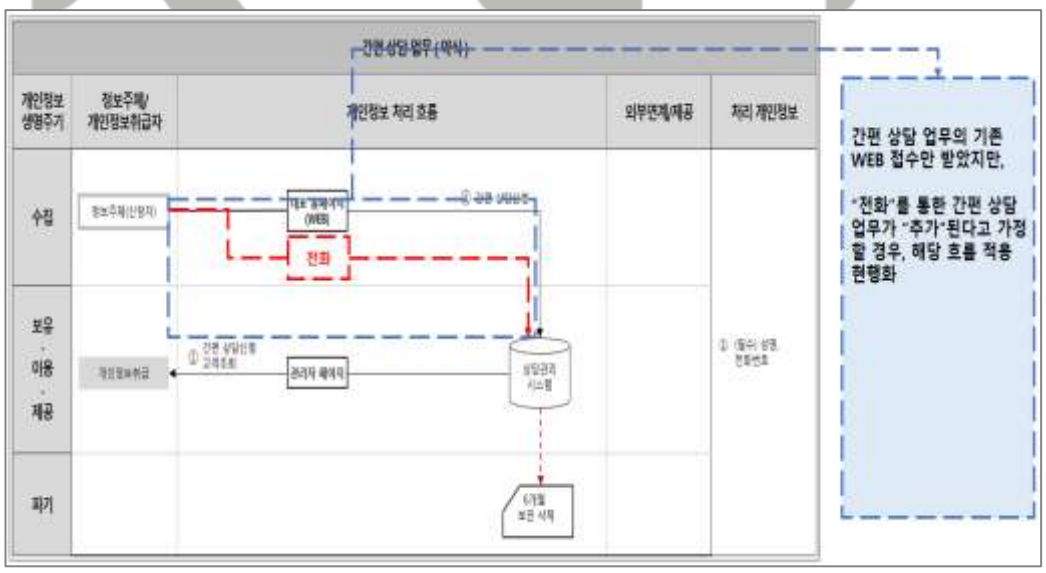
※ 출처: 개인정보 영향평가 수행안내서 (개인정보보호위원회·KISA)

◇ 서비스 및 업무, 정보자산 등의 변화에 따른 업무절차 및 개인정보 흐름을 주기적으로 검토하여 흐름도 등 관련 문서의 최신성을 유지하고 있는가?

주기적(최소 연 1회 이상) 검토 및 정보 흐름 최신성 유지

① 기존 서비스, 업무 및 개인정보 흐름의 변화 여부

1. 신규 서비스 오픈 또는 개편, 업무절차의 변경, 개인정보 처리 방법 변화, 조직의 변경, 외부 연계 및 제공 흐름 변경 등



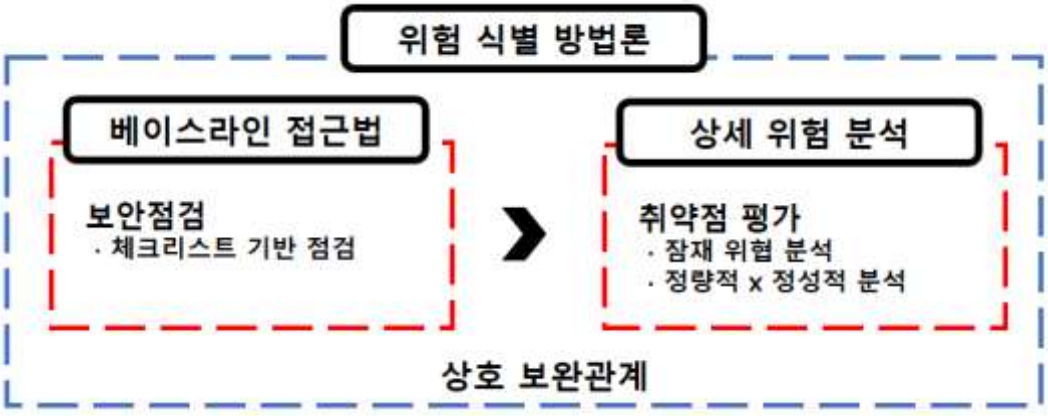
※ 개인정보 흐름도 변경 사항 반영 (이해를 돕기 위한 예시)

1.2.3 위험 평가

세부분야	1.2.3 위험 평가
인증 기준	조직의 대내외 환경분석을 통하여 유형별 위협정보를 수집하고 조직에 적합한 위험 평가 방법을 선정하여 관리체계 전 영역에 대하여 연 1회 이상 위험을 평가하며, 수용할 수 있는 위험은 경영진의 승인을 받아 관리하여야 한다.
주요 확인사항	• 조직 또는 서비스의 특성에 따라 다양한 측면에서 발생할 수 있는 위험을 식별하고 평가할 수 있는 방법을 정의하고 있는가? • 위험관리 방법 및 절차(수행인력, 기간, 대상, 방법, 예산 등)를 구체화한 위험관리 계획을 매년 수립하고 있는가? • 위험관리 계획에 따라 연 1회 이상 정기적으로 또는 필요한 시점에 위험평가를 수행하고 있는가? • 조직에서 수용 가능한 목표 위험수준을 정하고, 그 수준을 초과하는 위험을 식별하고 있는가? • 위험식별 및 평가 결과를 경영진에게 보고하고 있는가?
기준 요약도	
운영 방안	**◇ 조직 또는 서비스의 특성에 따라 다양한 측면에서 발생할 수 있는 위험을 식별하고 평가할 수 있는 방법을 정의하고 있는가?** **(예시) 위험평가 방법 문서화** 「**위험평가 관리지침**」 제 ○○조 (위험식별) ① 정보 자산의 위험평가 방법은 각 호와 같이 적용한다.

1. 베이스라인 접근법: 식별 정보자산 공통적용(Gap analysis)

2. 상세 위험 분석: 자산분석·위협평가·취약성 평가를 거쳐 위험식별



※ 위험관리 방법론 (이해를 돕기 위한 예시)

◇ 위험관리 방법 및 절차(수행인력, 기간, 대상, 방법, 예산 등)를 구체화한 위험관리 계획을 매년 수립하고 있는가

(예시) 수행인력, 기간 대상, 방법, 예산 등 계획 반영

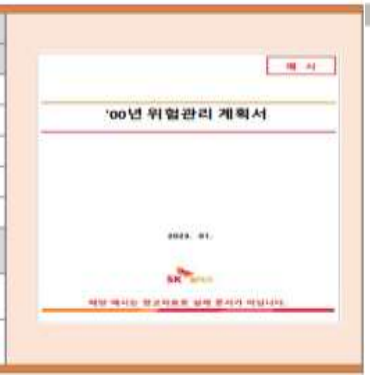
「**위험평가 관리지침**」제 ○○조 (위험평가)

① 위험관리 계획을 수립하고 위험관리 계획에 따라 연 1회 이상 위험평가를 실시한다.

1. 인력·대상·방법·예산 포함
2. 정보서비스 현황분석 및 흐름분석이 반영된 위험평가
3. 법적 요구사항 및 정보보호 관리체계 인증기준 준수 여부

00년 위험관리계획서

순번	내용			
1	위험관리 수행인력(역할)			
2	위험관리 기간			
3	위험관리 대상			
4	위험관리 방법			
5	위험관리 예산			
구분	직위	성명	일자	서명
승인	정보보호 최고책임자	OOO	2023-01-01	승인
상신	정보보호 담당자	OOO	2022-12-20	-



※ 위험관리 계획서 (이해를 돕기 위한 예시)

◇ 위험관리 계획에 따라 연 1회 이상 정기적으로 또는 필요한 시점에 위험평가를 수행하고 있는가?

연 1회 이상 정기적 또는 필요 시점에 따라 점검

① 사전에 수립된 위험관리 방법 및 계획에 따라 체계적으로 수행

1. 위험평가는 연 1회 이상 정기적으로 수행하되 조직의 변화, 신규 시스템 도입 등 중요한 사유가 발생한 경우 해당 부분에 대하여 정기적인 위험평가 이외에 별도로 위험평가 수행
2. 서비스 및 정보자산의 현황과 흐름분석 결과 반영
3. 최신 법규를 기반으로 정보보호 및 개인정보보호 관련 법적 요구사항 준수 여부 확인
4. 정보보호 및 개인정보보호 관리체계 인증기준의 준수 여부 확인
5. 기 적용된 정보보호 및 개인정보보호 대책의 실효성 검토 포함

00년 위험관리결과보고서

순번	내용
1	위험평가 방법선정
2	위험도 산정
3	DOA(Degree of Assurance)
4	위험처리 전략 결정
5	수행결과

구분	직위	성명	일자	서명
승인	정보보호 최고책임자	OOO	2023-01-01	승인
상신	정보보호 담당자	OOO	2022-12-20	-

※ 연 1회 위험평가 실시 (이해를 돕기 위한 예시)

◇ 조직에서 수용 가능한 목표 위험수준을 정하고, 그 수준을 초과하는 위험을 식별하고 있는가?

(예시) 위험도 산정기준 마련

「**위험평가 관리지침**」 제 ○○조 (위험도 산정 기준)

① 위험도는 발생가능성과 영향도를 고려하여 산정한다.

구분	점 수	상세 내역
발생 가능성	1 (하)	• 서비스 운영기간 (1년) 동안 1회 발생
	2 (중)	• 서비스 운영기간 (1년) 동안 2회 – 5회 발생
	3 (상)	• 서비스 운영기간 (1년) 동안 5회 이상
영향도	1 (하)	• 자산 손실 : 미묘한 소실 • 서비스 중단 : 4시간 이하 서비스 중단 • 법적 책임 : 처벌 없음 • 재정 피해 : 운영예산 5% 이하 재산피해 • 인명 사고 : 신체적 상처 없음
	2 (중)	• 자산 손실 : 자산 피해발생 • 서비스 중단 : 1일 – 1주 이하 서비스 중단 • 법적 책임 : 시정 명령 또는 과태료 • 재정 피해 : 운영예산 25% 이하 재산피해 • 인명 사고 : 상해 발생
	3 (상)	• 자산 손실 : 자산 심각한 피해발생 • 서비스 중단 : 1주 이상 서비스 중단 • 법적 책임 : 과징금 또는 벌금 • 재정 피해 : 운영예산 25% 이상 재산피해 • 인명 사고 : 사망사고 발생

위험 수준 산정 기준

위험도 = 발생 가능성 * 영향도

영향도 \ 자산 등급	1 (하)	2 (중)	3 (상)
1 (하)	1 (하)	2 (하)	3 (중)
2 (중)	2 (하)	4 (중)	6 (상)
3 (상)	3 (중)	6 (상)	9 (상)

※ 위험도 기준 마련 (이해를 돕기 위한 예시)

(예시) 위험수준(DoA) 산정 및 관리

「**위험평가 관리지침**」 제 ○○조 (위험 관리 절차)

① 정보보호 최고책임자는 위험평가 결과를 바탕으로 위험 수용 수준(DoA)을 정보보호실무협의회의 검토 후 정보보호위원회에 상정한다

1. 범위 및 환경에 따라 정보보호 최고책임자가 판단하여 정보보호실무협의회에서 위험 별 대책을 결정할 수 있다.

② 정보보호 관리자는 위험 수용 수준(DoA) 및 식별된 관리대상 위험을 바탕으로 위험관리 목표를 정한다.

③ 정보보호 관리자는 도출된 위험관리 목표에 따라 위험관리 방법 및 단계별 위험관리 방안을 작성하여 정보보호 최고책임자에게 보고하고, 정보보호 최고책임자는 정보보호실무협의회에서 심의하도록 한다.

④ 정보보호실무협의회는 위험평가 결과 도출된 노출 위험에 대하여 해당 위험을 어떻게 다룰 것인지(회피, 전이, 감소, 수용 중) 심의한다. 위험관리 방법의 결정시 다음 각

호를 따른다.

1. 위험을 회피, 전이, 감소시키는 것으로 결정된 위험은 위험관리의 구체적인 방법 도출
2. 수용하는 것으로 결정된 위험은 합당한 사유 명시 필요
3. 위험관리 방법은 위험관리 목표를 달성할 수 있는 수준으로 결정

수립 단계에서는 우선 위험을 허용 가능한 위험수준(DoA) 이하로 감소시키기 위해 필요한 정보보호 대책을 선택하고, 이 중 유사한 대책들은 필요 시 하나의 이행과제로 묶는다.

위험수준(DoA) 산정 시 고려사항

① 설정 원칙

1. 자원 제약 고려: 인력, 시간, 비용 등을 종합적으로 고려하여 DoA 결정
2. 업무 효율성: 정보보호 목표를 충족하면서도 업무 수행 효율성을 저해하지 않는 수준
3. 법적 요구사항: ISMS 인증기준 및 관련 법규를 대부분 이행할 수 있도록 DoA 결정
4. 경영진 승인: 정보보호 최고책임자 등 경영진의 의사결정에 의한 승인

② 주의사항

1. 과도한 DoA 설정 금지: 타당한 사유 없이 과도하게 높게 설정하여 실질적 대응이 필요한 위험을 방치하는 것은 부적절
2. 법적 위험 배제: 법률 위반에 해당하는 위험은 수용 가능한 위험에 포함할 수 없음
3. 객관적 근거: 위험수용 결정 시 명확하고 객관적인 근거에 기반해야 함

위험수준(DoA) 별 대책

① **수용불가**: 위험도가 수용불가능 단계이면 문제점이 개선되지 않는 한 운영이 즉시 중단되어야 한다. 실제로 위험이 발생하면 심각도나 발생가능성을 감소시키기 위해 위험 경감이 필요하다. 일반적으로 사건발생의 가능성을 줄이는 것을 심각도보다 먼저 고려한다.

② **수용**: 위험도가 수용 단계이면, 사건발생의 심각도나 가능성을 검토하여 위험을 "현실적으로 타당한 최저수준"으로 경감하기 위한 수단을 강구해야 한다. 잔여 위험은 비용 등을 고려하여 효과적으로 적용하고 정보보호 책임자의 승인하에 수용 가능하게 한다.

③ **허용** : 위험이 허용 가능하면 위험 가능성이 없거나 또는 우려할 만큼 심각하지 않다는 것을 의미하나, 위험을 더 감소시키기 위한 검토가 지속적으로 이루어져야 한다.

위험도 및 조치수준

위험도			위험조치수준
심각	수용불가	6 ~ 9 (상)	• 문제점 개선되지 않으면 운영중단
주의	수용	3 ~ 4 (중)	• 위험경감조치를 통한 수용 가능
경미	허용가능	1 ~ 2 (하)	• 별다른 조치없이 운영하나 지속적 관리

※ 위험도 및 조치수준 선정 예시 (이해를 돕기 위한 예시)

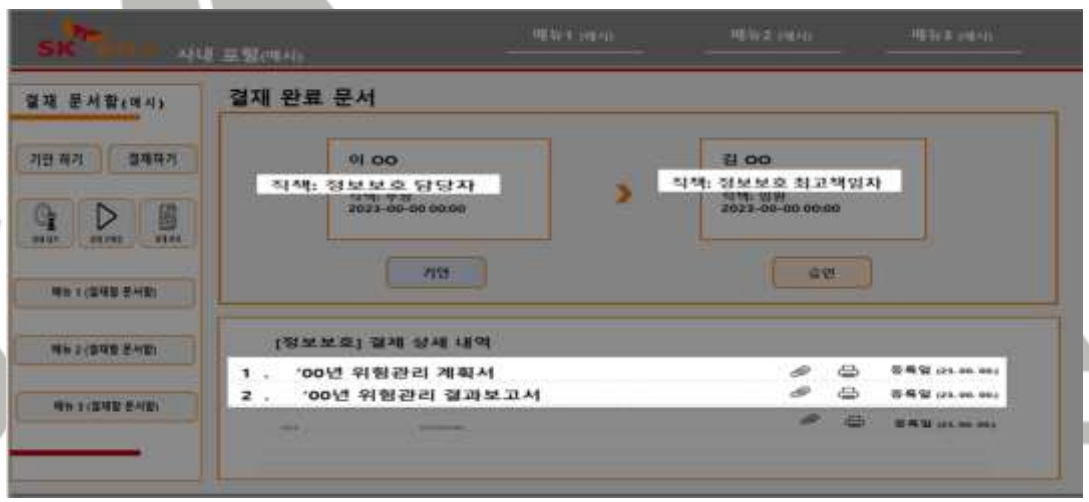
◇ 위험식별 및 평가 결과를 경영진에게 보고하고 있는가?

위험식별 및 평가 결과 보고

① 식별된 위험에 대한 평가보고서 작성

② 식별된 위험별로 관련된 이해관계자에게 내용 공유 및 논의

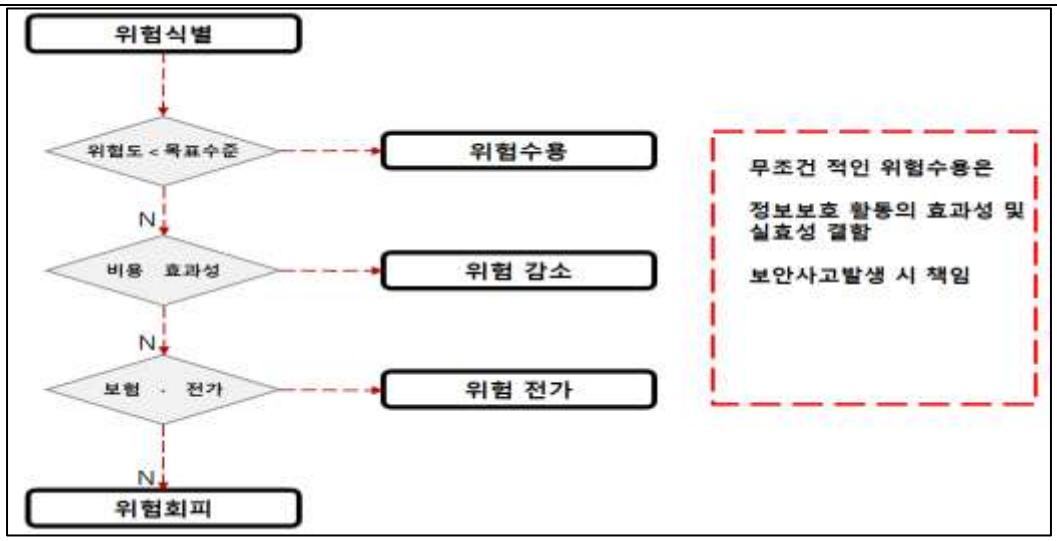
③ IT, 법률적 전문 용어보다는 경영진의 눈높이에서 쉽게 이해하고 의사 결정할 수 있도록 보고서를 작성하여 보고



※ 경영진 보고 승인 (이해를 돕기 위한 예시)

1.2.4 보호 대책 선정

세부분야	1.2.4 보호 대책 선정
인증 기준	위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 조직에 적합한 보호 대책을 선정하고, 보호 대책의 우선순위와 일정·담당자·예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.
주요 확인사항	• 식별된 위험에 대한 처리 전략(감소, 회피, 전가, 수용 등)을 수립하고 위험처리를 위한 보호 대책을 선정하고 있는가? • 보호 대책의 우선순위를 고려하여 일정, 담당부서 및 담당자, 예산 등의 항목을 포함한 보호 대책 이행계획을 수립하고 경영진에 보고하고 있는가?
기준 요약도	
운영 방안	**◇ 식별된 위험에 대한 처리 전략(감소, 회피, 전가, 수용 등)을 수립하고 위험처리를 위한 보호 대책을 선정하고 있는가?** **위험 처리 전략 수립** ① 수용 가능한 목표 위험수준과 비교(목표 위험수준과 같거나 이하일 경우 수용) ② 목표 위험보다 높을 경우 목표 위험수준까지 감소시킬 대책 구현 절차 수립 ③ 대책 구현 및 유지에 대한 비용과 감소되는 위험을 비교하여 가치평가 ④ 대책 구현으로 목표 위험수준 이하로 감소될 경우 대책 선정



※ 위험처리 기준 (이해를 돕기 위한 예시)

◇ 보호 대책의 우선순위를 고려하여 일정, 담당부서 및 담당자, 예산 등의 항목을 포함한 보호 대책 이행계획을 수립하고 경영진에 보고하고 있는가?

보호 대책 구현을 위한 우선 순위 결정

① 위험의 심각성 및 시급성, 구현의 용이성, 예산 할당, 자원의 가용성, 선후행 관계 등을 고려하여 우선순위 결정

1. 즉시 교정 가능한 취약점 제거
2. 정책 및 절차 수립 및 변경
3. 시스템 도입 등의 예산이 필요한 정보보안 세부 업무 계획 수립

정보보호 대책 이행계획서

정보보호 관리자	정보보호 책임자

위험ID	위험명	처리전략	보호대책	우선순위	담당부서	담당자	시작일	완료일	예산(천원)	비고
R001	관리자 계정 취약성	감소	계정 잠금 임계값 설정	높음	IT보안팀	김보안	2025.09.15	2025.10.15	2000	즉시 적용
R002	개인정보 유출 위험	전가	사이버보험 가입	중간	경영지원팀	최관리	2025.10.01	2025.11.30	5000	연간 보험료
R003	웹사이트 보안 취약	회피	회원가입 기능 제거	낮음	웹서비스팀	박웹	2025.11.01	2025.12.01	3000	시스템 개선

※ 정보보호 대책 이행계획서 (이해를 돕기 위한 예시)

1.3 관리체계 운영

1.3.1 보호 대책 구현

세부분야	1.3.1 보호 대책 구현
인증 기준	선정한 보호 대책은 이행계획에 따라 효과적으로 구현하고, 경영진은 이행결과의 정확성과 효과성 여부를 확인하여야 한다.
주요 확인사항	• 이행계획에 따라 보호 대책을 효과적으로 구현하고 이행결과의 정확성 및 효과성 여부를 경영진이 확인할 수 있도록 보고하고 있는가? • 관리체계 인증기준별로 보호 대책 구현 및 운영 현황을 기록한 운영명세서를 구체적으로 작성하고 있는가?
기준 요약도	
운영 방안	**◇ 이행계획에 따라 보호 대책을 효과적으로 구현하고 이행결과의 정확성 및 효과성 여부를 경영진이 확인할 수 있도록 보고하고 있는가?** **보호 대책 이행 계획 수립 및 경영진 보고** ① 보호 대책 구현, 이행 성과 경영진 보고

00년 정보보호 및 개인정보보호 이행계획 경과보고

구분	직위	성명	일자	서명
승인	정보보호 최고책임자	OOO	2023-01-01	승인
상신	정보보호 담당자	OOO	2022-12-20	-

※ 출처: 이행성과 보고 (이해를 돕기 위한 예시)

과제별 보호대책

과제	• IT 위탁사 보안관리 체계 도입			
목적	• IT 위탁사 중요 정보 및 개인정보에 대한 외부유출 방지 • 위탁사 정보보호 관리실태 점검 실시			
추진목표	• IT 위탁사 정보보호 관리 현황 파악 및 DOA(수용가능 위험) 조과 취약점 관리			
세부 단계	순서	추진단계	주요내용	예상소요시간
	1	요구 사항 분석	IT 위탁사 정보보호 관리실태 점검 계획 수립	2 주
	2	점검 조직 구성	외부 보안 협력업체 점검	2개월
	3	보안 위협 조치	도출 취약점 보완 조치 및 관리대책 수립	1개월
	4	이행 점검	도출 취약점 효과성 확인	1개월
기대 효과	• IT 위탁사 보안사고 사전 예방 및 보안인식 강화			

※ 과제별 구체적 보호 대책 수립 (이해를 돕기 위한 예시)

◇ 관리체계 인증기준별로 보호 대책 구현 및 운영 현황을 기록한 운영명세서를 구체적으로 작성하고 있는가?

보호 대책 및 운영 현황 운영명세서 기록 작성

① 보호 대책 구현 현황 운영명세서 작성

1. 모호한 표현보다는 구체적이고 측정 가능한 표현을 사용하여 명확히 이해할 수 있도록 작성
2. 인증기준의 모든 요구사항이 어떻게 이행되고 있는지 누락 없이 기술
3. 관련 문서와 기록 간 내용의 일관성을 유지하여 혼선을 방지
4. 실제 운영 상황과 완전히 일치하는 내용만을 작성

※ 작성 시 한국인터넷진흥원(isms.kisa.or.kr)의 '정보보호 및 개인정보보호 관리체계 인증 신청서 양식' 참고

ISMS 인증 운영명세서 (기업명: SK 쉴더스)

※ ISMS 인증 운영명세서 (이해를 돕기 위한 예시)

1.3.2 보호 대책 공유

세부분야	1.3.2 보호 대책 공유
인증기준	보호 대책의 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여 지속적으로 운영되도록 하여야 한다.
주요 확인사항	• 구현된 보호 대책을 운영 또는 시행할 부서 및 담당자를 명확하게 파악하고 있는가? • 구현된 보호 대책을 운영 또는 시행할 부서 및 담당자에게 관련 내용을 공유 또는 교육하고 있는가?
기준 요약도	
운영 방안	**◇ 구현된 보호 대책을 운영 또는 시행할 부서 및 담당자를 명확하게 파악하고 있는가?** **부서 및 담당자 현황 관리** **「정보자산 관리지침」**제 ○○조 (정보자산 등록) ① 자산 등록·변경·삭제는 정보 소유자가 필요 시 부서 정보보호 책임자의 허가를 득하고 부서 자산목록에 직접 등록한다. ② 부서 정보보호 책임자는 등록된 자산의 보안 등급에 따라 자산코드를 부여하여야 한다. ③ 정보보호담당자는 분기별 각 부서의 자산목록을 검토, 취합, 현행화한다. ④ 정보보호담당자는 연 1회 이상 자산현황을 실사하여야 하며, 그 결과를 정보보호 최고책임자에게 보고해야 한다.


정보자산 관리대장

※ 정보자산 관리대장 (이해를 돕기 위한 예시)

◇ 구현된 보호 대책을 운영 또는 시행할 부서 및 담당자에게 관련 내용을 공유 또는 교육하고 있는가?

(예시) 보호대책 공유 또는 교육

① 공지 방법

1. 이메일 공지 : 전사 또는 특정 부서 대상 정책 변경 안내 메일
2. 사내 게시판/포털 공지 : 정보보호 정책 제·개정 안내, 보안 캠페인 공지 게시글
3. 그룹웨어/메신저 공지 : 긴급 보안 공지, 보안 업데이트 안내 메시지

② 주요 확인 내용

1. 공유 시점 : 정책 시행 전 충분한 시간을 두고 공유되었는지
2. 공유 대상 : 해당 정책의 영향을 받는 모든 임직원에게 전파되었는지
3. 내용 : 변경된 정책의 핵심 내용, 시행일, 담당 부서가 명확히 기재되었는지
4. 수신 확인(가능한 경우) : 수신 확인 여부나 조회수 등 전파 범위를 증빙
5. 기타 증빙 : 게시판, 이메일, 회의록, 교육이력 등

1.3.3 운영현황 관리

세부분야	1.3.3 운영현황 관리
인증 기준	조직이 수립한 관리체계에 따라 상시적 또는 주기적으로 수행하여야 하는 운영활동 및 수행 내역은 식별 및 추적이 가능하도록 기록하여 관리하고, 경영진은 주기적으로 운영활동의 효과성을 확인하여 관리하여야 한다.
주요 확인사항	• 관리체계 운영을 위하여 주기적 또는 상시적으로 수행하여야 하는 정보보호 및 개인정보보호 활동을 문서화하여 관리하고 있는가? • 경영진은 주기적으로 관리체계 운영활동의 효과성을 확인하고 이를 관리하고 있는가?
기준 요약도	
운영 방안	**◇ 관리체계 운영을 위하여 주기적 또는 상시적으로 수행하여야 하는 정보보호 및 개인정보보호 활동을 문서화하여 관리하고 있는가?** **정보보호 및 개인정보보호 활동 작성** 「**정보보호 운영지침**」 제 ○○조 (운영현황 관리) ① 정보보호 관리체계의 효과적인 운영을 위하여 주기적 또는 상시적으로 수행하여야 하는 정보보호 활동을 운영현황표로 작성하여 관리하여야 한다. ② 운영현황표에는 다음 각 호의 사항을 포함하여야 한다. 1. 정보보호 활동의 구분 및 세부 항목 2. 수행 주기 (일일, 주간, 월간, 분기, 반기, 연간 등) 3. 수행 주체 (담당부서 및 담당자)

4. 확인 및 승인자

5. 관련 문서 및 기록

③ 각 부서의 장은 소관 업무와 관련된 정보보호 활동의 수행 현황을 매월 점검하고, 그 결과를 정보보호 담당부서에 보고하여야 한다.

④ 정보보호 담당부서는 전사 운영현황을 취합·분석하여 분기별로 정보보호 최고책임자에게 보고하여야 한다.

정보보호 관리체계 운영현황표

구분	정보보호관리체계 기준	산출물	담당자	점검자	수행주기	12월	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	진행률	비고
정보보호 정책	1.1.1 정보보호정책승인	정책 승인 증적 - 정책지침 제개정(안)	· 정보보호관리자	· 정보보호관리자 정보보호책임자	년 1회 이상						1							100%	
	1.1.2 정책공표	정책배포 증적 - 전자우편 게시판	· 정보보호관리자	·	제개정시						1							-	
—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
정보자산 보호대책	2.1.3 정보자산 관리	자산관리대장 현행화	· 정보보호관리자	·	분 2회 이상			1										50%	
업무 연속성관리	2.11.4 사고대응훈련	모의훈련 결과보고서	· 정보보호관리자	· 정보보호관리자 · 정보보호책임자	분 1회 이상													0%	
—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—

※ 정보보호 관리체계 운영현황표 (이해를 돕기 위한 예시)

정보보호 및 개인정보보호 활동 이해를 돕기 위한 예시

① 연간계획 및 주기적 활동 계획을 작성하여 연간 운영현황표로 작성 관리

구분	업무 내용	주기 및 시기	보안 적용 실적	책임자
정보자산분류	정보자산 대장 관리	연 1회	- 정보 자산 등급 현행화 - 정보자산 별 라벨링	정보보호최고책임자
인적보안	보안서약서 관리	상시	- 중요정보 취급자 보안서약서 징구	정보보호담당자
운영관리	통제 구역 출입대장관리	상시	- IDC 출입관리 검토	물리보안담당자
	사무실보안점검	상시	- 사무실 업무환경 점검	정보보호담당자
업무연속성	복구테스트 모의훈련	연 1회	- 업무연속성 모의훈련 - 데이터 복구 모의훈련	정보보호담당자
접근통제	사용자 계정관리	분기 1회	- 정보시스템별 계정신청서 - 계정발급현황	정보시스템담당자
	사용자 권한 검토	분기 1회	- 계정별 권한 검토 및 현행화	정보시스템담당자
운영관리	백업관리	주 1회	- 주간백업 현황 관리 - 소산백업 현황 관리	정보시스템담당자
	보안성검토	상시	- 신규시스템 및 변경시스템 보안성 검토	정보보호담당자
	사이버보안진단의날	월 1회	- 백신 최신패치, 현황, PC상태 등	정보보호최고책임자
...	...	...	...	...

※ 정보보호 관리체계 주기적 활동 문서화 (이해를 돕기 위한 예시)

◇ 경영진은 주기적으로 관리체계 운영활동의 효과성을 확인하고 이를 관리하고 있는가?

주기적인 업무 효과성 확인

① 관리체계 운영활동이 운영현황표에 따라 주기적·상시적으로 이루어지고 있는지 정기적으로 확인하여 경영진에게 보고

② 경영진은 관리체계 운영활동의 효과성을 평가하여 필요시 개선 조치(수행주체 변경, 수행 주기 조정, 운영활동의 추가·변경·삭제 등)

※ 정보보호 관리체계 운영 효과성 검토 (이해를 돕기 위한 예시)

1.4 관리체계 점검 및 개선

1.4.1 법적 요구사항 준수 검토

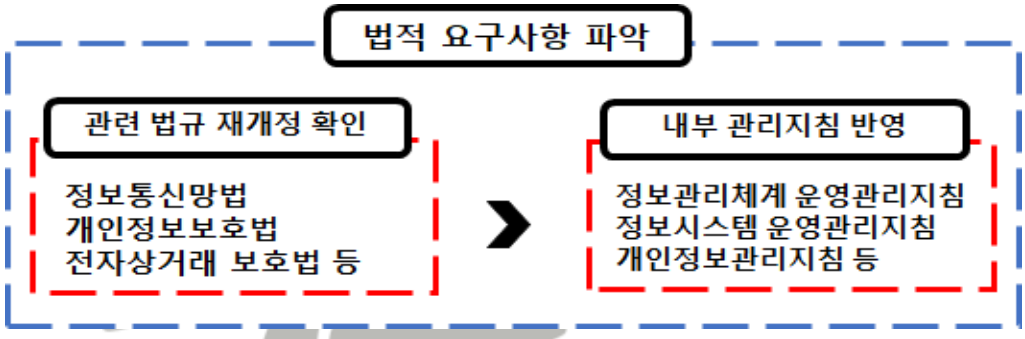
세부분야	1.4.1 법적 요구사항 준수 검토
인증 기준	조직이 준수하여야 할 정보보호 및 개인정보보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토하여야 한다.
주요 확인사항	• 조직이 준수하여야 하는 정보보호 및 개인정보보호 관련 법적 요구사항을 파악하여 최신성을 유지하고 있는가? • 법적 요구사항의 준수 여부를 연 1회 이상 정기적으로 검토하고 있는가?
기준 요약도	
운영 방안	**◇ 조직이 준수하여야 하는 정보보호 및 개인정보보호 관련 법적 요구사항을 파악하여 최신성을 유지하고 있는가?** **(예시) 지침 내 법적 요구사항 파악 및 최신성유지 내용 반영** 「**정보보호 운영지침**」 제 ○○조 (정보보호 정책 검토) ① 정보보호 및 개인정보보호 관리체계 운영에 필요한 법적 요구사항을 명확히 식별하고, 관련 법령의 제·개정사항을 지속적으로 모니터링하여 최신성을 유지하여야 한다. ② 법적 요구사항 준수 검토는 연 1회 이상 실시하여야 하며, 다음 각 호의 사항을 포함하여야 한다.

1. 현행 법적 요구사항 준수 현황 점검
2. 미준수 사항 식별 및 원인 분석
3. 개선계획 수립 및 이행
4. 법적 요구사항 변경에 따른 추가 조치사항 검토

③ 법적 요구사항 준수 검토 결과는 정보보호최고책임자 및 개인정보보호책임자에게 보고하고, 필요시 경영진 승인을 받아 개선조치를 실시하여야 한다.

④ 법적 요구사항을 위반하거나 위반 우려가 있는 경우, 즉시 관련 부서에 통보하고 시정조치를 실시하여야 한다.

⑤ 법적 요구사항에 변경이 발생한 경우, 그 내용을 즉시 분석하여 조직의 정보보호 정책 및 절차에 미치는 영향을 평가하고 필요한 개선조치를 실시하여야 한다.



※ 법적 요구사항 파악 (이해를 돕기 위한 예시)

2025년 기준 법적 요구사항 주요 개정내용(2024년 대비 변경사항)

「**개인정보보호법**」[시행 2025. 10. 2.] 기준

① 국내대리인의 지정

1. 국내에 주소 또는 영업소가 없는 개인정보처리자가 국내대리인을 지정하는 경우
- 국내 법인을 설립하여 운영하고 있는 등 일정 요건을 갖춘 경우에는 해당 국내 법인을 우선 지정
- 지정한 국내대리인에 대한 관리·감독 의무를 부여하며, 위반 시 과태료 부과

「**개인정보보호법 시행령**」[시행 2025. 10. 2.] 기준

① 개인정보 전송요구권 도입

1. 정보주체가 본인의 개인정보를 직접 다운로드하거나 다른 서비스 제공자에게 전송 요구 가능
2. 보건의료 등 의료정보, 통신 이용 이력 등 통신정보, (2026년 예정)에너지 사용량 등 에너지정보 대상
3. 데이터 이동성 보장 및 서비스 간 경쟁 촉진

② 이동형 영상정보처리기기 규제 신설

1. 드론, 로봇, 차량 등 이동형 기기의 영상 수집 규제
2. 공공장소에서 촬영 시 정보주체가 촬영 사실과 목적을 알 수 있도록 조치 의무

③ 온·오프라인 규제 통합

1. 온라인과 오프라인 개인정보 처리에 대한 통합적 규제 체계 구축

④ 자동화된 결정에 대한 정보주체 권리 강화

1. AI 등 자동화된 결정에 대한 정보주체의 알 권리 및 거부권 신설

⑤ 개인정보관리 전문기관의 본인전송정보 관리·분석 업무 규정

1. 개인정보관리 전문기관의 본인전송정보에 대한 관리·분석 업무를 규정
2. 정보주체의 필요에 따라 안전성 및 신뢰성이 검증된 개인정보관리 전문기관을 통하여 관리할 수 있도록 규정

「**정보통신망법 시행령**」[시행 2025. 5. 20.] 기준

① 연계정보 생성·처리 관련 규정 신설 및 강화

1. 연계정보 생성·처리 승인 대상 서비스 범위 구체화
2. 모바일 전자고지 서비스와 금융 마이데이터 서비스를 연계정보 생성·처리 승인 대상 서비스로 규정
3. 기존 한시적 허용에서 상시적·안정적 서비스 제공 가능하도록 개선

② 본인확인기관의 물리적·기술적·관리적 조치 신설

1. 연계정보 생성·처리의 안전성 확보를 위한 조치 의무화
2. 연계정보 생성 소프트웨어에 대한 보안 통제
3. 연계정보의 위조·변조 방지 조치
4. 연계정보 생성·처리 사실 확인자료의 기록·보관

③ 연계정보 이용기관의 안전조치 강화

1. 연계정보와 주민등록번호의 분리·보관·관리 의무
2. 안전한 암호화 기술 적용
3. 침해사고 발생 시 대응 계획 수립 및 시행

④ 불법정보 유통방지를 위한 조치 강화

1. 콘텐츠 전송 네트워크(CDN) 사업자 규제 신설
2. 정보통신서비스 부문 매출액 10억원 이상인 CDN 사업자를 불법정보 유통방지의무 대상으로 지정
3. 기술적·관리적 조치 업무 담당자 지정 의무
4. 불법정보 유통 신고 접수 시 방송통신심의위원회 통보 의무
5. 불법정보 유통금지 규정을 이용약관 또는 계약서류에 명시 의무

「**전자금융감독규정**」[시행 2025. 2. 5.] 기준

	① 규제 체계 변경 1. 수범사항 대폭 축소 및 합리화 - 기존 293개의 세세한 행위규칙(Rule)을 166개로 정비 - 미시적이고 세부적인 사항 삭제 - 이용자 보호 관련 내용 강화 - 금융보안 핵심사항 현행 유지 - 기타 규정 조정·합리화 2. 자율성 확대 - 건물·설비·전산실 관리, 각종 내부통제·사업운영 등에서 금융회사 자율성 대폭 확대 - 형식적인 수범사항 준수에서 벗어나 실질적인 보안체계 구축으로 유도 ② 보안 거버넌스 강화 1. 정보보호최고책임자(CISO)가 정보보호위원회의 주요 심의·의결사항을 이사회에 보고 의무화 2. 전사적 차원의 보안 역량 강화 유도. 2025년 8월 5일부터 적용 (6개월 유예) ③ 재해복구센터 구축 의무 확대 1. 설치 의무 대상 확대 - 기존 은행, 금융투자업자, 보험회사 외에 다음 기관으로 확대: - 여신전문금융회사: 총자산 2조원 이상 + 상시종업원 300명 이상 - 전자금융업자: 연간 총거래액 2조원 이상 - 총자산 2조원 이상: 시설대여업자, 할부금융업자, 신기술사업금융업자 - 자체 전산시스템 구축: 상호저축은행 - 시행일: 2026년 2월 5일부터 적용 (1년 유예) ④ 전자금융사고 책임이행보험 한도 상향 1. 보상한도 상향 - 자산 2조원 이상 금융투자업자: 5억원 → 10억원 - 여신전문금융회사·보험회사·저축은행: 1억원 → 2억원 - 선불전자금융업자·PG업자 등: 1억원 → 2억원 - 시행일: 2026년 2월 5일부터 적용 (1년 유예) ⑤ 클라우드 컴퓨팅 서비스 이용 기준 개선 1. 이용 절차 구체화 - 기존 클라우드 계약을 통한 신규 업무 처리 시에도 금융감독원 보고 의무 신설 - 업무 연속성 계획 관련 운영 매뉴얼, 유지보수 관리대장, 책임자 명부 작성·보관 의무 추가 - 클라우드 환경에서 물리적 망분리 예외 인정 (VPN 이용 가능)

※ 상기 법률·법령·행정규칙 등 기업이 준수해야 할 최신 법적요구사항과 해당 내용의 준수여부를 검토하여야 함

◇ 법적 요구사항의 준수 여부를 연 1회 이상 정기적으로 검토하고 있는가?

법적 요구사항의 준수 여부 주기적 검토

「**정보보호 운영지침**」 제 ○○조 (정보보호 정책 검토)

① 정보보호 및 개인정보보호 관리체계 운영에 필요한 법적 요구사항을 명확히 식별하고, 관련 법령의 제·개정사항을 지속적으로 모니터링하여 최신성을 유지하여야 한다.

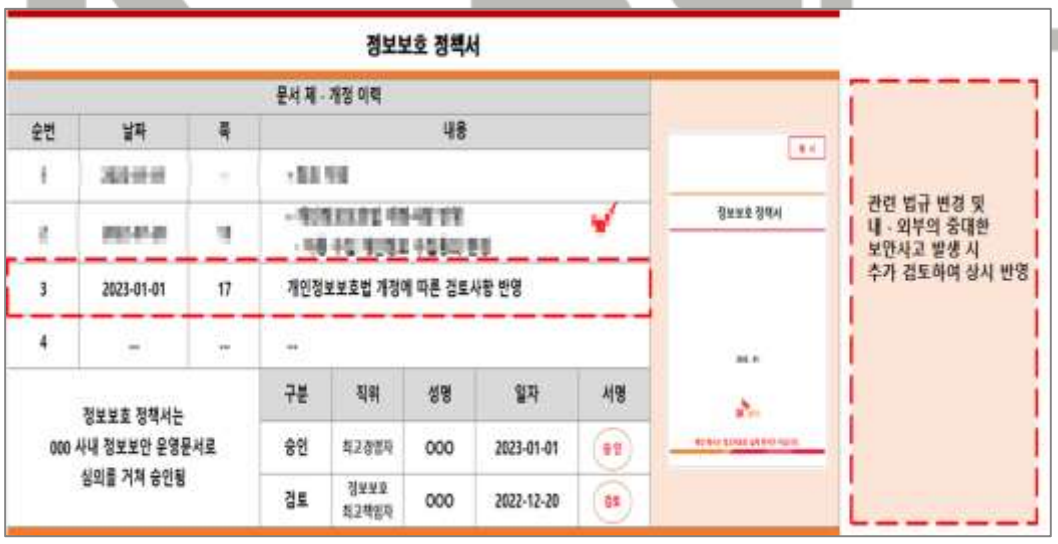
② 법적 요구사항 준수 검토는 연 1회 이상 실시하여야 하며, 다음 각 호의 사항을 포함하여야 한다.

1. 현행 법적 요구사항 준수 현황 점검
2. 미준수 사항 식별 및 원인 분석
3. 개선계획 수립 및 이행
4. 법적 요구사항 변경에 따른 추가 조치사항 검토

③ 법적 요구사항 준수 검토 결과는 정보보호최고책임자 및 개인정보보호책임자에게 보고하고, 필요시 경영진 승인을 받아 개선조치를 실시하여야 한다.

④ 법적 요구사항을 위반하거나 위반 우려가 있는 경우, 즉시 관련 부서에 통보하고 시정조치를 실시하여야 한다.

⑤ 법적 요구사항에 변경이 발생한 경우, 그 내용을 즉시 분석하여 조직의 정보보호 정책 및 절차에 미치는 영향을 평가하고 필요한 개선조치를 실시하여야 한다.



※ 주기적 검토내용 반영 (이해를 돕기 위한 예시)

1.4.2 관리체계 점검

세부분야	1.4.2 관리체계 점검
인증 기준	관리체계가 내부 정책 및 법적 요구사항에 따라 효과적으로 운영되고 있는지 독립성과 전문성이 확보된 인력을 구성하여 연 1회 이상 점검하고, 발견된 문제점을 경영진에게 보고하여야 한다.
주요 확인사항	• 법적 요구사항 및 수립된 정책에 따라 정보보호 및 개인정보보호 관리체계가 효과적으로 운영되는지를 점검하기 위한 관리체계 점검기준, 범위, 주기, 점검인력 자격요건 등을 포함한 관리체계 점검 계획을 수립하고 있는가? • 관리체계 점검 계획에 따라 독립성, 객관성 및 전문성이 확보된 인력을 구성하여 연 1회 이상 점검을 수행하고 발견된 문제점을 경영진에게 보고하고 있는가?
기준 요약도	
운영 방안	**◇ 법적 요구사항 및 수립된 정책에 따라 정보보호 및 개인정보보호 관리체계가 효과적으로 운영되는지를 점검하기 위한 관리체계 점검기준, 범위, 주기, 점검인력 자격요건 등을 포함한 관리체계 점검 계획을 수립하고 있는가?** **관리체계 점검 계획 수립** 「**정보보호 운영지침**」 제 ○○조 (보안관리실태점검) ① 정보보호 책임자는 자체 보안 관리실태 점검을 연 1회 이상 실시하여야 하며, 각 분야의 점검항목은 '정보보호 관리실태 점검항목'을 기준으로 한다. 1. 점검기준: 정보보호 및 개인정보보호 관리체계 인증기준 포함 2. 점검범위: 전사 또는 인증범위 포함 3. 점검주기: 최소 연 1회 이상 수행 필요 4. 점검인력 자격요건: 점검의 객관성, 독립성 및 전문성을 확보

'00년 정보보호관리실태 점검 계획서

순번	내용			
1	점검 목적			
2	관리실태 점검 사항			
3	관리실태 점검기간 및 장소			
4	관리실태 점검 구성원			
5	추진 일정			
구분	직위	성명	일자	서명
승인	정보보호 최고책임자	OOO	2023-01-01	승인
상신	정보보호 담당자	OOO	2022-12-20	-

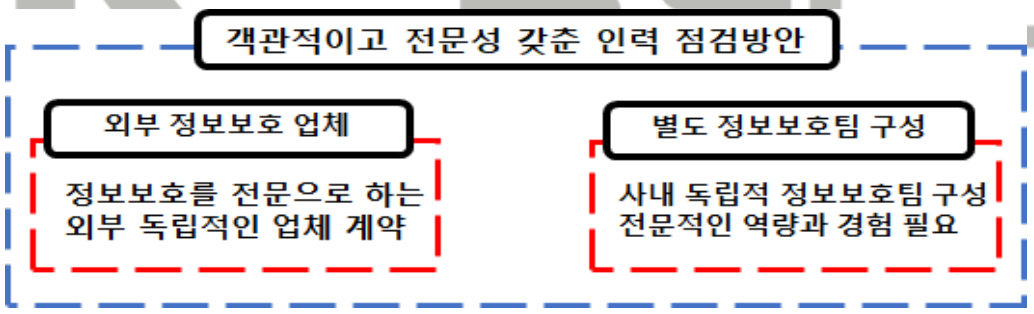
※ 정보보호 관리실태 점검 계획 (이해를 돕기 위한 예시)

◇ 관리체계 점검 계획에 따라 독립성, 객관성 및 전문성이 확보된 인력을 구성하여 연 1회 이상 점검을 수행하고 발견된 문제점을 경영진에게 보고하고 있는가?

객관적이고 독립적인 전문인력 확보 필요

① 정보보호 최고책임자(CISO) 역할

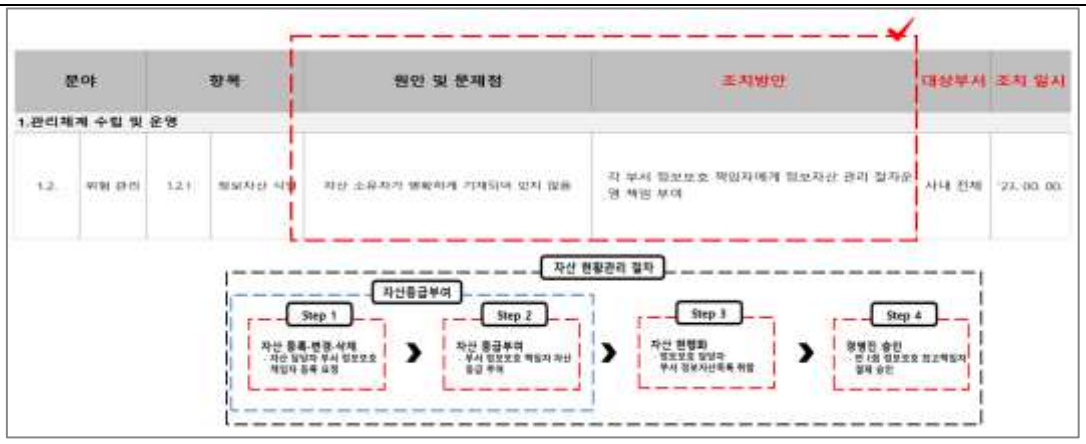
1. 점검의 객관성, 독립성 및 전문성을 확보할 수 있도록 점검조직 구성
2. 점검 계획에 따라 연 1회 이상 점검 수행
3. 점검 결과 발견된 문제점에 대해서는 조치계획을 수립·이행하고, 조치 완료 여부에 대하여 추가 확인
4. 점검 결과보고서를 작성하여 정보보호 최고책임자 및 개인정보보호책임자 등 경영진에게 보고



※ 객관적 전문성 갖춘 인력 확보 (이해를 돕기 위한 예시)

1.4.3 관리체계 개선

세부분야	1.4.3 관리체계 개선
인증 기준	법적 요구사항 준수검토 및 관리체계 점검을 통하여 식별된 관리체계상의 문제점에 대한 원인을 분석하고 재발방지 대책을 수립·이행하여야 하며, 경영진은 개선 결과의 정확성과 효과성 여부를 확인하여야 한다.
주요 확인사항	• 법적 요구사항 준수 검토 및 관리체계 점검을 통하여 식별된 관리체계상의 문제점에 대한 근본 원인을 분석하여 재발방지 및 개선 대책을 수립·이행하고 있는가? • 재발방지 및 개선 결과의 정확성 및 효과성 여부를 확인하기 위한 기준과 절차를 마련하고 있는가?
기준 요약도	
운영 방안	**◇ 법적 요구사항 준수 검토 및 관리체계 점검을 통해 식별된 관리체계 상의 문제점에 대한 근본 원인을 분석하여 재발방지 및 개선 대책을 수립·이행하고 있는가?** **근본원인 분석하여 재발방지 대책 수립 및 이행** ① 식별된 관리체계상의 문제점 및 결함사항에 대한 근본 원인 분석

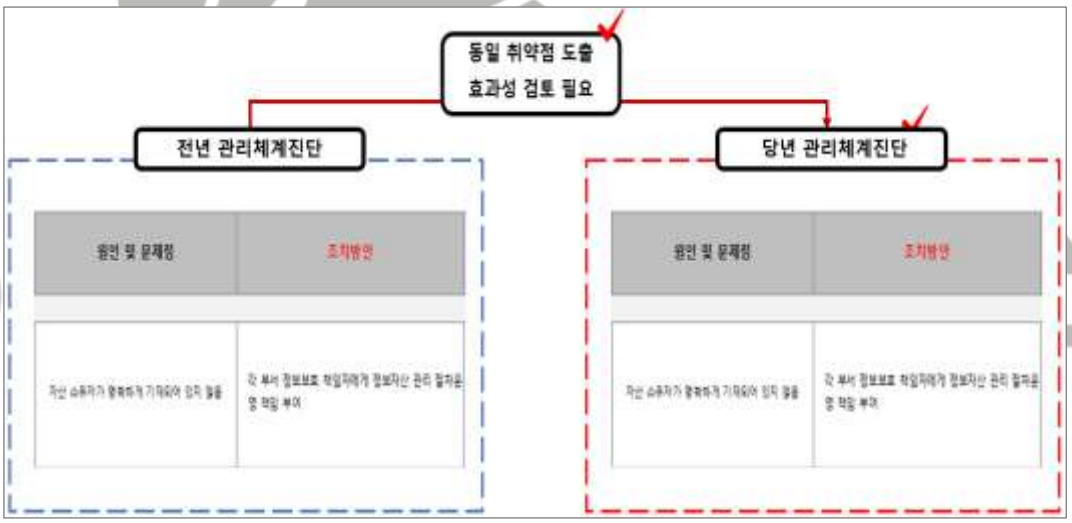


※ 근본원인 분석 및 보안대책 수립 (이해를 돕기 위한 예시)

◇ 재발방지 및 개선 결과의 정확성 및 효과성 여부를 확인하기 위한 기준과 절차를 마련하고 있는가?

재발방지 및 개선 효과성 확인

① 재발방지 및 개선조치의 정확성 및 효과성을 측정하기 위하여 관리체계 측면에서의 핵심성과지표 도출

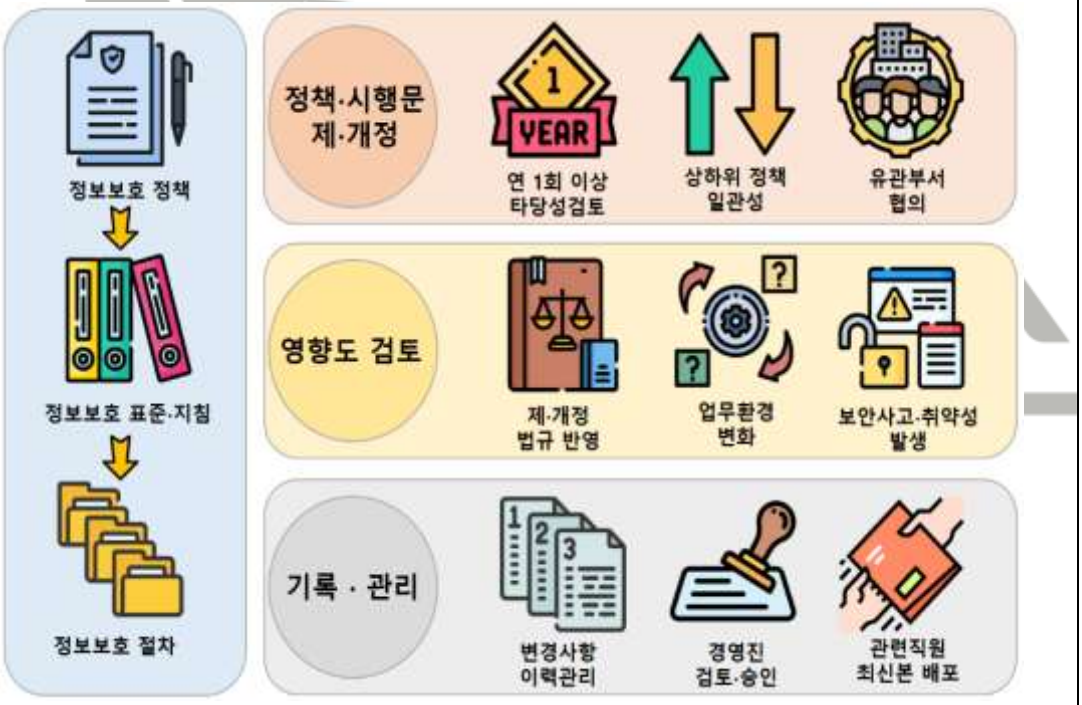


※ 재발방지 효과성 검토 (이해를 돕기 위한 예시)

2. 보호 대책 요구사항

2.1 정책, 조직, 자산 관리

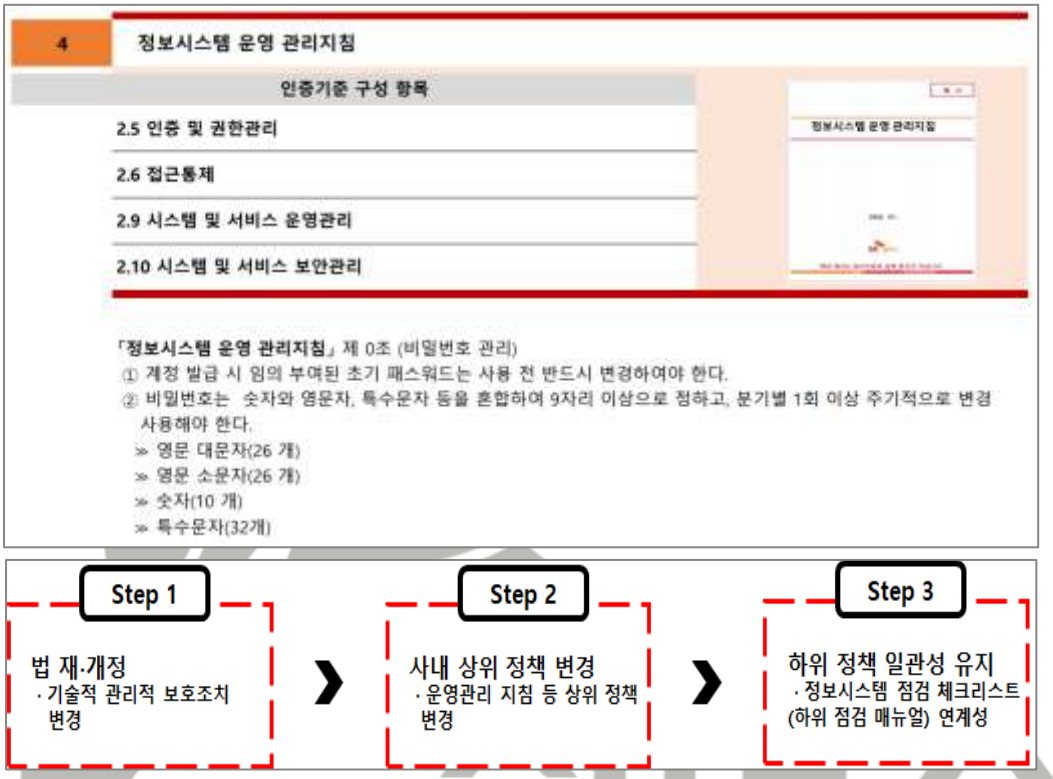
2.1.1 정책의 유지관리

세부분야	2.1.1 정책의 유지관리
인증 기준	정보보호 및 개인정보보호 관련 정책과 시행문서는 법령 및 규제, 상위 조직 및 관련 기관 정책과의 연계성, 조직의 대내외 환경변화 등에 따라 주기적으로 검토하여 필요한 경우 제·개정하고 그 내역을 이력 관리하여야 한다.
주요 확인사항	• 정보보호 및 개인정보보호 관련 정책 및 시행문서에 대한 정기적인 타당성 검토 절차를 수립·이행하고 있는가? • 조직의 대내외 환경에 중대한 변화 발생 시 정보보호 및 개인정보보호 관련 정책 및 시행문서에 미치는 영향을 검토하고 필요시 제·개정하고 있는가? • 정보보호 및 개인정보보호 관련 정책 및 시행문서의 제·개정 시 이해관계자의 검토를 받고 있는가? • 정보보호 및 개인정보보호 관련 정책 및 시행문서의 제·개정 내역에 대하여 이력 관리를 하고 있는가?
기준 요약도	
운영 방안	**◇ 정보보호 및 개인정보보호 관련 정책 및 시행문서에 대한 정기적인 타당성 검토 절차를 수립·이행하고 있는가?** **법적 요구사항의 준수 여부를 정기적으로 검토할 수 있는 절차 수립** 「**정보보호정책서**」 제 ○○조 (정보보호 정책) ① 정보보호정책 및 정책시행 문서에 대한 타당성 검토를 최소 연 1회 이상 수행하여야

한다.

② 관련 법규 변경 및 내·외부 보안사고 발생 등의 중대한 사유 발생 시 추가로 검토하고 변경하여야 한다.

③ 정보보호 정책 및 정책 시행문서의 이력관리 절차를 수립하고 시행하며, 최신본으로 유지하여야 한다.



※ 정책 타당성 검토 (이해를 돕기 위한 예시)

◇ 조직의 대내외 환경에 중대한 변화 발생 시 정보보호 및 개인정보보호 관련 정책 및 시행문서에 미치는 영향을 검토하고 필요시 제·개정하고 있는가?

(예시) 대내·외 환경 변화에 따른 지침 제·개정

① 환경 변화 상황

1. 재택근무 및 원격근무 전환
2. VPN, 클라우드 서비스 대규모 도입
3. 개인 디바이스 업무 사용 허용

② 영향 검토 결과 기존 정보보호 정책의 한계 확인

1. 사무실 내 업무 환경만 고려된 접근통제 정책
2. 개인 디바이스 사용에 대한 보안 기준 부재
3. 원격 접속 시 보안 요구사항 미비

③ 정책 개정 내용

1. 원격근무 보안 정책 신설
   - VPN 접속 시 이중인증 의무화
   - 개인 디바이스 보안 요구사항 정의
   - 클라우드 서비스 이용 시 데이터 분류 및 보호조치
2. 접근통제 정책 개정
   - 원격 접속 시 접근 권한 제한
   - 네트워크 세분화 및 제로트러스트 모델 적용

◇ 정보보호 및 개인정보보호 관련 정책 및 시행문서의 제·개정 시 이해관계자의 검토를 받고 있는가?

부서 이해관계자 회의 및 의견 취합

① 정보보호 최고책임자 및 개인정보보호책임자, 정보보호 및 개인정보보호 관련조직, IT 부서, 중요정보 및 개인정보 처리부서, 중요정보취급자 및 개인정보 취급자 등 이해관계자 식별 및 협의

② 정보보호 및 개인정보보호 관련 정책 및 시행문서 변경으로 인한 업무 영향도, 법적 준거성 등 고려

③ 회의록 등 검토 사항에 대한 증적을 남기고 정책·지침 등에 관련 사항 반영

구분	주요 내용
검토 대상 문서	정책·지침·절차서 개정안
필수 이해관계자	CISO, CPO, IT부서, 개인정보·중요정보 처리부서
추가 이해관계자	법무팀, 사업부문, 시스템담당자, 감사팀, 경영진
검토 항목	1. 업무 영향도 및 법적 준거성 2. 문서 간 일관성 및 연계성
검토 절차	1. 개정안 배포 및 의견 수집 2. 의견 수렴 회의 및 조정 3. 최종안 작성 후 경영진 승인
증적자료	- 검토 회의록 - 검토 의견서 및 반영 내역 - 승인문서
주의사항	- 누락된 이해관계자 없이 검토 - 의견 미 반영 시 사유 문서화

※ 이해관계자 검토 (이해를 돕기 위한 예시)

◇ 정보보호 및 개인정보보호 관련 정책 및 시행문서의 제·개정 내역에 대하여 이력 관리를 하고 있는가?

정보보호·개인정보보호 정책 및 시행문서 개정 시 변경 내역을 체계적으로 기록·관리

① 체계적 이력관리를 통해 투명성, 책임성, 문서 일관성 확보

1. 문서 버전(번호), 개정 일자, 개정 사유, 작성자, 승인자 등 이력을 기록 및 관리

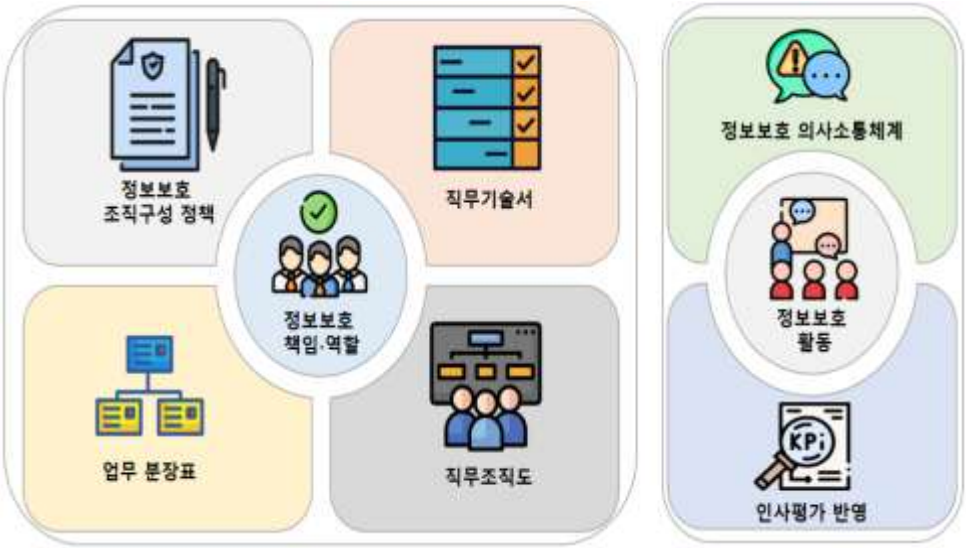
정보보호 정책서

구분	직위	성명	일자	서명
승인	정보보호최고책임자	OOO	0000.00.00	OOO
검토	정보보호담당자	OOO	0000.00.00	OOO

제 · 개정 이력			
번호	내용	담당자	일자
1	최초 작성	OOO	0000.00.00
2	일부 개정(정보통신망법 개정사항 반영)	OOO	0000.00.00
3	일부 개정(개인정보보호법 개정사항 반영)	OOO	0000.00.00

※ 정보보호 정책서 이력 관리 (이해를 돕기 위한 예시)

2.1.2 조직의 유지관리

세부분야	2.1.2 조직의 유지관리
인증 기준	조직의 각 구성원에게 정보보호와 개인정보보호 관련 역할 및 책임을 할당하고, 그 활동을 평가할 수 있는 체계와 조직 및 조직의 구성원 간 상호 의사소통 할 수 있는 체계를 수립하여 운영하여야 한다.
주요 확인사항	• 정보보호 및 개인정보보호 관련 책임자와 담당자의 역할 및 책임을 명확히 정의하고 있는가? • 정보보호 및 개인정보보호 관련 책임자와 담당자의 활동을 평가할 수 있는 체계를 수립하고 있는가? • 정보보호 및 개인정보보호 관련 조직 및 조직의 구성원 간 상호 의사소통 할 수 있는 체계 및 절차를 수립·이행하고 있는가?
기준 요약도	
운영 방안	**◇ 정보보호 및 개인정보보호 관련 책임자와 담당자의 역할 및 책임을 명확히 정의하고 있는가?** **정보보호 및 개인정보보호 관련 책임자와 담당자의 직무기술서 작성** ① 「정보보호 조직관리지침」 등 관련지침에 조직구성 내용 및 직무기술서 작성 1. 정보보호최고책임자 : 정보보호 업무 지휘 감독 2. 개인정보보호책임자 : 개인정보 보호업무 전반에 대한 업무 3. 정보보호관리자 : 정보보호 조직 운영 및 업무 지휘 감독 4. 개인정보보호관리자 : 개인정보보호 계획 수립 및 개인정보 업무 지휘 감독 3. 부서별 정보보호 담당자 : 소관업무별 정보보호 대책 강구 및 시행 등 4. 개인정보보호담당자 : 개인정보 보호 계획 이행 및 개인정보보호 시스템 운영 등 **구분** | **내용**

직무 명칭	정보보호최고책임자(CISO)
직무 개요	전사 정보보호 전략 수립·운영, 보안관리체계 구축·유지 및 보안 사고 대응을 총괄하며 경영진에 보고한다.
주요 책임	- 정보보호·개인정보보호 정책 수립 및 최종 승인 - 관리체계 운영 예산·자원 할당 및 모니터링 - 연간 위험평가 계획 승인 및 결과 검토 - 보안사고 대응 의사결정 및 사고조사 지휘 - 보안 위원회 개최 및 경영진 대상 정기보고
보고 라인	최고경영자(CEO) 또는 이사회
협업 부서	개인정보보호팀, 정보보호팀, IT 부서, 법무팀, 감사팀
자격 요건	- 정보보호 또는 유관 분야 석사학위 이상 또는 관련 분야 10년 이상 경력 - ISMS-P 인증 심사원 자격 또는 CISM, CISSP, CISA 등 국제 공인 정보보호 자격증 보유 - 보안 전략 수립 및 경영진 보고 경험 - 리더십 및 의사결정 능력, 커뮤니케이션 스킬
주요 성과지표(KPI)	- 연간 보안 사고 건수 및 대응 속도 - 정보보호 인증(ISMS-P, ISO27001) 유지·갱신 여부 - 위험평가 조치 이행률 - 보안교육 이수율 - 예산 집행 효율성
직무 성과 기대	- 조직 전반의 보안 수준 향상 및 규제 준수 확보 - 보안 사고 예방 및 피해 최소화 - 경영진 신뢰 확보를 통한 보안 투자 확대

※ 직무기술서 작성 (이해를 돕기 위한 예시

(예시) 정보보호 및 개인정보보호 조직구성, 업무분장

① 전략·관리 계층

1. 정보보호최고책임자(CISO): 전사 보안 전략 수립·예산·자원 배분 총괄, 경영진 보고·주요 보안 의사결정
2. 개인정보보호책임자(CPO): 개인정보보호 정책·법적 준거성 관리, 영향평가·침해사고 대응 주도

② 운영 계층

1. 정보보호팀: 보안정책 시행·모니터링, 보안감사·사고 분석·보안교육 운영
2. 개인정보보호팀: 개인정보 처리 절차 운영·내부 점검, 정보주체 권리 요청 처리·문서

관리

3. IT보안기술팀: 방화벽·IDS·VPN 등 보안장비 운영, 취약점 점검·로그관리·기술적 대응

4. 사업부 개인정보취급자: 부서별 개인정보 처리 기록·보고·안전조치 이행·정보주체 요청 지원

③ 지원 계층

1. 법무팀: 법령·규제 준거성 검토, 계약서·정책 법률 자문

2. 감사팀: 관리체계 내부감사·시정조치 점검

3. 경영진: 운영 성과 검토·주요 정책·투자 승인·보안사고 대응 지시

※ 출처: 정보보호 및 개인정보보호 관리체계 인증신청 양식 (한국인터넷진흥원)

※ 정보보호 조직 업무분장 (이해를 돕기 위한 예시)

◇ 정보보호 및 개인정보보호 관련 책임자와 담당자의 활동을 평가할 수 있는 체계를 수립하고 있는가?

(예시) 담당자와 책임자 활동을 평가할 수 있는 체계/지표 설정

① CISO 평가지표

1. 연간 보안사고 발생 건수 및 대응시간
2. 위험평가 계획 대비 이행률 (95% 이상)
3. 보안교육 목표 이수율 (100% 달성)
4. 내부감사 지적사항 해결률 (90% 이상)
5. 예산 집행률 및 효율성

② IT보안기술 담당자 평가지표

1. 시스템 취약점 해결률 (중요도별 기한 내 100%)
2. 보안장비 가용률 (99.9% 이상)
3. 로그 수집·분석 완료율 (100%)
4. 보안패치 적용률 (긴급 24시간, 중요 1주일)

◇ 정보보호 및 개인정보보호 관련 조직 및 조직의 구성원 간 상호 의사소통 할 수 있는 체계 및 절차를 수립·이행하고 있는가?

조직 구성원 간의 의사소통 체계 마련

① 의사소통 관리 계획 개요: 목적 및 범위

② 의사소통 체계: 전사 협의체, 실무 협의체, 위원회 등 보고 및 협의체 운영방안, 참여 대상, 참여대상별 역할 및 책임, 주기 등

③ 의사소통 방법: 보고 및 회의(월간보고, 주간보고 등), 공지, 이메일, 메신저, 정보보호포털 등

④ 의사소통 양식: 유형별 보고서 양식, 회의록 양식 등

2.1.3 정보자산 관리

<table>
<tr><th>세부분야</th><th>2.1.3 정보자산 관리</th></tr>
<tr><td>인증
기준</td><td>정보자산의 용도와 중요도에 따른 취급 절차 및 보호 대책을 수립·이행하고, 자산별 책임 소재를 명확히 정의하여 관리하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 정보자산의 보안등급에 따른 취급절차(생성·도입, 저장, 이용, 파기) 및 보호 대책을 정의하고 이행하고 있는가?
• 식별된 정보자산에 대하여 책임자 및 관리자를 지정하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>
◇ 정보자산의 보안등급에 따른 취급절차(생성·도입, 저장, 이용, 파기) 및 보호 대책을 정의하고 이행하고 있는가?

(예시) 보안등급 별 취급절차
<table>
<tr><th>구분</th><th>기밀(Confidential)</th><th>대외비(Restricted)</th><th>일반(General)</th></tr>
<tr><td>생성·도입</td><td>부서장급 이상 승인
정보보호책임자 검토
생성 즉시 "기밀" 마킹</td><td>팀장급 이상 승인
부서 내 검토
"대외비" 표시</td><td>담당자 단독 생성
사후 확인</td></tr>
<tr><td>저장</td><td>암호화 전용 서버
이중인증 접근
오프라인 백업</td><td>보안 서버/제한폴더
부서별 접근권한
암호화 백업 권장</td><td>일반 공유서버
기본 인증
정기 백업</td></tr>
<tr><td>이용</td><td>필수 인원만
복사·인쇄 승인 필요
모든 이력 로그저장</td><td>업무 관련자
팀장 승인
주요 이력 기록</td><td>임직원 누구나
기본 로그만</td></tr>
<tr><td>파기</td><td>정보보호책임자 승인 및 검토
디가우징/완전파쇄
영상기록/입회확인
파기증명서 작성</td><td>부서장 승인
3회 이상 덮어쓰기
담당자 확인서
목록 및 일시 등 상세 로그</td><td>담당자 판단
일반 삭제
별도 확인 불요
기본 삭제 로그</td></tr>
</table>
※ 보안등급 별 취급절차 (이해를 돕기 위한 예시)

◇ 식별된 정보자산에 대하여 책임자 및 관리자를 지정하고 있는가?
</td></tr>
</table>

(예시) 책임자 및 관리자 지정 절차

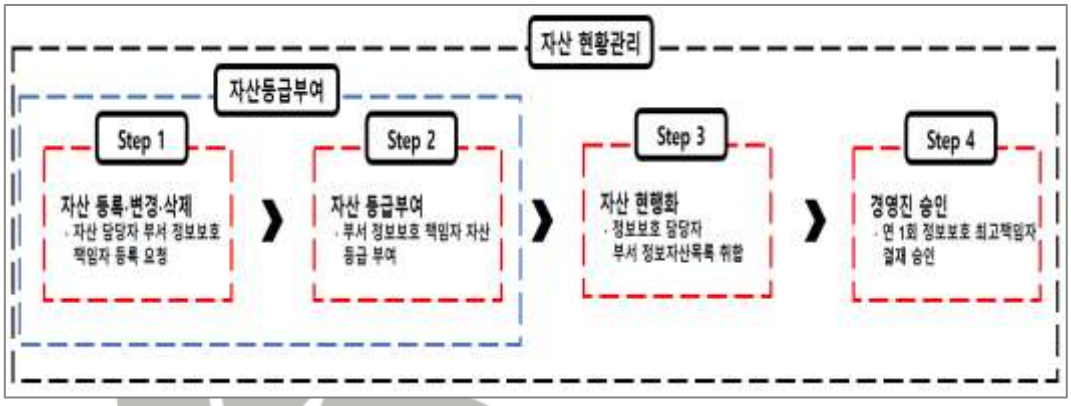
「**정보보호 운영지침**」 제 ○○조 (정보자산 등록)

① 자산 등록·변경·삭제는 정보 소유자가 필요 시 부서 정보보호 책임자의 허가를 득하고 부서 자산목록에 직접 등록한다.

② 부서 정보보호 책임자는 등록된 자산의 보안 등급에 따라 자산코드를 부여하여야 한다.

③ 정보보호담당자는 분기별 각 부서의 자산목록을 검토, 취합, 현행화한다.

④ 정보보호담당자는 연 1회 자산 실사하여야 하며, 그 결과를 정보보호 최고책임자에게 보고해야 한다.



※ 식별된 자산 관리자 지정 (이해를 돕기 위한 예시)

2.2 인적보안

2.2.1 주요 직무자 지정 및 관리

<table>
<tr><th>세부분야</th><th>2.2.1 주요 직무자 지정 및 관리</th></tr>
<tr><td>인증
기준</td><td>개인정보 및 중요정보의 취급이나 주요 시스템 접근 등 주요 직무의 기준과 관리방안을 수립하고, 주요 직무자를 최소한으로 지정하여 그 목록을 최신으로 관리하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 개인정보 및 중요정보의 취급, 주요 시스템 접근 등 주요 직무의 기준을 명확히 정의하고 있는가?
• 주요 직무를 수행하는 임직원 및 외부자를 주요 직무자로 지정하고 그 목록을 최신으로 관리하고 있는가?
• 업무상 개인정보를 취급하는 자를 개인정보취급자로 지정하고 목록을 최신으로 관리하고 있는가?
• 업무 필요성에 따라 주요 직무자 및 개인정보취급자 지정을 최소화하는 등 관리방안을 수립·이행하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 개인정보 및 중요정보의 취급, 주요 시스템 접근 등 주요 직무의 기준을 명확히 정의하고 있는가?

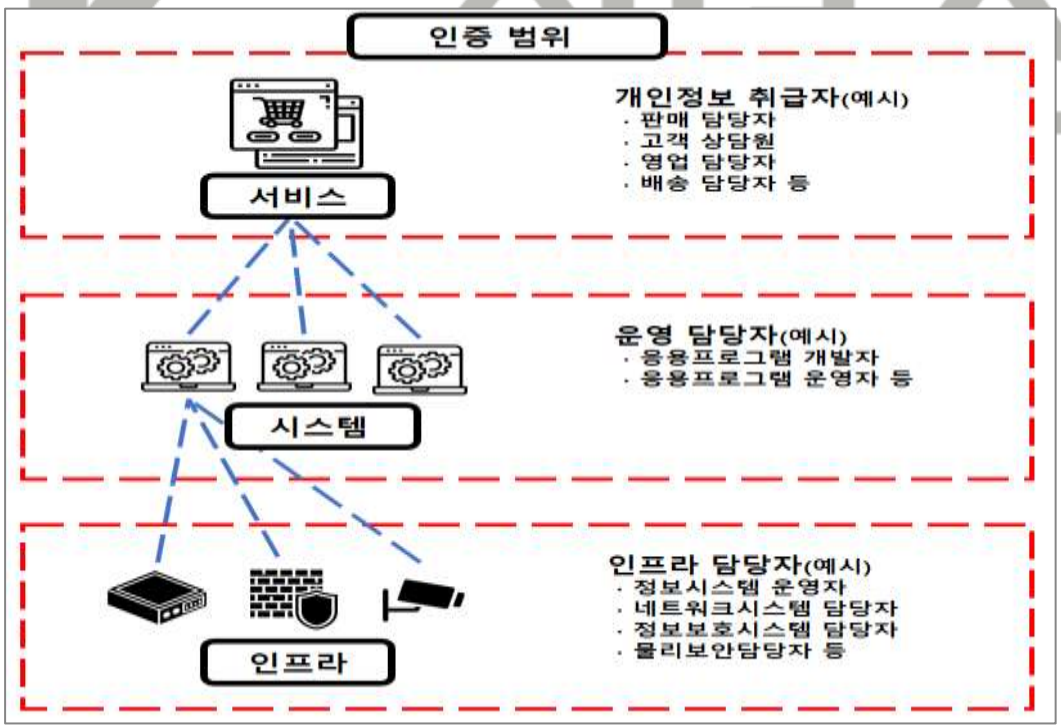
(예시) 주요 직무자 기준 정의
① 개인정보 취급자
<table>
<tr><th>구분</th><th>세부 기준</th><th>업무 예시</th></tr>
<tr><td>개인정보처리시스템 관리</td><td>개인정보처리시스템에 대한 관리 권한 보유자</td><td>회원관리시스템 관리자, CRM 시스템 운영자</td></tr>
</table></td></tr>
</table>

대량/중요 개인정보 취급	1만명 이상 또는 민감정보 1천명 이상 처리	고객센터 상담원, 마케팅팀 담당자
개인정보 파일 관리	개인정보 파일의 생성·변경·삭제 권한	DB 관리자, 백업 담당자
개인정보 분석·통계	개인정보를 활용한 분석 업무 수행	데이터분석가, 맞춤형 서비스 개발자

② 시스템 및 인프라 담당 관련 직무

구분	세부 기준	업무 예시
시스템 관리자	서버, 네트워크, DB에 대한 관리자 권한	시스템 엔지니어, DBA, 네트워크 관리자
보안시스템 운영	방화벽, IDS/IPS, 보안솔루션 운영	보안관제 요원, SOC 분석가
개발시스템 접근	운영환경 또는 개발환경 소스코드 접근	시스템 개발자, 프로그램 관리자
감사 및 모니터링	로그분석, 감사 관련 시스템 접근	내부감사팀, 컴플라이언스 담당자

③ 개인정보 및 중요정보의 취급, 주요 시스템 접근 등 주요 직무의 기준을 명확히 정의하고 주요 직무자를 최소한으로 지정·관리



※ 주요 직무 지정 및 범위 산정 (이해를 돕기 위한 예시)

◇ 주요 직무를 수행하는 임직원 및 외부자를 주요 직무자로 지정하고 그 목록을 최신으로 관리하고 있는가?

주요 직무자 현황관리

① 주요 직무 기준 정의

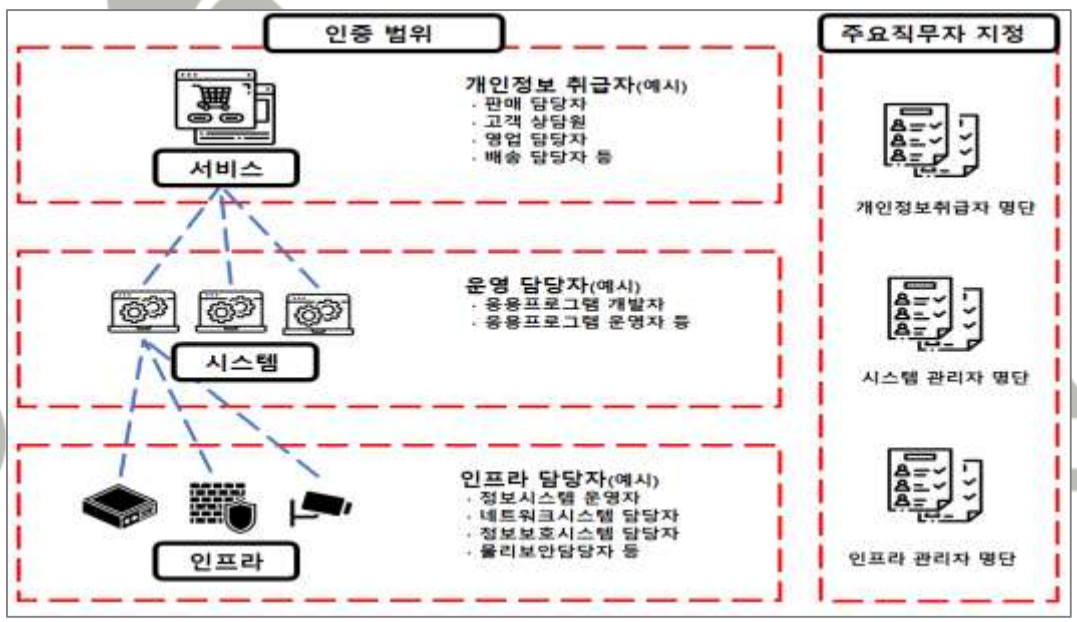
1. 개인정보·중요정보 취급, 주요 정보시스템 접근·운영 등 주요 직무 범위를 명확히 문서화

② 주요 직무자 지정

1. 위 기준에 따라 임직원 및 업무 위탁·파견 등 외부자 중에서 주요 직무자를 지정.

③ 목록 관리 및 최신화

1. 지정 현황을 전산대장에 등록하고, 인사 변경(입사·퇴사·부서 이동) 시 즉시 반영.
2. 주기적(반기/분기별)으로 목록을 검토하여 누락·과다 지정 여부를 점검하고 수정



정보시스템 사용자 관리대장 (예시)

번호	사용자 ID	사용자명	부서	직위	시스템명	IP 주소	계정 생성일	계정 종료일	접근 권한	비고
1	USER0001	김철수	IT 부서	과장	ERP 시스템	192.168.1.101	2023-01-10	-	관리자	정기 점검 필요
2	USER0002	이영희	인사 부서	대리	HR 시스템	192.168.1.102	2023-03-15	-	사용자	보안 교육 필요
3	USER0004	최유리	재무 부서	팀장	재무관리 시스템	192.168.1.104	2023-05-22	-	관리자	비밀번호 정기 변경 필요
4	USER0005	김준호	영업 부서	주임	영업관리 시스템	192.168.1.105	2023-07-01	-	사용자	2단계 인증 설정 필요

※ 주요 직무자 현황관리 (이해를 돕기 위한 예시)

◇ 업무상 개인정보를 취급하는 자를 개인정보취급자로 지정하고 목록을 최신으로 관리하고 있는가?

개인정보취급자 지정 및 최신화 관리

① 개인정보취급자 범위 정의

1. 권한 및 업무 상 개인정보를 직접 조회·수정·삭제할 수 있는 자를 개인정보취급자로 규정

② 지정 및 목록화

1. 전산 처리권한 현황과 업무별 접근 권한 대장을 대조하여 지정.

③ 목록 최신화

1. 개인정보 취급 권한 변경(신규·변경·해제) 시 즉시 목록에 반영.
2. 주기적(반기/분기별) 자체 감사 시 목록 정확성을 검증하고 이슈를 개선

개인정보처리시스템 접근권한 관리대장 (예시)

번호	사용자 ID	사용자명	부서	직위	시스템명	IP 주소	접근권한 부여일	접근권한 해지일	접근권한	비고
1	USER0001	김철수	IT 부서	과장	개인정보처리시스템 A	192.168.1.101	2023-01-10	-	관리자	정기 점검 필요
2	USER0002	이영희	인사 부서	대리	개인정보처리시스템 A	192.168.1.102	2023-03-15	-	사용자	교육 필요
3	USER0003	박민수	마케팅 부서	사원	개인정보처리시스템 A	192.168.1.103	2022-11-05	2023-02-20	읽기 전용	권한 해지 완료
4	USER0004	최유리	재무 부서	팀장	개인정보처리시스템 B	192.168.1.104	2023-05-22	-	관리자	정기 비밀번호 변경 필요
5	USER0005	김준호	영업 부서	주임	개인정보처리시스템 B	192.168.1.105	2023-07-01	-	사용자	2단계 인증 설정 필요

※ 개인정보처리시스템 접근권한 관리대장 (이해를 돕기 위한 예시)

◇ 업무 필요성에 따라 주요 직무자 및 개인정보취급자 지정을 최소화하는 등 관리방안을 수립·이행하고 있는가?

지정 최소화 및 관리방안 수립·이행

① 최소 권한 원칙

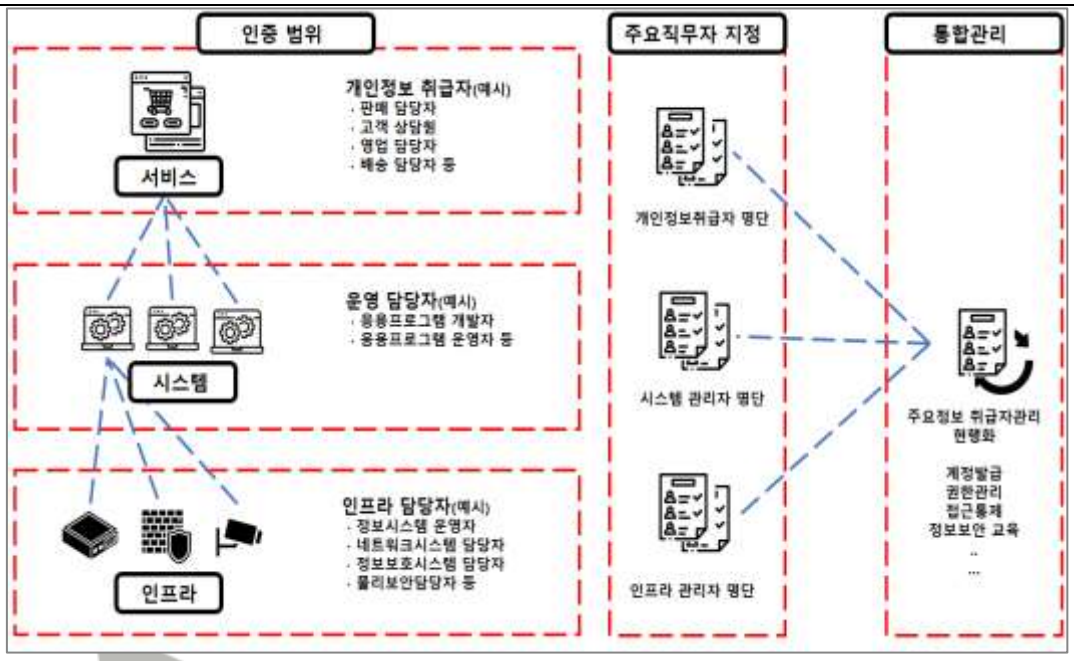
1. 주요 직무자 및 개인정보취급자 지정을 업무 필요성에 한정하여 수행

② 주요 직무자 및 개인정보취급자 지정 시 승인 절차

1. 요청 시 보안 책임자 및 정보 보호 담당자의 이중 승인을 거치도록 프로세스를 정의

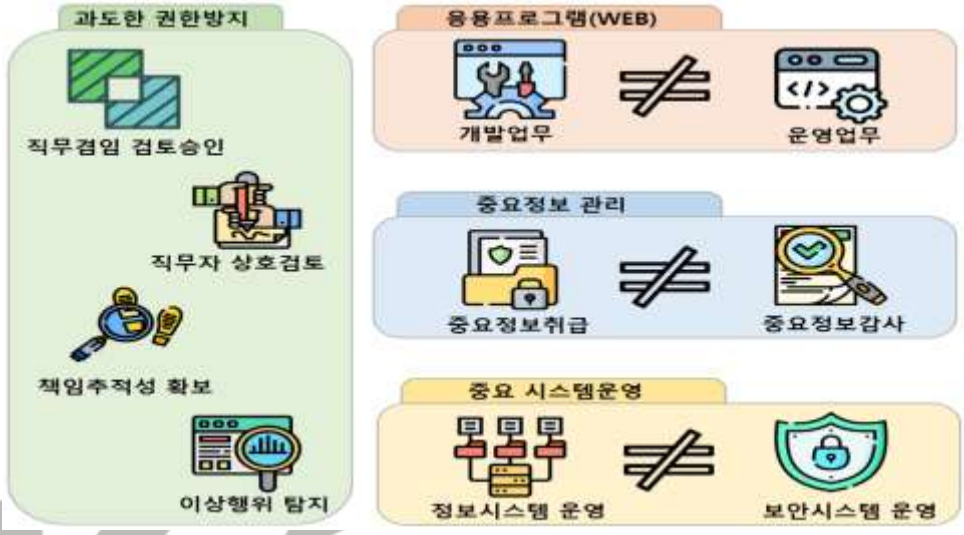
③ 정기 검토 및 교육

1. 권한의 적정성을 정기 검토하며, 과다 지정자에 대한 권한 회수 절차를 운영
2. 지정된 모든 대상자는 신규 지정 시 보안 서약 및 역할별 교육을 이수



※ 주요 직무자 및 개인정보취급자 관리방안 수립 (이해를 돕기 위한 예시)

2.2.2 직무 분리

세부분야	2.2.2 직무 분리
인증 기준	권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여 직무 분리 기준을 수립하고 적용하여야 한다. 다만 불가피하게 직무 분리가 어려운 경우 별도의 보완대책을 마련하여 이행하여야 한다.
주요 확인사항	• 권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여 직무 분리 기준을 수립하여 적용하고 있는가? • 직무 분리가 어려운 경우 직무자 간 상호 검토, 상위관리자 정기 모니터링 및 변경 사항 승인, 책임 추적성 확보 방안 등의 보완통제를 마련하고 있는가?
기준 요약도	
운영 방안	**◇ 권한 오·남용 등으로 인한 잠재적인 피해 예방을 위하여 직무 분리 기준을 수립하여 적용하고 있는가?** **(예시) 직무 분리 기준 수립** ① 개발·운영 직무 : 시스템 개발자와 운영자의 역할을 명확히 구분하고 별도 계정 및 개발·운영 환경을 분리하여 운영 ② 정보보호관리와 시스템 운영·개발 : 정보보호 담당자와 시스템 운영·개발자의 업무를 상호 독립화 ③ 시스템 유형별 : 서버·DB·네트워크 등 주요 시스템 간 운영 직무를 분리 ④ 감사·모니터링 업무 : 보안 감사·로그 분석 등의 업무를 별도의 조직 또는 인력에 배정 ⑤ 그 밖에 내부통제와 관련하여 직무의 분리가 요구되는 경우 **◇ 직무 분리가 어려운 경우 직무자 간 상호 검토, 상위관리자 정기 모니터링 및**

변경 사항 승인, 책임 추적성 확보 방안 등의 보완통제를 마련하고 있는가?

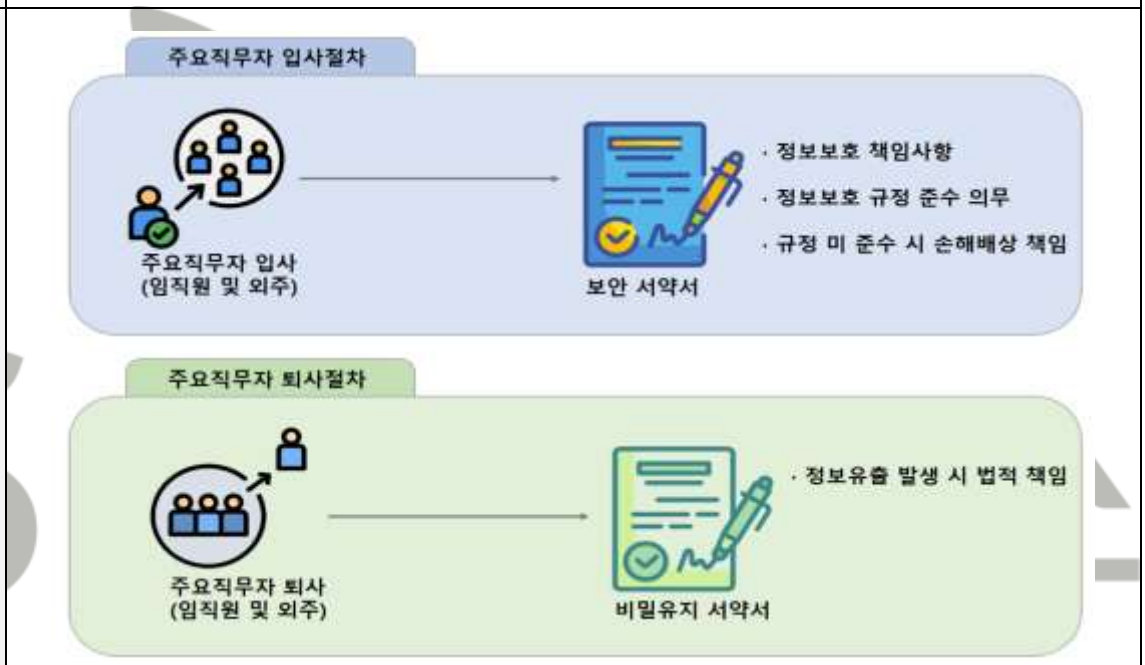
직무분리가 어려운 경우 직무자 보완통제 절차 마련

① 적용 조건

1. 물리적·기술적·운영적 제약으로 직무 분리가 불가능한 경우
2. 소규모 조직 또는 특정 시스템 특성으로 분리가 어려운 경우

구분	보완통제
상호 검토(Peer Review)	업무 결과·변경사항을 동료가 2차 검토하고 승인
상위관리자 모니터링	변경 전·후 작업 내용을 보안책임자 또는 관리자에게 보고·승인
책임추적성 확보(Audit Trail)	모든 작업 로그를 시스템에 기록, 주기적 감사 및 분석 시행
예외보고 및 조치	비정상 변경·오류 발생 시 즉시 예외 보고, 원인 분석 및 후속 조치 실시
승인 이력 관리	변경 요청서, 승인서 등 증적 문서화 및 중앙 저장

2.2.3 보안 서약

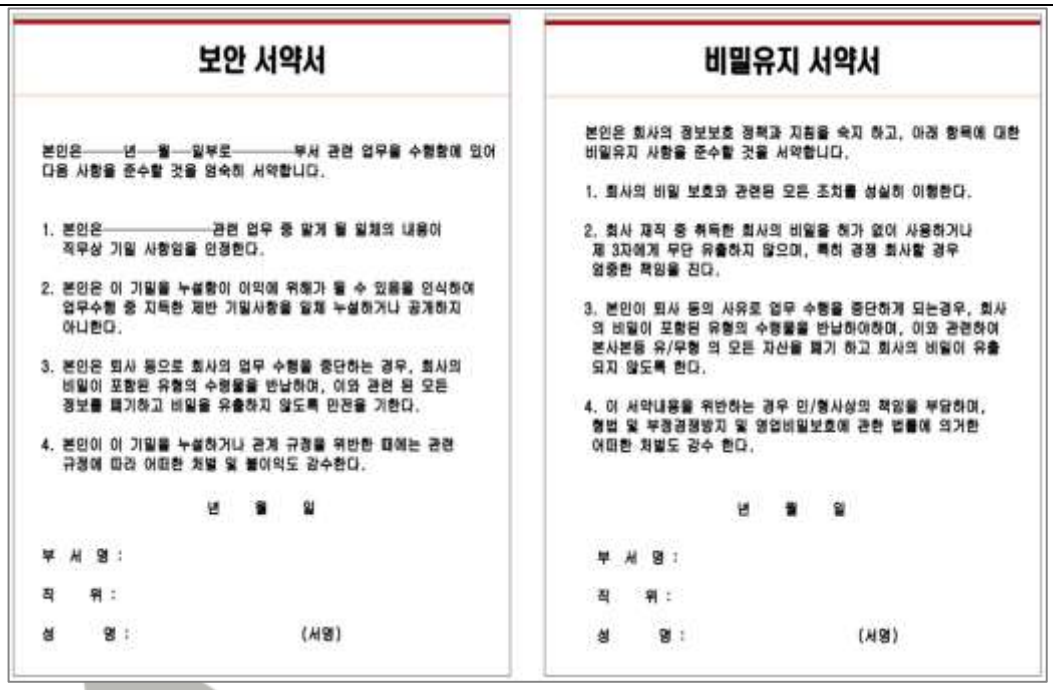
세부분야	2.2.3 보안 서약
인증 기준	정보자산을 취급하거나 접근권한이 부여된 임직원·임시직원·외부자 등이 내부 정책 및 관련 법규, 비밀유지 의무 등 준수사항을 명확히 인지할 수 있도록 업무 특성에 따른 정보보호 서약을 받아야 한다.
주요 확인사항	• 신규 인력 채용 시 정보보호 및 개인정보보호 책임이 명시된 정보보호 및 개인정보보호 서약서를 받고 있는가? • 임시직원, 외주용역직원 등 외부자에게 정보자산에 대한 접근권한을 부여할 경우 정보보호 및 개인정보보호에 대한 책임, 비밀유지 의무 등이 명시된 서약서를 받고 있는가? • 임직원 퇴직 시 별도의 비밀유지에 관련한 서약서를 받고 있는가? • 정보보호, 개인정보보호 및 비밀유지 서약서는 안전하게 보관하고 필요시 쉽게 찾아볼 수 있도록 관리하고 있는가?
기준 요약도	
운영 방안	**◇ 신규 인력 채용 시 정보보호 및 개인정보보호 책임이 명시된 정보보호 및 개인정보보호 서약서를 받고 있는가?** **서약서 징구** ① 신규, 임시직원, 외주용역직원 등 정보자산, 정보시스템 접근 시 보안서약서 징구 ② 임직원 퇴직 시 별도의 비밀유지 서약서 작성

※ 보안서약서 작성 (이해를 돕기 위한 예시)

◇ 임시직원, 외주용역직원 등 외부자에게 정보자산에 대한 접근권한을 부여할 경우 정보보호 및 개인정보보호에 대한 책임, 비밀유지 의무 등이 명시된 서약서를 받고 있는가?

정보보호 및 개인정보보호에 대한 책임, 비밀유지 의무 등이 명시된 서약서

① 정보보호 및 개인정보보호 책임, 비밀유지 의무, 내부 규정 및 관련 법규 준수 의무, 관련 의무의 미준수로 인한 사건·사고 발생 시 손해배상 책임 등 필요한 내용을 포함한 서약서 작성



보안 서약서

본인은 ____년 ____월 ____일부로 ____부서 관련 업무를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 ____관련 업무 중 알게 될 일체의 내용이 직무상 기밀 사항임을 인정한다.
2. 본인은 이 기밀을 누설함이 이익에 위해가 될 수 있음을 인식하여 업무수행 중 지득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.
3. 본인은 회사 등으로 회사의 업무 수행을 중단하는 경우, 회사의 비밀이 포함된 유형의 수행물을 반납하며, 이와 관련 된 모든 정보를 폐기하고 비밀을 유출하지 않도록 만전을 기한다.
4. 본인이 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 규정에 따라 어떠한 처벌 및 불이익도 감수한다.

년 월 일

부 서 명 :

직 위 :

성 명 : (서명)

비밀유지 서약서

본인은 회사의 정보보호 정책과 지침을 숙지 하고, 아래 항목에 대한 비밀유지 사항을 준수할 것을 서약합니다.

1. 회사의 비밀 보호와 관련된 모든 조치를 성실히 이행한다.
2. 회사 재직 중 취득한 회사의 비밀을 허가 없이 사용하거나 제 3자에게 무단 유출하지 않으며, 특히 경쟁 회사할 경우 엄중한 책임을 진다.
3. 본인이 회사 등의 사유로 업무 수행을 중단하게 되는경우, 회사의 비밀이 포함된 유형의 수행물을 반납하여야며, 이와 관련하여 본사본등 유/무형 의 모든 자산을 폐기 하고 회사의 비밀이 유출 되지 않도록 한다.
4. 이 서약내용을 위반하는 경우 민/형사상의 책임을 부담하며, 형법 및 부정경쟁방지 및 영업비밀보호에 관한 법률에 의거한 어떠한 처벌도 감수 한다.

년 월 일

부 서 명 :

직 위 :

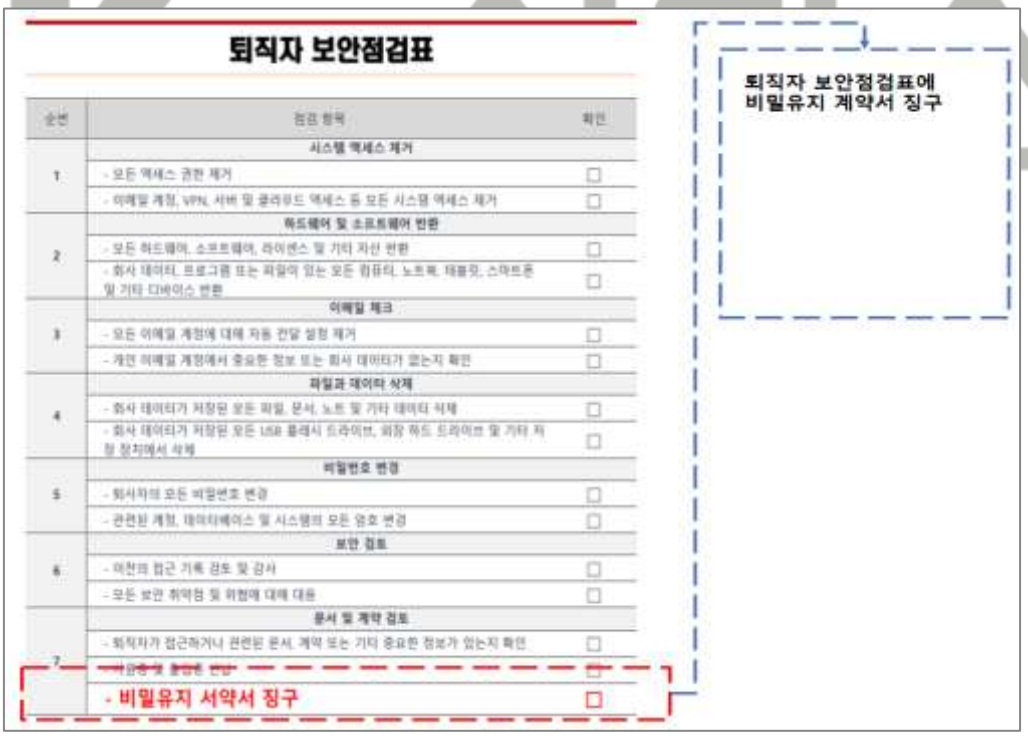
성 명 : (서명)

※ 보안서약서 작성 (이해를 돕기 위한 예시)

◇ 임직원 퇴직 시 별도의 비밀유지에 관련한 서약서를 받고 있는가?

퇴직 시 보안 체크리스트 작성 적용

① 퇴직자에게 정보 유출 발생 시 그에 따르는 법적 책임이 있음을 명확히 인식시킬 수 있도록 비밀유지 서약서 징구(퇴직 절차 내 포함)



퇴직자 보안점검표

순번	점검 항목	확인
1	시스템 액세스 제거	
	- 모든 액세스 권한 제거	☐
	- 이메일 계정, VPN, 서버 및 클라우드 액세스 등 모든 시스템 액세스 제거	☐
2	하드웨어 및 소프트웨어 반환	
	- 모든 하드웨어, 소프트웨어, 라이센스 및 기타 자산 반환	☐
	- 회사 데이터, 프로그램 또는 파일이 있는 모든 컴퓨터, 노트북, 태블릿, 스마트폰 및 기타 디바이스 반환	☐
3	이메일 체크	
	- 모든 이메일 계정에 대해 자동 전달 설정 제거	☐
	- 개인 이메일 계정에서 중요한 정보 또는 회사 데이터가 없는지 확인	☐
4	파일과 데이터 삭제	
	- 회사 데이터가 저장된 모든 파일, 문서, 노트 및 기타 데이터 삭제	☐
	- 회사 데이터가 저장된 모든 USB 플래시 드라이브, 외장 하드 드라이브 및 기타 저장 장치에서 삭제	☐
5	비밀번호 변경	
	- 퇴사자의 모든 비밀번호 변경	☐
	- 관련된 계정, 데이터베이스 및 시스템의 모든 암호 변경	☐
6	보안 검토	
	- 이전의 접근 기록 검토 및 감사	☐
	- 모든 보안 취약점 및 위협에 대해 대응	☐
7	문서 및 계약 검토	
	- 퇴직자가 접근하거나 관련된 문서, 계약 또는 기타 중요한 정보가 있는지 확인	☐
	[illegible]	☐
	- 비밀유지 서약서 징구	☐

퇴직자 보안점검표에 비밀유지 계약서 징구

※ 퇴직자 체크리스트 (이해를 돕기 위한 예시)

	◇ 정보보호, 개인정보보호 및 비밀유지 서약서는 안전하게 보관하고 필요시 쉽게 찾아볼 수 있도록 관리하고 있는가? **서약서는 안전하게 보존** ① 법적 분쟁 발생 시 법률적 책임에 대한 증거자료로 사용할 수 있도록 잠금장치가 있는 캐비닛 또는 출입통제가 적용된 문서고 등에 안전하게 보관·관리

2.2.4 인식제고 및 교육훈련

세부분야	2.2.4 인식제고 및 교육훈련
인증 기준	임직원 및 관련 외부자가 조직의 관리체계와 정책을 이해하고 직무별 전문성을 확보할 수 있도록 연간 인식제고 활동 및 교육훈련 계획을 수립·운영하고, 그 결과에 따른 효과성을 평가하여 다음 계획에 반영하여야 한다.
주요 확인사항	• 정보보호 및 개인정보보호 교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 교육 계획을 수립하고 경영진의 승인을 받고 있는가? • 관리체계 범위 내 모든 임직원과 외부자를 대상으로 연간 교육 계획에 따라 연 1회 이상 정기적으로 교육을 수행하고, 관련 법규 및 규정의 중대한 변경 시 이에 대한 추가교육을 수행하고 있는가? • 임직원 채용 및 외부자 신규 계약 시 업무 시작 전에 정보보호 및 개인정보보호 교육을 시행하고 있는가? • IT 및 정보보호, 개인정보보호 조직 내 임직원은 정보보호 및 개인정보보호와 관련하여 직무별 전문성 제고를 위한 별도의 교육을 받고 있는가? • 교육 시행에 대한 기록을 남기고 교육 효과와 적정성을 평가하여 다음 교육 계획에 반영하고 있는가?
기준 요약도	
운영 방안	**◇ 정보보호 및 개인정보보호 교육의 시기, 기간, 대상, 내용, 방법 등의 내용이 포함된 연간 교육 계획을 수립하고 경영진의 승인을 받고 있는가?** **연간 교육 계획 수립 및 지침 반영** 「**인적보안 지침**」 제 ○○조 (교육 및 훈련) ① 정보보호 관리자는 매년 각 호를 포함한 정보보안 교육 및 훈련 계획을 수립하고 정보보호 최고책임자(CISO)의 승인을 받아야 한다. 1. 교육 유형: 임직원 인식제고 교육, 주요직무자, 개인정보취급자 교육, 수탁자 교육, 전문 교육

2. 교육 방법: 교육 목적, 교육 대상, 교육 일정, 교육 시간, 교육 내용, 온라인 및 집합교육

3. 교육 승인: 교육 계획을 검토, 승인하여 계획에 따라 이행될 수 있도록 예산 배정 지원

00년 정보보호 교육계획

구분	직위	성명	일자	서명
승인	정보보호 최고책임자	OOO	2023-01-01	승인
상신	정보보호 담당자	OOO	2022-12-20	-

※ 정보보호 교육계획 (이해를 돕기 위한 예시)

◇ 관리체계 범위 내 모든 임직원과 외부자를 대상으로 연간 교육 계획에 따라 연 1회 이상 정기적으로 교육을 수행하고, 관련 법규 및 규정의 중대한 변경 시 이에 대한 추가교육을 수행하고 있는가?

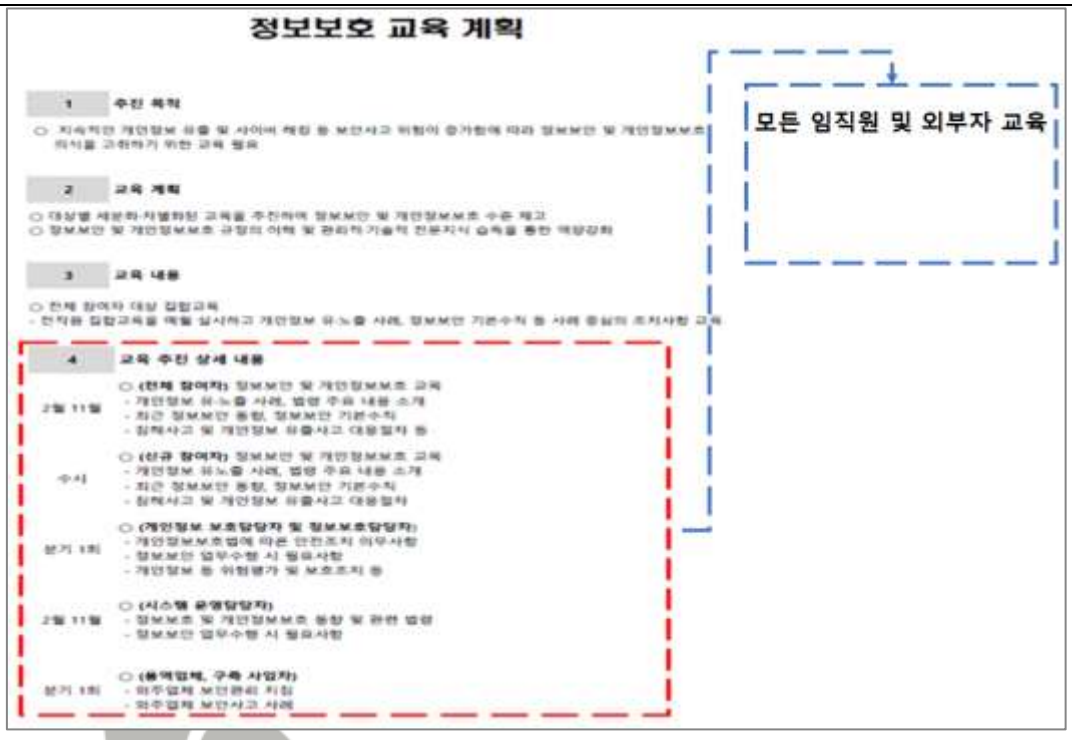
관리체계 범위 내 모든 임직원과 외부자를 대상으로 연간 교육 계획

① 정보자산에 직·간접적으로 접근하는 임직원, 임시직원, 외주용역업체 직원 등 모든 인력 포함

② 수탁자 및 파견된 직원인 경우 해당 업체가 교육 수행할 수 있도록 관련 자료 제공, 시행 여부를 관리·감독

③ 최소 연 1회 이상 교육 수행(특히 개인정보취급자의 경우 법적 요구사항에 따라 연 1회 이상 개인정보보호 교육 필요)

④ 교육 내용에는 임직원 및 관련 외부자가 조직의 관리체계와 정책을 이해하고, 이를 준수할 수 있도록 필요한 내용을 모두 포함하여야 함

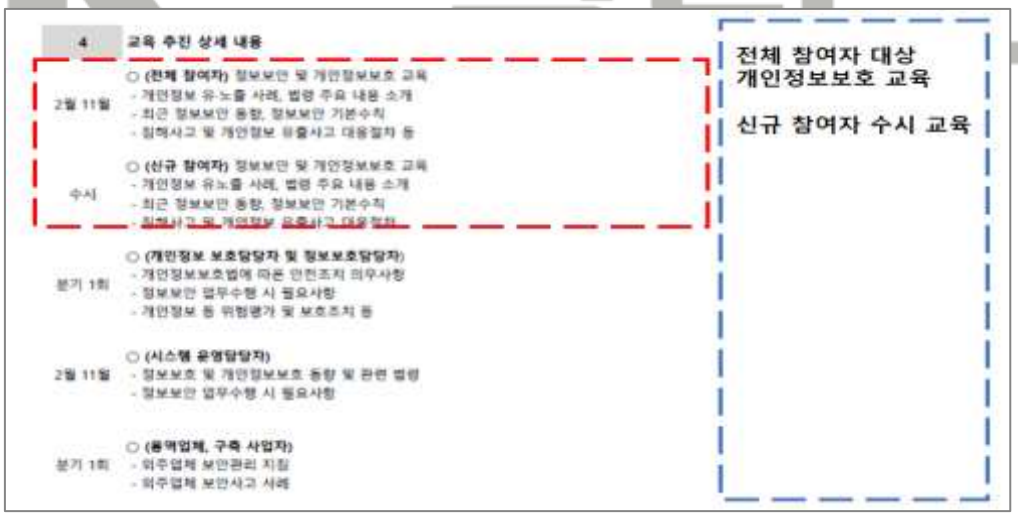


※ 정보보호 교육 계획(이해를 돕기 위한 예시)

◇ 임직원 채용 및 외부자 신규 계약 시 업무 시작 전에 정보보호 및 개인정보보호 교육을 시행하고 있는가?

임직원 채용 및 외부자 신규 계약 시 업무 시작 전에 정보보호 및 개인정보보호 교육 시행

① 신규 인력 발생 시점 또는 업무 수행 전에 정보보호 및 개인정보보호 교육을 시행하여 조직 정책, 주의사항, 규정 위반 시 법적 책임 등에 대한 내용 숙지



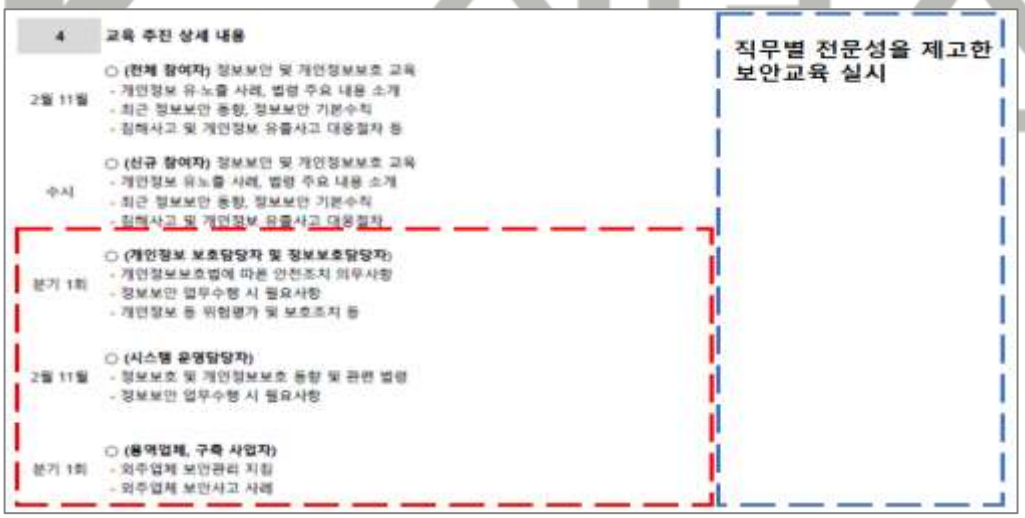
※ 정보보호 교육 상세 일정 (이해를 돕기 위한 예시)

◇ IT 및 정보보호, 개인정보보호 조직 내 임직원은 정보보호 및 개인정보보호와 관련하여 직무별 전문성 제고를 위한 별도의 교육을 받고 있는가?

(예시) 직무별 전문성 제고를 위한 교육

① 주요 직무 그룹 별 권장되는 교육자료 및 교육방법 모색

대상 그룹	교육 주제	교육자료 예시
IT 운영팀	시스템 보안 설정 및 로그 분석	Linux 서버 보안 가이드 SIEM을 활용한 실시간 로그 모니터링
애플리케이션 개발팀	안전한 코딩(OWASP Top 10)	웹 취약점 이해 및 대응 온라인 강의 SAST 도구 활용 실습
정보보호팀	취약점 진단·침투 테스트	보호나라 사이버 시큐리티 훈련
개인정보보호팀	개인정보 처리 위탁 관리	개인정보보호법 개정 설명회 개인정보보호 과정 온라인 강의
주요 직무자 개인정보취급자	보안서약 및 역할 책임 이해	주요 직무자 역할별 권한·책임
외부자 (수탁·파견 인력)	계약 기반 보안·개인정보보호 의무	수탁사 보안 준수 체크리스트 보안 교육 동영상



※ 전문적 정보보호 교육 실시 (이해를 돕기 위한 예시)

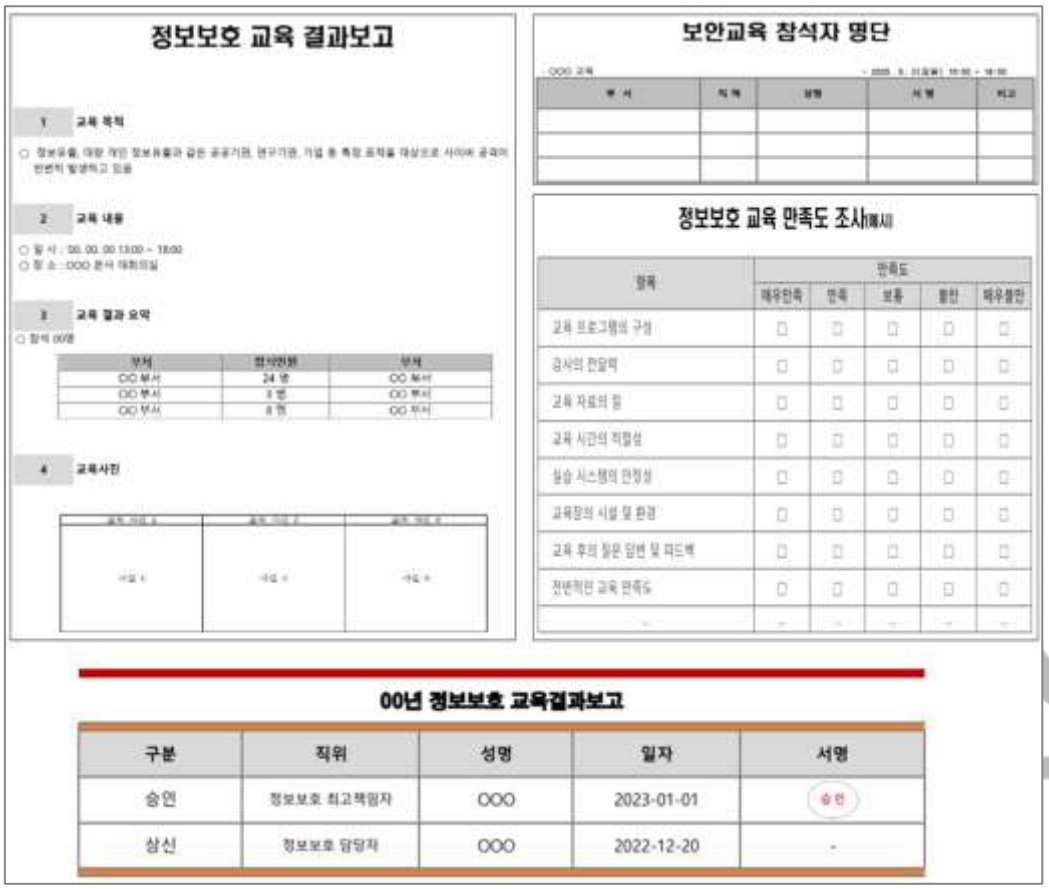
◇ 교육 시행에 대한 기록을 남기고 교육 효과와 적정성을 평가하여 다음 교육 계획에 반영하고 있는가?

교육 기록 보관 및 평가

① 교육 시행 후 출석 기록

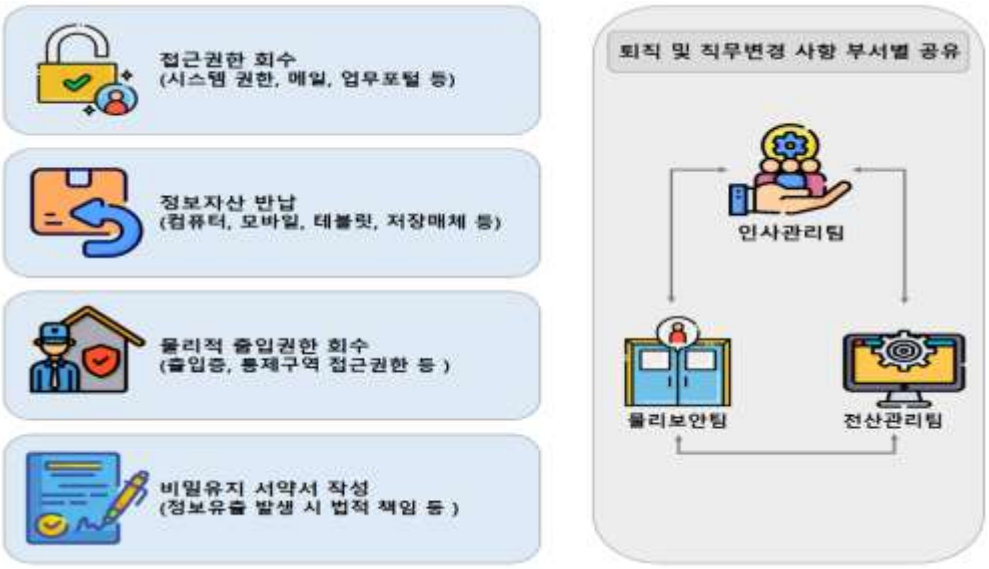
② 설문조사 등을 통한 교육 만족도 조사

③ 만족도 조사를 토대로 차년도 계획 수립



※ 정보보호 교육 결과보고 (이해를 돕기 위한 예시)

2.2.5 퇴직 및 직무변경 관리

세부분야	2.2.5 퇴직 및 직무변경 관리
인증 기준	퇴직 및 직무변경 시 인사·정보보호·개인정보보호·IT 등 관련 부서별 이행하여야 할 자산반납, 계정 및 접근권한 회수·조정, 결과확인 등의 절차를 수립·관리하여야 한다.
주요 확인사항	• 퇴직, 직무변경, 부서이동, 휴직 등으로 인한 인사변경 내용이 인사부서, 정보보호 및 개인정보보호 부서, 정보시스템 및 개인정보처리시스템 운영부서 간 공유되고 있는가? • 조직 내 인력(임직원, 임시직원, 외주용역직원 등)의 퇴직 또는 직무변경 시 지체 없는 정보자산 반납, 접근권한 회수·조정, 결과 확인 등의 절차를 수립·이행하고 있는가?
기준 요약도	
운영 방안	**◇ 퇴직, 직무변경, 부서이동, 휴직 등으로 인한 인사변경 내용이 인사부서, 정보보호 및 개인정보보호 부서, 정보시스템 및 개인정보처리시스템 운영부서 간 공유되고 있는가?** **(예시) 인사변경 발생 시 관련 부서 간 신속·정확한 정보 공유** ① 실시간 API 연동 또는 동기화 1. 인사관리시스템(HRMS) 변경 시 IT·보안·개인정보시스템에 즉시 전송 2. 일배치 동기화를 통해 매일 새벽 HRMS 변경 이력 파일(SFTP) → 대상 시스템 배치 스크립트 실행 ② 통합 계정관리(IAM) 시스템 1. 본사·협력업체 인력 계정 통합 등록 2. IAM 시스템이 AD, 클라우드, ERP, 개인정보시스템에 계정 생성·수정·폐기 동기화 ③ 퇴직 프로세스 내 공유 1. HRMS "퇴직예정" 등록 시 IT·보안·개인정보팀 자동 알림

2. 퇴직 확정 시 API/배치로 계정 비활성화 및 자산 반납 요청

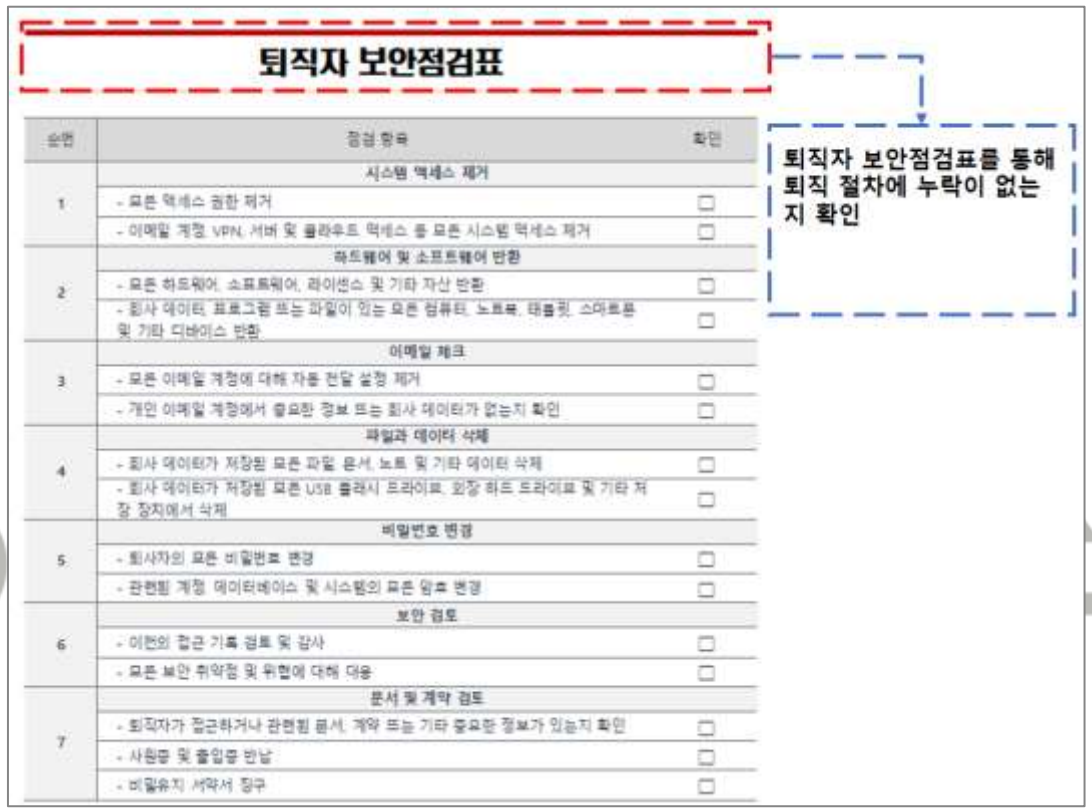
3. 각 부서 완료 확인 후 HRMS "퇴직완료" 상태 변경

◇ 조직 내 인력(임직원, 임시직원, 외주용역직원 등)의 퇴직 또는 직무변경 시 지체 없는 정보자산 반납, 접근권한 회수·조정, 결과 확인 등의 절차를 수립·이행하고 있는가?

(예시) 퇴직자 확인 절차 마련

「**인적보안 관리지침**」 제 ○○조 (퇴직 및 계약해지 시)

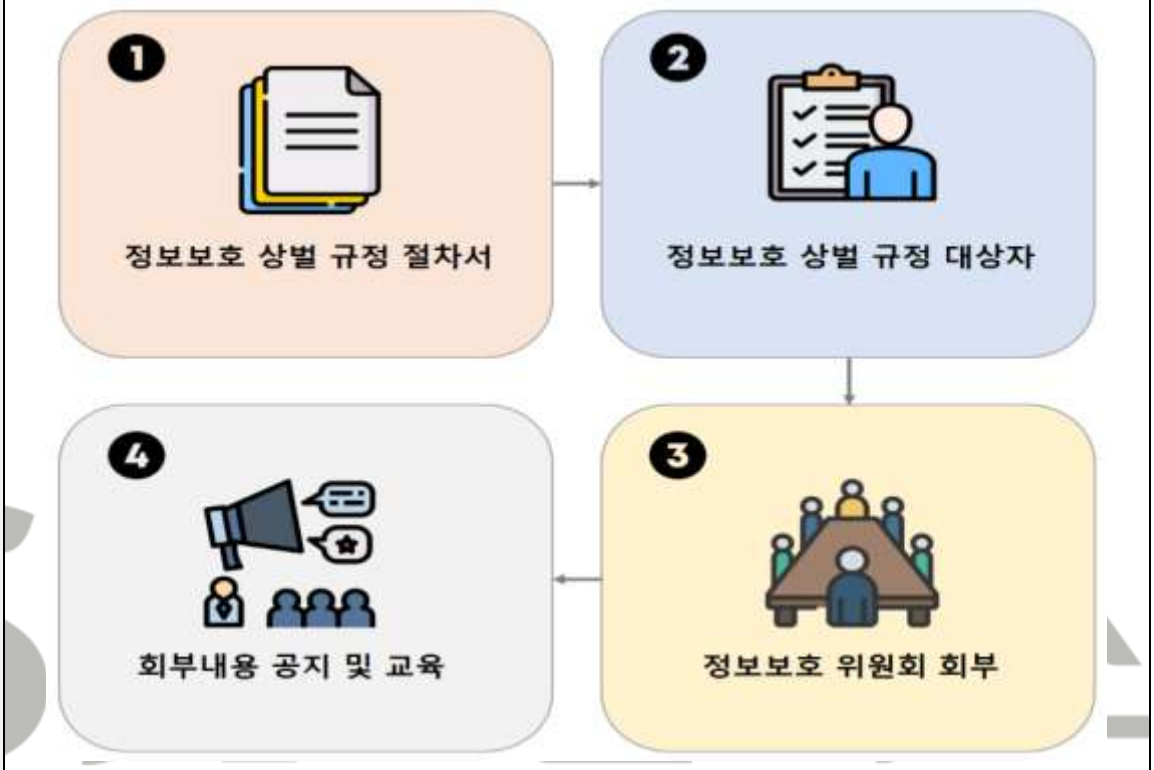
① 퇴직자는 재직 중 보유한 모든 정보자산을 반환할 의무가 있으며, 보안담당자는 "퇴직자 보안점검표"를 이용해 처리결과를 확인해야 한다.



순번	점검 항목	확인
1	시스템 액세스 제거	
	- 모든 액세스 권한 제거	☐
	- 이메일 계정, VPN, 서버 및 클라우드 액세스 등 모든 시스템 액세스 제거	☐
2	하드웨어 및 소프트웨어 반환	
	- 모든 하드웨어, 소프트웨어, 라이센스 및 기타 자산 반환	☐
	- 회사 데이터, 프로그램 또는 파일이 있는 모든 컴퓨터, 노트북, 태블릿, 스마트폰 및 기타 디바이스 반환	☐
3	이메일 체크	
	- 모든 이메일 계정에 대해 자동 전달 설정 제거	☐
	- 개인 이메일 계정에서 중요한 정보 또는 회사 데이터가 없는지 확인	☐
4	파일과 데이터 삭제	
	- 회사 데이터가 저장된 모든 파일, 문서, 노트 및 기타 데이터 삭제	☐
	- 회사 데이터가 저장된 모든 USB 플래시 드라이브, 외장 하드 드라이브 및 기타 저장 장치에서 삭제	☐
5	비밀번호 변경	
	- 퇴사자의 모든 비밀번호 변경	☐
	- 관련된 계정, 데이터베이스 및 시스템의 모든 암호 변경	☐
6	보안 검토	
	- 이전의 접근 기록 검토 및 감사	☐
	- 모든 보안 취약점 및 위협에 대해 대응	☐
7	문서 및 계약 검토	
	- 퇴직자가 접근하거나 관련된 문서, 계약 또는 기타 중요한 정보가 있는지 확인	☐
	- 사원증 및 출입증 반납	☐
	- 비밀유지 서약서 징구	☐

※ 퇴직자 보안점검표 (이해를 돕기 위한 예시)

2.2.6 보안 위반 시 조치

세부분야	2.2.6 보안 위반 시 조치
인증 기준	임직원 및 관련 외부자가 법령, 규제 및 내부정책을 위반한 경우 이에 따른 조치 절차를 수립·이행하여야 한다.
주요 확인사항	• 임직원 및 관련 외부자가 법령과 규제 및 내부정책에 따른 정보보호 및 개인정보보호 책임과 의무를 위반한 경우에 대한 처벌 규정을 수립하고 있는가? • 정보보호 및 개인정보보호 위반 사항이 적발된 경우 내부 절차에 따른 조치를 수행하고 있는가?
기준 요약도	
운영 방안	**◇ 임직원 및 관련 외부자가 법령과 규제 및 내부정책에 따른 정보보호 및 개인정보보호 책임과 의무를 위반한 경우에 대한 처벌 규정을 수립하고 있는가?** **(예시) 처벌 규정 수립** 「**인사 규정**」 제 ○○조 (처벌 기준) ① 임직원 및 관련 외부자가 정보보호·개인정보보호 관련 법령・규제・내부정책상의 책임과 의무를 위반할 경우의 하기의 징계 및 민・형사 책임을 진다. 1. 고객정보·민감정보 유출 또는 변조, 보안장비 우회·무단 변경, 내부통제 절차 고의적 무력화 등 고의 또는 중대한 과실로 인한 위반 2. 보안절차 미준수, 알림 등 의무 불이행으로 인한 경미 사고 ② 위반 시 인사위원회 심의결과에 따른 처벌을 받는다.

1. 직위 해제 후 해고 또는 최소 정직 3개월
2. 손해배상 청구 및 민·형사 고발
3. 서면 경고 또는 감봉(1~3개월)
4. 보안교육 재이수명령 등

◇ 정보보호 및 개인정보보호 위반 사항이 적발된 경우 내부 절차에 따른 조치를 수행하고 있는가?

내부 절차에 따른 조치 내용 기록 및 전파

① 상벌 규정에 따른 분류
1. 위반 등급 판정 : 고의·중대한 과실, 일반 과실, 경미 위반 등으로 분류
2. 분류에 따른 징계 조치

② 결과 기록
1. 인사위원회 회의록, 징계 결정서, 고발장 등 증빙 문서를 전산 인사시스템 및 문서관리시스템 등에 보관
2. 관련자 이력에 징계 내역을 등록하여 향후 평가에 반영

③ 전사 공지 및 교육 사례 활용
1. 사례 선정 및 요약 : 중대한 위반사례 중 핵심 위반 유형과 조치 과정을 익명화하여 요약
2. 전사 공지 : 정기 보안 뉴스레터, 사내 인트라넷, 메일링 리스트 등을 통해 전 직원에게 공유. 위반 원인, 발생 경위, 조치 결과, 재발 방지 대책 포함
3. 교육 자료 반영 : 보안·개인정보보호 정기 교육 커리큘럼에 사례 반영 등

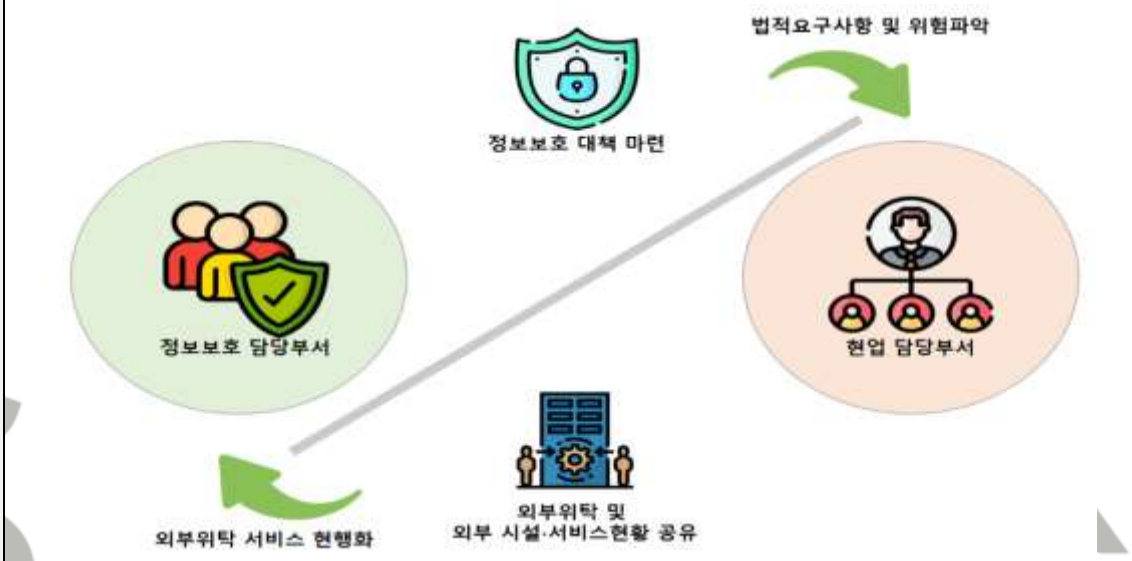
00.00 인사위원회 심의 결과

심의 일시	2025년 9월 20일 14:00
장소	본사 3층 대회의실
참석 위원	홍보안 이사(위원장), 박인사 팀장(인사부서장), 이현 변호사(법무팀장), 김보안 부장(정보보호팀장), 이정노무 노무사(외부 전문가)
피심의자	A팀 OOO **(공지 시 개인정보를 기재하면 안됨)**
적발 내용	타사 영업을 목적으로 내부 고객정보(주민등록번호 포함)를 개인 이메일(상용 이메일)로 전송 (DLP 알림 적발)
위반 유형	고의·중대한 과실 위반
징계 수준	해고
민·형사 고발 여부	진행 (개인정보보호법 제75조 위반)
손해배상 청구	회사 내부 손해액 조사 후 배상 청구 검토
교육 및 개선 조치	피심의자 소속부서 보안·개인정보 보호 재교육 명령
후속 조치	- 인사부서: 징계 통보 공문 발송 및 인사기록 반영 - 법무팀: 민·형사 고발 절차 개시 및 손해액 산정 - 정보보호팀: 전사 보안교육 사례 공유 - 개선 방안: DLP 정책 강화 및 이메일 모니터링 확대

※인사위원회 심의결과/회의록 (이해를 돕기 위한 예시)

2.3 외부자 보안

2.3.1 외부자 현황 관리

세부분야	2.3.1 외부자 현황 관리
인증 기준	업무의 일부(개인정보취급, 정보보호, 정보시스템 운영 또는 개발 등)를 외부에 위탁하거나 외부의 시설 또는 서비스(직접정보통신시설, 클라우드 서비스, 애플리케이션 서비스 등)를 이용하는 경우 그 현황을 식별하고 법적 요구사항 및 외부 조직·서비스로부터 발생되는 위험을 파악하여 적절한 보호 대책을 마련하여야 한다.
주요 확인사항	• 관리체계 범위 내에서 발생하고 있는 업무 위탁 및 외부 시설·서비스의 이용 현황을 식별하고 있는가? • 업무 위탁 및 외부 시설·서비스의 이용에 따른 법적 요구사항과 위험을 파악하고 적절한 보호 대책을 마련하고 있는가?
기준 요약도	
운영 방안	**◇ 관리체계 범위 내에서 발생하고 있는 업무 위탁 및 외부 시설·서비스의 이용 현황을 식별하고 있는가?** **(예시) 업무위탁 유형** ① 운영 용역 1. 업무망 내 시스템 네트워크 및 보안 장비 운영 2. 기업 내부망에 대한 취약점점검 및 모의해킹 ② 유지보수 용역 1. 업무망에 온라인 접속권한으로 수행된 업무에 대한 유지보수 2. 기업 내 온라인으로 진행되는 시스템 네트워크 및 IT보안장비 유지보수 3. IT 외주업체 내에서 운영되는 시스템 네트워크 및 보안장비 유지보수 4. 원격시스템 네트워크 및 보안장비 유지보수

5. 원격 유지보수 및 장애 관리

③ SI 용역

1. IT 업무지원 시스템 개발 구축

④ 데이터처리 용역

1. 기업 내의 헬프데스크 운영

2. 기업 내부데이터를 활용한 대리점 운영

⑤ 오프라인 지원

1. 오프라인으로 출력된 산출물을 관리하는 용역업체

2. 오프라인으로 출력된 내부데이터를 활용하여 면담으로 진행되는 정보보호컨설팅

3. 오프라인으로 출력된 내부데이터를 활용하여 진행되는 기업 회계감사 및 보안컨설팅

위탁사업 운영 현황

위탁 사업명	수탁사명	중요·개인정보취급자	위탁업무	계약 시작일	계약 종료일	중요도	부서	담당자	담당자 연락처
OOO 포털 시스템 운영	㈜OOO 주식회사	4명	정보시스템 운영	2022-01-01	2022-12-31	상	IT전략기획팀	김OO	010-1234-5678
쇼핑몰 고객상담	㈜OOO 콜센터	20명	고객 상담	2022-01-01	2022-12-31	상	고객가치팀	이OO	010-9874-5632

※ 업무위탁현황표 (이해를 돕기 위한 예시)

◇ 업무 위탁 및 외부 시설·서비스의 이용에 따른 법적 요구사항과 위험을 파악하고 적절한 보호 대책을 마련하고 있는가?

위탁사업 법적 요구사항 및 위험 파악

① 개인정보 처리업무 위탁에 해당되는지 확인

② 개인정보 등의 국외 이전에 해당되는지 확인

③ 개인정보보호법, 정보통신망법 등 관련된 법적 요구사항 파악

④ 법적 요구사항을 포함하여 업무 위탁 및 외부 시설·서비스 이용에 따른 위험평가

⑤ 위험평가 결과를 반영하여 적절한 보호 대책 마련 및 이행

2.3.2 외부자 계약 시 보안

<table>
<tr><th>세부분야</th><th>2.3.2 외부자 계약 시 보안</th></tr>
<tr><td>인증
기준</td><td>외부 서비스를 이용하거나 외부자에게 업무를 위탁하는 경우 이에 따른 정보보호 및
개인정보보호 요구사항을 식별하고, 관련 내용을 계약서 또는 협정서 등에 명시하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 중요정보 및 개인정보 처리와 관련된 외부 서비스 및 위탁 업체를 선정하는 경우
정보보호 및 개인정보보호 역량을 고려하도록 절차를 마련하고 있는가?
• 외부 서비스 이용 및 업무 위탁에 따른 정보보호 및 개인정보보호 요구사항을
식별하고 이를 계약서 또는 협정서에 명시하고 있는가?
• 정보시스템 및 개인정보처리시스템 개발을 위탁하는 경우 개발 시 준수하여야 할
정보보호 및 개인정보보호 요구사항을 계약서에 명시하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 중요정보 및 개인정보 처리와 관련된 외부 서비스 및 위탁 업체를 선정하는 경우 정보보호 및 개인정보보호 역량을 고려하도록 절차를 마련하고 있는가?

보안 요구사항 제안요청서(RFP) 명시
① 정보보호 및 개인정보보호 역량이 있는 업체가 선정될 수 있도록 관련 요건을
제안요청서(RFP) 및 제안 평가항목에 반영하여 업체 선정 시 적용</td></tr>
</table>

수탁자 개인정보 보호 역량 분석 평가 지표(예시)		
평가 지표		
관리적 보호 수준	내부관리계획을 수립하고 정기적으로 현행화	
	개인정보처리시스템에 대한 정기적인 위험평가 실시	
	개인정보취급자에 대한 보안 각서 징구 및 개인정보보호 교육 실시	
기술적 보호 수준	물리적·기술적 보호조치를 마련	
	개인정보처리시스템에 침입차단 및 침입탐지 시스템 구축	
	개인정보처리시스템에 대한 접근 권한 및 접근 이력 관리	
물리적 보호 수준	주요 개인정보 처리 관련 설비에 대한 보호구역 지정 및 관리	
	개인정보처리시스템에 대한 출입통제, 보안, 저장매체 등 관리	
	개인정보취급자의 업무 환경에서 개인정보 보호를 위한 보안 관리 등 실시 여부 정기 점검	
기타	PIMS 등 정보보호 및 개인정보보호 인증 획득 여부	
※ 해당 지표는 예시로, 사용 시 각 위·수탁자의 사정에 맞게 수정 활용 가능		

위탁자는 수탁자의 개인정보 보호 역량을 종합적으로 검토하여 개인정보 위험을 최소화 할 수 있는자를 선정 해야한다.

※ 출처: 개인정보 처리 위·수탁 안내서 (개인정보보호위원회·KISA)

◇ 외부 서비스 이용 및 업무 위탁에 따른 정보보호 및 개인정보보호 요구사항을 식별하고 이를 계약서 또는 협정서에 명시하고 있는가?

위탁 또는 외부 서비스 이용 시 보안 요구사항 계약서 반영

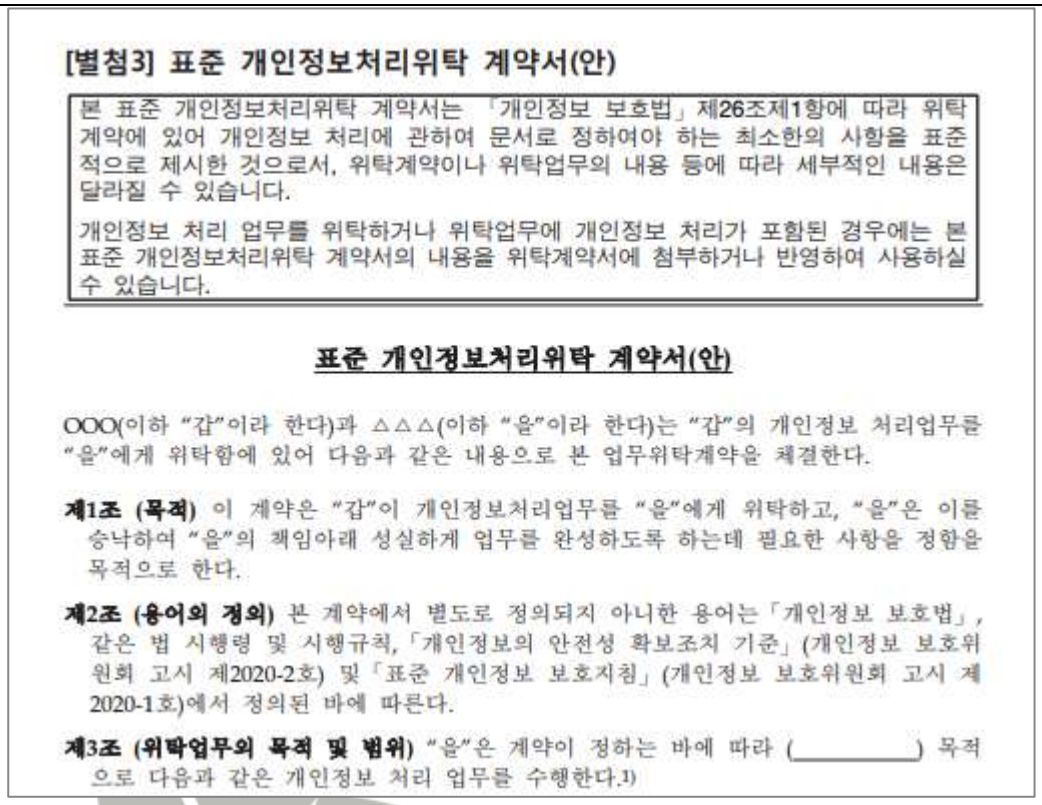
① 위탁 업무 수행 직원 대상 주기적인 정보보호 교육 수행 및 주기적 보안점검 수행

② 업무수행 관련 취득한 중요정보 유출 방지 대책

③ 외부자 인터넷 접속 제한, 물리적 보호조치(장비 및 매체 반출입 등), PC 등 단말 보안(백신 설치, 안전한 패스워드 설정 및 주기적 변경, 화면보호기 설정 등), 무선 네트워크 사용 제한

④ 정보시스템 접근 허용 시 과도한 권한이 부여되지 않도록 접근권한 부여 및 해지 절차

⑤ 재위탁 제한 및 재위탁이 필요한 경우의 절차와 보안 요구사항 정의, 보안 요구사항 위반 시 처벌, 손해배상 책임, 보안사고 발생에 따른 보고 의무 등



[별첨3] 표준 개인정보처리위탁 계약서(안)

본 표준 개인정보처리위탁 계약서는 「개인정보 보호법」 제26조제1항에 따라 위탁계약에 있어 개인정보 처리에 관하여 문서로 정하여야 하는 최소한의 사항을 표준적으로 제시한 것으로서, 위탁계약이나 위탁업무의 내용 등에 따라 세부적인 내용은 달라질 수 있습니다.

개인정보 처리 업무를 위탁하거나 위탁업무에 개인정보 처리가 포함된 경우에는 본 표준 개인정보처리위탁 계약서의 내용을 위탁계약서에 첨부하거나 반영하여 사용하실 수 있습니다.

표준 개인정보처리위탁 계약서(안)

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

제1조 (목적) 이 계약은 "갑"이 개인정보처리업무를 "을"에게 위탁하고, "을"은 이를 승낙하여 "을"의 책임아래 성실하게 업무를 완성하도록 하는데 필요한 사항을 정함을 목적으로 한다.

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

제3조 (위탁업무의 목적 및 범위) "을"은 계약이 정하는 바에 따라 (_____) 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.1)

※ 출처: 개인정보 처리 위·수탁 안내서(개인정보보호위원회·KISA)

◇ 정보시스템 및 개인정보처리시스템 개발을 위탁하는 경우 개발 시 준수하여야 할 정보보호 및 개인정보보호 요구사항을 계약서에 명시하고 있는가?

(예시) 업무 위탁 보안 요구사항 계약 시 반영

「**인적 보안지침**」 제 ○○조 (외부위탁 계약 시 보안 요구사항)

① 외부위탁 계약 시 사전에 요구되는 보안사항을 점검하여야 한다.

② 외부위탁 계약 시 정보시스템, 네트워크, 인력 및 사무환경 등을 관리 통제하기 위한 보안 요구사항을 계약서에 명시하여야 한다

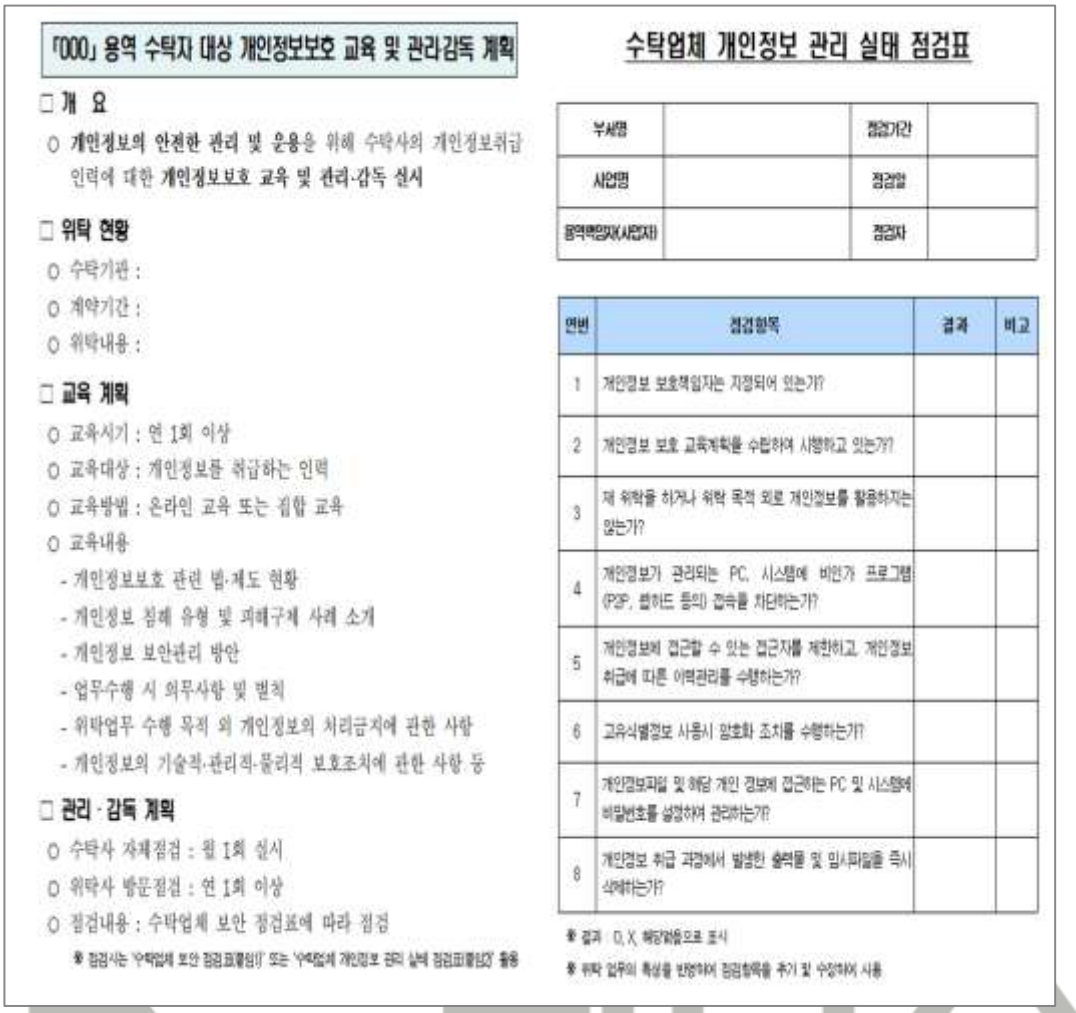
③ 계약사항에는 보안 요구사항에 대한 위반 시 처벌 및 손해배상에 대한 조항이 포함되어야 한다.

④ 외부인 계약 시 계약서에는 외부인의 보안준수와 관련된 내용이 반드시 포함되어야 하며, 계약서를 사전에 작성하여 정보보호최고책임자와 협의하여야 한다.

2.3.3 외부자 보안 이행 관리

세부분야	2.3.3 외부자 보안 이행 관리
인증 기준	계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보보호 요구사항에 따라 외부자의 보호 대책 이행 여부를 주기적인 점검 또는 감사 등 관리·감독하여야 한다.
주요 확인사항	• 외부자가 계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보보호 요구사항을 준수하고 있는지 주기적으로 점검 또는 감사를 수행하고 있는가? • 외부자에 대한 점검 또는 감사 시 발견된 문제점에 대하여 개선 계획을 수립·이행하고 있는가? • 개인정보 처리업무를 위탁받은 수탁자가 관련 업무를 제3자에게 재위탁하는 경우 위탁자의 동의를 받도록 하고 있는가?
기준 요약도	
운영 방안	**◇ 외부자가 계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보보호 요구사항을 준수하고 있는지 주기적으로 점검 또는 감사를 수행하고 있는가?** **(예시) 외부자 정보보호 및 개인정보보호 요구사항 준수 주기적 검토** 「**인적 보안지침**」 제 ○○조 (외부자 보안관리) ① 외부 위탁 시행 시 기밀사항이나 고객정보에 관한 사항을 접할 수 있는 경우, 외부인으로부터 보안유지 및 책임에 관한 '비밀유지 서약서'를 징구하여야 한다. ② 정보보호 최고책임자는 1개월 이상 상주하는 외부인력을 대상으로 주기적으로 보안준수 여부를 검사하여야 한다.

③ 외부인력을 교육하고 감독한 결과 또는 이를 입증할 수 있는 관련 자료 등을 기록·보관한다.



「000」 용역 수탁자 대상 개인정보보호 교육 및 관리감독 계획

□ 개 요

○ 개인정보의 안전한 관리 및 운용을 위해 수탁사의 개인정보취급 인력에 대한 개인정보보호 교육 및 관리·감독 실시

□ 위탁 현황

○ 수탁기관 :
○ 계약기간 :
○ 위탁내용 :

□ 교육 계획

○ 교육시기 : 연 1회 이상
○ 교육대상 : 개인정보를 취급하는 인력
○ 교육방법 : 온라인 교육 또는 집합 교육
○ 교육내용
- 개인정보보호 관련 법·제도 현황
- 개인정보 침해 유형 및 피해구제 사례 소개
- 개인정보 보안관리 방안
- 업무수행 시 의무사항 및 벌칙
- 위탁업무 수행 목적 외 개인정보의 처리금지에 관한 사항
- 개인정보의 기술적·관리적·물리적 보호조치에 관한 사항 등

□ 관리·감독 계획

○ 수탁사 자체점검 : 월 1회 실시
○ 위탁사 방문점검 : 연 1회 이상
○ 점검내용 : 수탁업체 보안 점검표에 따라 점검

※ 점검시는 '수탁업체 보안 점검표(붙임1)' 또는 '수탁업체 개인정보 관리 실태 점검표(붙임2)' 활용

수탁업체 개인정보 관리 실태 점검표

부서명		점검기간	
사업명		점검일	
용역책임자(사업자)		점검자	

연번	점검항목	결과	비고
1	개인정보 보호책임자는 지정되어 있는가?		
2	개인정보 보호 교육계획을 수립하여 시행하고 있는가?		
3	제 위탁을 하거나 위탁 목적 외로 개인정보를 활용하지는 않는가?		
4	개인정보가 관리되는 PC, 시스템에 비인가 프로그램(P2P, 웹하드 등의) 접속을 차단하는가?		
5	개인정보에 접근할 수 있는 접근자를 제한하고, 개인정보 취급에 따른 이력관리를 수행하는가?		
6	고유식별정보 사용시 암호화 조치를 수행하는가?		
7	개인정보파일 및 해당 개인 정보에 접근하는 PC 및 시스템에 비밀번호를 설정하여 관리하는가?		
8	개인정보 취급 과정에서 발생한 출력물 및 임시파일을 즉시 삭제하는가?		

※ 결과 : O, X, 해당없음으로 표시

※ 위탁 업무의 특성을 반영하여 점검항목을 추가 및 수정하여 사용

※ 출처: 개인정보 내부 관리계획 및 처리 위탁 계약서 교육자료 (KISA)

◇ 외부자에 대한 점검 또는 감사 시 발견된 문제점에 대하여 개선 계획을 수립·이행하고 있는가?

발견된 문제점에 대하여 개선 계획을 수립·이행

① 점검 및 감사 결과에 대하여 공유하고 발견된 문제점에 대한 개선방법 및 재발방지 대책을 수립하여 이행

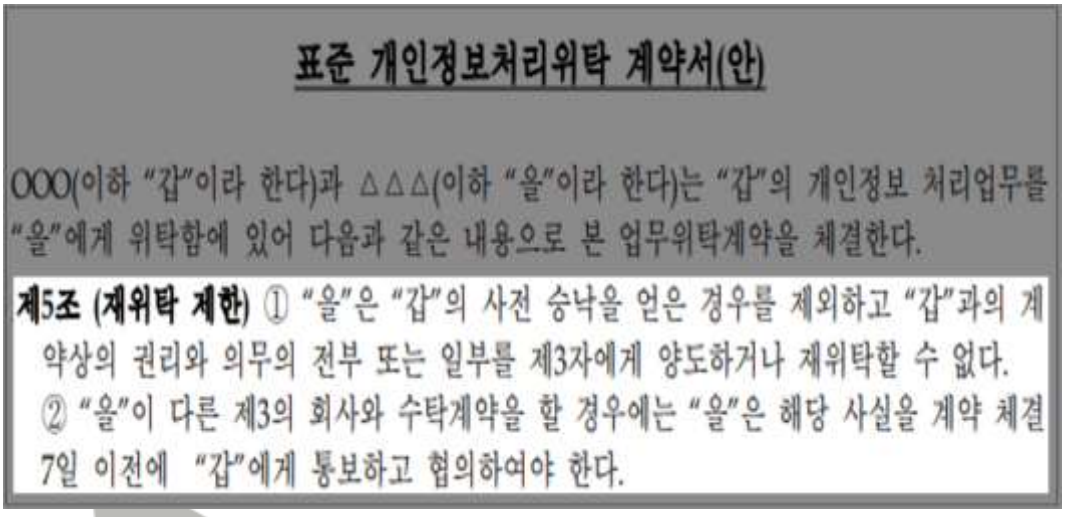
② 개선 조치 완료 여부에 대한 이행점검 수행

◇ 개인정보 처리업무를 위탁받은 수탁자가 관련 업무를 제3자에게 재위탁하는 경우 위탁자의 동의를 받도록 하고 있는가?

재위탁 관리감독 사항

① 개인처리방침 재위탁에 대한 위탁자 승인

1. 수탁자는 위탁받은 개인정보의 처리 업무를 제3자에게 다시 위탁하려는 경우에는 반드시 위탁자의 동의를 받아야 함



표준 개인정보처리위탁 계약서(안)

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

제5조 (재위탁 제한) ① "을"은 "갑"의 사전 승낙을 얻은 경우를 제외하고 "갑"과의 계약상의 권리와 의무의 전부 또는 일부를 제3자에게 양도하거나 재위탁할 수 없다.
② "을"이 다른 제3의 회사와 수탁계약을 할 경우에는 "을"은 해당 사실을 계약 체결 7일 이전에 "갑"에게 통보하고 협의하여야 한다.

※ 출처: 개인정보 처리 위수탁 안내서 (정보보호 위원회·KISA)

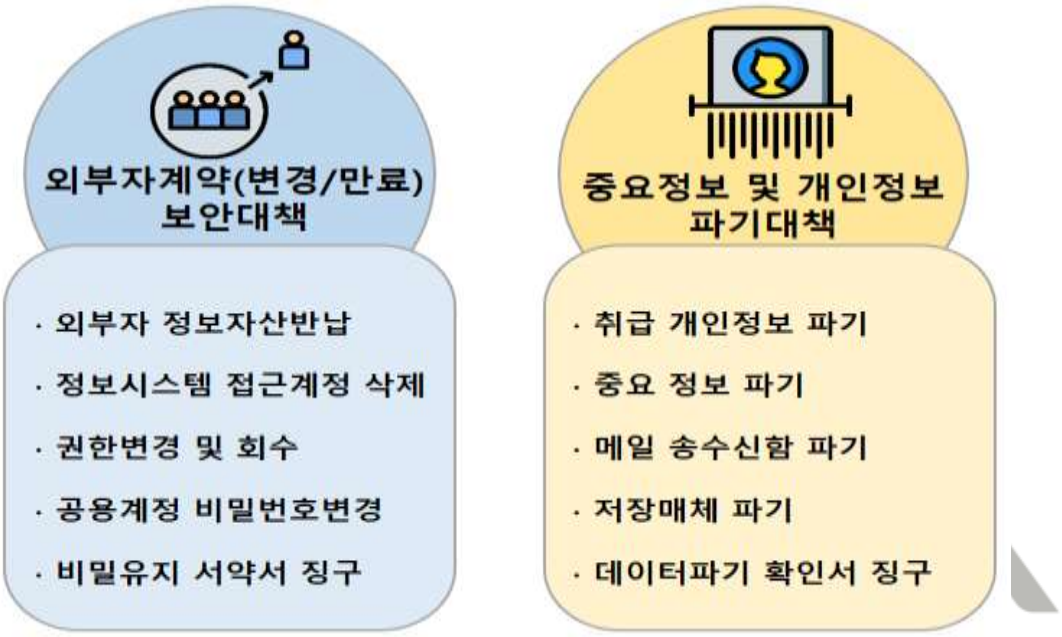
② 재위탁자 관리감독 의무에 관한 사항

1. 위탁자는 재수탁자를 교육하고 개인정보 처리 현황을 감독할 의무가 있음
2. 위탁자는 재위탁하는 업무의 내용과 재수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 공개해야 함

③ 재위탁 동의 및 관리 절차

1. 재위탁 이전에 위탁자에게 서면 또는 전자문서로 통보
2. 재위탁 사유와 재수탁자 정보 포함(재위탁 업무 목적·범위, 재수탁자 정보, 개인정보 항목, 보호조치 계획 등 기재)
4. 위탁자에게 동의서 전달
5. 위탁자 검토 및 승인(재수탁자의 적격성 및 보호조치 검토)
6. 추가 자료 요청 후 동의 여부를 서면으로 통보
7. 재위탁 현황 대장에 등록·관리

2.3.4 외부자 계약 변경 및 만료 시 보안

<table>
<tr><th>세부분야</th><th>2.3.4 외부자 계약 변경 및 만료 시 보안</th></tr>
<tr><td>인증
기준</td><td>외부자 계약만료, 업무 종료, 담당자 변경 시에는 제공한 정보자산 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 업무 수행 중 취득정보의 비밀유지 확약서 징구 등의 보호대책을 이행하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 외부자 계약만료, 업무 종료, 담당자 변경 시 공식적인 절차에 따른 정보자산 반납, 정보시스템 접근계정 삭제, 비밀유지 확약서 징구 등이 이루어질 수 있도록 보안대책을 수립·이행하고 있는가?
• 외부자 계약 만료 시 위탁 업무와 관련하여 외부자가 중요정보 및 개인정보를 보유하고 있는지 확인하고 이를 회수·파기할 수 있도록 절차를 수립·이행하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 외부자 계약만료, 업무 종료, 담당자 변경 시 공식적인 절차에 따른 정보자산 반납, 정보시스템 접근계정 삭제, 비밀유지 확약서 징구 등이 이루어질 수 있도록 보안대책을 수립·이행하고 있는가?

(예시) 외부자 계약 변경 및 만료 시 보안대책 수립
「인적 보안지침」 제 ○○조 (외부자 계약해지)
① 사업완료 후 생산되는 최종 산출물 중 대외보안이 요구되는 자료는 대외비로 작성·관리하고 불필요한 자료는 삭제 및 세단 후 폐기한다.
② 아웃소싱 업체에 제공한 제반자료, 장비 서류와 중간·최종 산출물 등 제반자료는 전량 회수하고 아웃소싱 업체에 복사본 등의 별도 보관을 금지한다.
③ 노트북·보조기억매체 등 전자적으로 기록된 자료는 '정보시스템 저장매체 불용처리 지침'에 따라 보안조치한다.</td></tr>
</table>

④ 아웃소싱 사업 관련자료 회수 및 삭제 조치 후 업체에게 복사본 등 사업관련 자료를 보유하고 있지 않다는 대표 명의 확약서를 징구한다.

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 비공개 부분에 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 O년간 자신을 위해 또는 귀사와 경쟁하는 사업자 그외 제3자를 위해 사용하지 않을 것을 서약합니다.

년 월 일
서약인 인
주식회사 귀중

투입 종료 확인서

1. 기본정보

이름			
소속회사		연 락 처	
근무기간	~	담 당 업 무	

※ 투입 종료 프로세스 안내
1. 아래 점검 사항의 1-4단계 업무를 모두 이행한후, 확인란에 √ 표시를 합니다.
2. 출입 ID카드와 투입종료확인서를 보안담당자에게 제출합니다.
3. 보안담당자는 각 단계별 이행점검을 하고 이행란에 서명을 합니다.

2. 점검사항

내용	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. 물품(스티커) 부착 - 개인사물함의 내용을 비우고 열쇠를 사업장 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 제거를 해야 함	PL/PM

3. 특이사항

년 월 일 작성자 성명: (인)

※ 출처: IT 외주인력 보안통제 안내서 (방송통신위원회)

◇ 외부자 계약 만료 시 위탁 업무와 관련하여 외부자가 중요정보 및 개인정보를 보유하고 있는지 확인하고 이를 회수·파기할 수 있도록 절차를 수립·이행하고 있는가?

중요정보 및 개인정보 보유 확인 및 이를 회수·파기할 수 있도록 절차를 수립

① 개인정보 등 중요정보를 회수·파기하기 위하여 수탁사 직접 방문 또는 원격으로 개인정보를 파기한 후 파기 확약서 작성

② 정보시스템과 담당자 PC뿐 아니라, 메일 송수신함 등 해당 정보가 저장되어 있는 모든 장치 및 매체에 대한 삭제 조치 필요

③ 해당 정보가 복구·재생되지 않도록 안전한 방법으로 파기

2.4 물리 보안

2.4.1 보호구역 지정

<table>
<tr><th>세부분야</th><th>2.4.1 보호구역 지정</th></tr>
<tr><td>인증
기준</td><td>물리적·환경적 위협으로부터 개인정보 및 중요정보, 문서, 저장매체, 주요 설비 및 시스템 등을 보호하기 위하여 통제구역·제한구역·접견구역 등 물리적 보호구역을 지정하고 구역별 보호 대책을 수립·이행하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 물리적·환경적 위협으로부터 개인정보 및 중요정보, 문서, 저장매체, 주요 설비 및 시스템 등을 보호하기 위하여 통제구역, 제한구역, 접견구역 등 물리적 보호구역 지정기준을 마련하고 있는가?
• 물리적 보호구역 지정기준에 따라 보호구역을 지정하고 구역별 보호 대책을 수립·이행하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 

<table>
<tr><th>장소</th><th>출입대상</th><th>출입통제방식</th></tr>
<tr><td>전산실,관제실,
발전실 등</td><td>인가 받은
최소인원</td><td>생체식별정보
특수권한부여</td></tr>
<tr><td>부서별 사무실,
직원 편의시설 등</td><td>임직원 및
상주 근무자</td><td>임시방문증,
사원증 등</td></tr>
<tr><td>접견실, 근린지역 등</td><td>방문자</td><td>제한 없음</td></tr>
</table></td></tr>
<tr><td>운영
방안</td><td>◇ 물리적·환경적 위협으로부터 개인정보 및 중요정보, 문서, 저장매체, 주요 설비 및 시스템 등을 보호하기 위하여 통제구역, 제한구역, 접견구역 등 물리적 보호구역 지정기준을 마련하고 있는가?

물리적 보호구역 지정기준 수립
① 보호구역 분류
1. 통제구역 : 접근 통제가 엄격히 관리되어야 하는 고위험 구역
2. 제한구역 : 출입이 제한되며 일정 권한 이상에만 허용되는 구역
3. 접견구역 : 외부인의 일시적 출입이 허용되나 일정 범위로 제한된 구역
② 위험도 평가
1. 개인정보·중요정보 보유량과 민감도
2. 구역 내 주요 설비·시스템의 중요도 및 연속성 영향도</td></tr>
</table>

3. 과거 보안 사고 이력 및 위협 시나리오 등

③ 접근 빈도 및 사용자 권한

1. 영업·지원·외부방문자 등 사용자 유형별 접근 필요성
2. 24시간 운영 여부, 긴급 출입 요구사항

④ 환경적 요건

1. 화재·수해·지진 등 자연재해 위험도
2. 전력·냉각·환기·배기 설비 현황
3. 유해 물질·소음·분진 노출 위험 등

⑤ 구조적 요건

1. 벽·바닥·천장 재질과 내화·방진 성능
2. 출입문·창문·벽체의 보안 등급
3. CCTV·경보·출입통제장치 설치 가능 여부 등

◇ 물리적 보호구역 지정기준에 따라 보호구역을 지정하고 구역별 보호 대책을 수립·이행하고 있는가?

(예시) 물리적 보호구역별 보호 대책 수립

① 통제구역

1. 출입통제시스템(생체인식·RFID) 설치
2. 24시간 CCTV 모니터링
3. 이중문(Man-trap) 구조 적용
4. 고강도 벽체·방화문·방진 설계
5. 비상전원·화재·누수 감지 센서 배치

② 제한구역

1. 전자출입카드 또는 비밀번호 인증
2. CCTV 설치 및 일정 주기 영상 보관
3. 출입 로그 점검 및 비인가 시 경보
4. 적정 환기·냉각·소방 설비 확보

③ 접견구역

1. 호스트 동반 출입 의무화
2. 방문자 출입증 발급·반납 절차
3. 출입구-사무구역 간 물리적 분리(유리막·가림막)
4. 제한적 CCTV 모니터링(프라이버시 고려)

2.4.2 출입통제

세부분야	2.4.2 출입통제
인증 기준	보호구역은 인가된 사람만이 출입하도록 통제하고 책임 추적성을 확보할 수 있도록 출입 및 접근 이력을 주기적으로 검토하여야 한다.
주요 확인사항	• 보호구역은 출입절차에 따라 출입이 허가된 자만 출입하도록 통제하고 있는가? • 각 보호구역에 대한 내·외부자 출입 기록을 일정기간 보존하고 출입 기록 및 출입 권한을 주기적으로 검토하고 있는가?
기준 요약도	
운영 방안	**◇ 보호구역은 출입 절차에 따라 출입이 허가된 자만 출입하도록 통제하고 있는가?** **내·외부자 출입통제 절차 마련** ① 보호구역별로 출입 가능한 부서·직무·업무를 정의, 출입 권한이 부여된 임직원을 식별하고 그 현황을 관리 ② 통제구역의 경우 업무 목적에 따라 최소한의 인원만 출입할 수 있도록 통제 ③ 출입 절차: 출입 신청, 책임자 승인, 출입 권한 부여 및 회수, 출입 내역 기록, 출입 기록 정기적 검토 등 ④ 출입통제 장치 설치: 비밀번호 기반, ID카드 기반, 생체정보 기반 등 ⑤ 출입통제 절차 수립·운영: 출입자 등록·삭제, 출입권한 관리, 방문자 관리, 출입대장 관리 등

※ 출처: ADT 출입보안 서비스 (SK쉴더스)

◇ 각 보호구역에 대한 내·외부자 출입 기록을 일정기간 보존하고 출입 기록 및 출입 권한을 주기적으로 검토하고 있는가?

(예시) 출입권한 주기적 검토

① 보존 기간 설정

1. 보호구역(통제·제한·접견)에 대한 내·외부자 출입기록을 최소 1년 이상 보존
2. 법·규제 요구사항에 따라 최대 3년까지 연장 가능

② 기록 항목

1. 출입자 신원(사원번호·이름·회사명)
2. 출입 일시 및 출입구역명
3. 출입 수단(출입카드·생체인식)
4. 입·퇴실 확인

③ 주기적 검토

1. 분기별로 출입기록 및 권한 현황 검토
2. 비인가 출입 여부 및 권한 과다 배정 점검
3. 검토 결과에 따른 권한 조정·제거 및 이상 징후 보고

④ 책임 및 절차

1. 보안운영팀 : 기록 보관 시스템 운영·백업
2. 인사·시설팀 : 권한 부여·해지 이력 관리
3. 정보보호팀 : 검토 절차 수립 및 검토 보고서 승인

⑤ 이상 징후 대응

	1. 비인가 출입 또는 권한 오·남용 발견 시 즉시 조사 2. 사고 발생 시 보안사고 대응 절차에 따라 조치

2.4.3 정보시스템 보호

<table>
<tr><th>세부분야</th><th>2.4.3 정보시스템 보호</th></tr>
<tr><td>인증
기준</td><td>정보시스템은 환경적 위협과 유해요소, 비인가 접근 가능성을 감소시킬 수 있도록 중요도와 특성을 고려하여 배치하고, 통신 및 전력 케이블이 손상을 입지 않도록 보호하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 정보시스템의 중요도, 용도, 특성 등을 고려하여 배치 장소를 분리하고 있는가?
• 정보시스템의 실제 물리적 위치를 손쉽게 확인할 수 있는 방안을 마련하고 있는가?
• 전력 및 통신 케이블을 외부로부터의 물리적 손상 및 전기적 영향으로부터 안전하게 보호하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 정보시스템의 중요도, 용도, 특성 등을 고려하여 배치 장소를 분리하고 있는가?

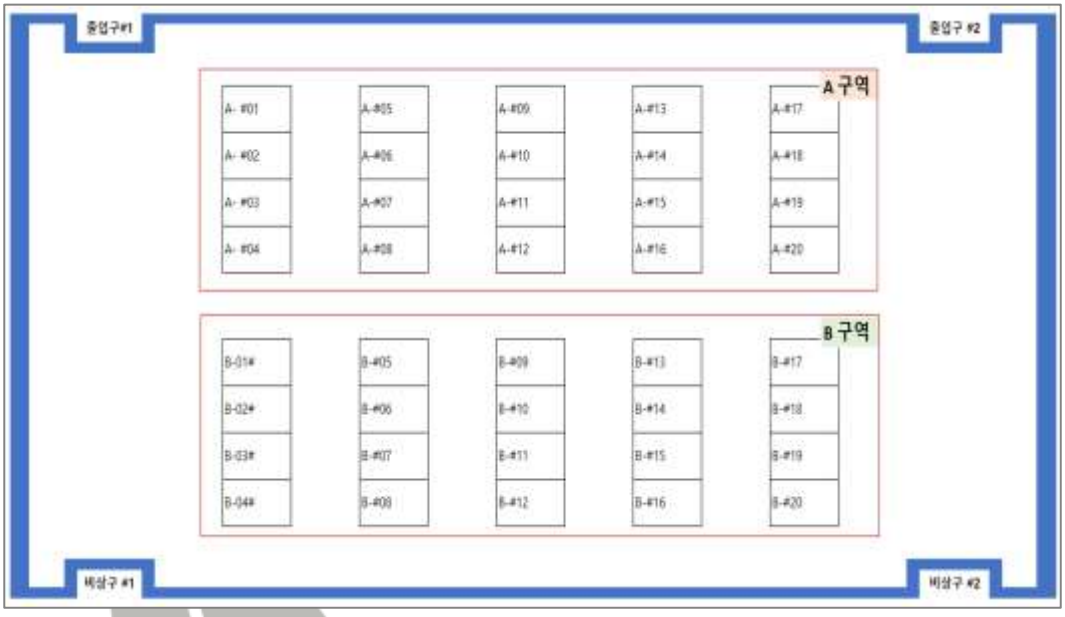
배치 장소 분리를 통한 물리적 보호
① 전산랙을 이용하여 시스템을 외부로부터 보호
② 중요 시스템 잠금 및 별도 물리적 안전장치 보호

◇ 정보시스템의 실제 물리적 위치를 손쉽게 확인할 수 있는 방안을 마련하고 있는가?

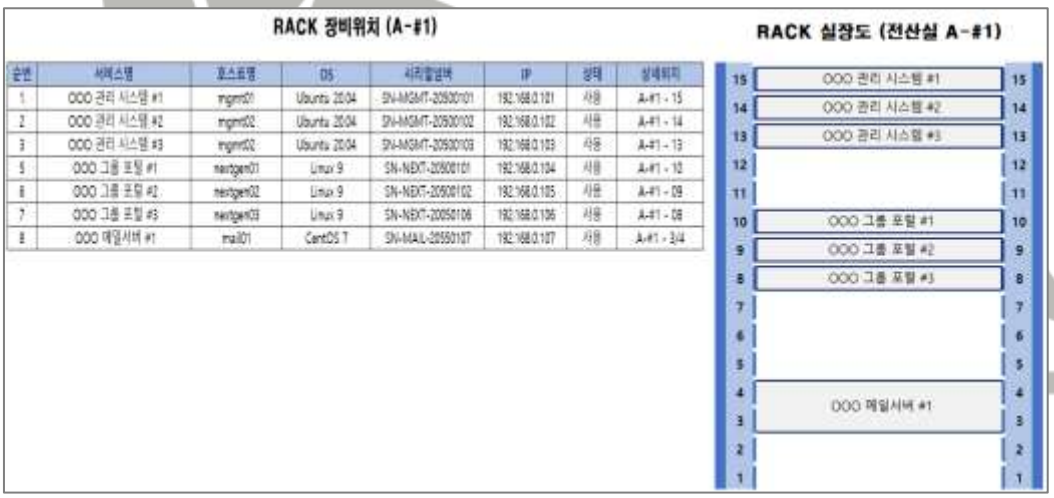
물리적 위치 확인 방안(배치도, 자산 목록 등) 마련
① 보안 사고, 장애 발생 시 신속한 조치를 위한 물리적 배치도 (시설 단면도, 배치도 등),</td></tr>
</table>

자산 목록 전사 관리

② 자산 목록 등에 물리적 위치 항목을 포함하고 현행화하여 최신본 유지



※ 전산실 구조도 (이해를 돕기 위한 예시)



※ 전산실 랙 실장도 (이해를 돕기 위한 예시)

◇ 전력 및 통신 케이블을 외부로부터의 물리적 손상 및 전기적 영향으로부터 안전하게 보호하고 있는가?

전력 및 통신 케이블을 물리적 손상 및 전기적 영향으로부터 안전하게 보호

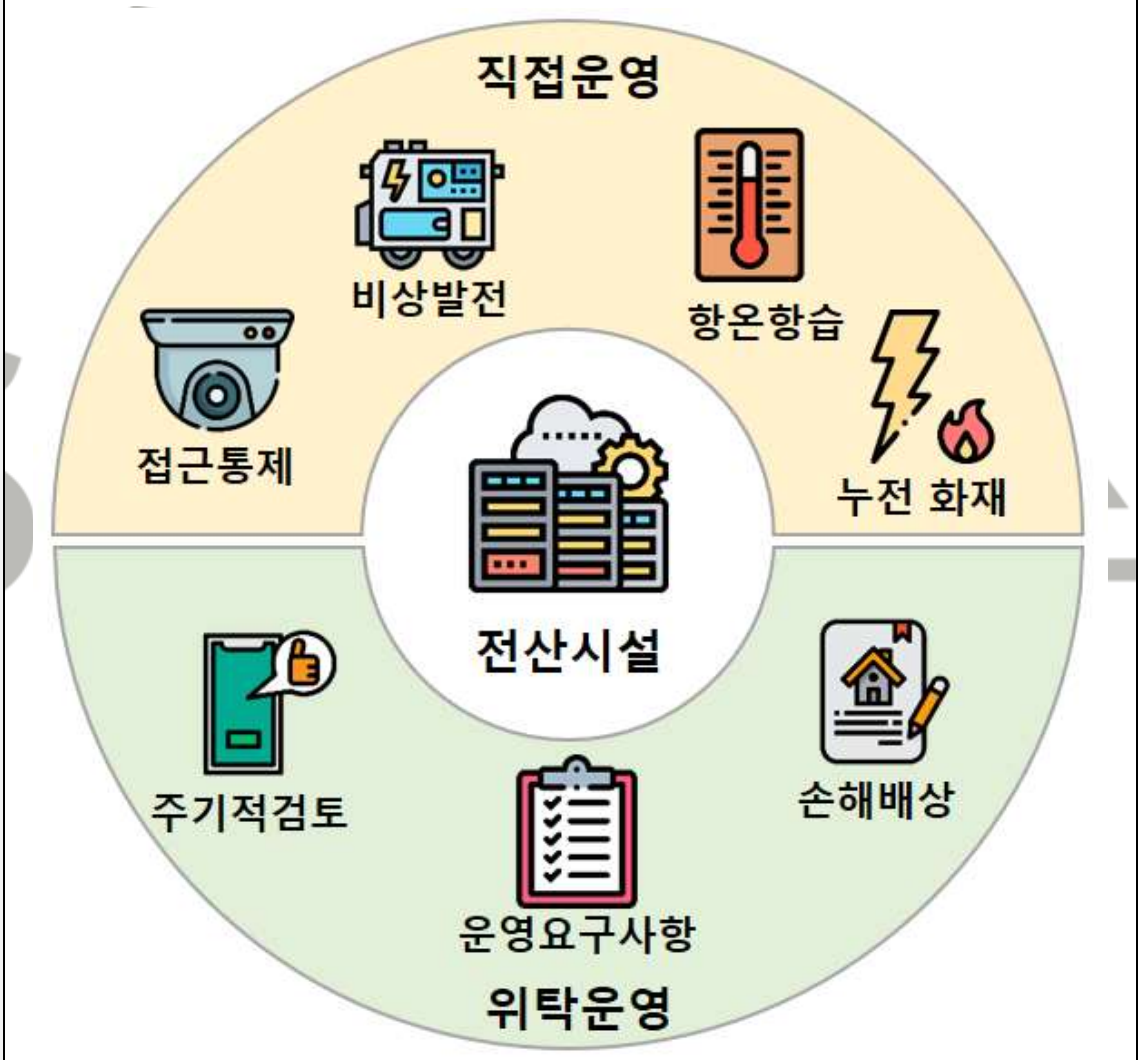
① 물리적으로 구분하여 배선, 식별 표시, 상호 간섭받지 않도록 거리 유지, 케이블 매설 등 조치

1. 전기와 통신 케이블 구분하여 배선

2. 통신 케이블과 전원 케이블은 상호 간섭이 발생하지 않도록 적정한 이격 거리 유지

	3. 출입 기록: 출입자(소속·성명·연락처), 출입 일시, 출입 사유, 출입증 번호, 승인자 ② 배전반, 강전실, 약전실 등에는 인가된 최소한의 인력만 접근할 수 있도록 접근통제 1. 분전반은 시건장치가 있어야 하며 인가된 시설관리자가 열쇠를 관리

2.4.4 보호설비 운영

세부분야	2.4.4 보호설비 운영
인증 기준	보호구역에 위치한 정보시스템의 중요도 및 특성에 맞춰 온·습도 조절, 화재 감지, 소화 설비, 누수 감지, UPS, 비상발전기, 이중전원선 등의 보호설비를 갖추고 운영 절차를 수립·운영하여야 한다.
주요 확인사항	• 각 보호구역의 중요도 및 특성에 따라 화재, 수해, 전력 이상 등 인재 및 자연재해 등에 대비하여 필요한 설비를 갖추고 운영 절차를 수립하여 운영하고 있는가? • 외부 집적정보통신시설(IDC)에 위탁 운영하는 경우 물리적 보호에 필요한 요구사항을 계약서에 반영하고 운영 상태를 주기적으로 검토하고 있는가?
기준 요약도	
운영 방안	◇ 각 보호구역의 중요도 및 특성에 따라 화재, 수해, 전력 이상 등 인재 및

자연재해 등에 대비하여 필요한 설비를 갖추고 운영 절차를 수립하여 운영하고 있는가?

화재, 수해, 전력 이상 등 인재 및 자연재해 등에 대비하여 필요한 설비

① 전기시설: 분전반·UPS·축전기·발전기·접지

② 공조시설: 항온항습기·이중마루

③ 소방시설: 화재감지기·소화설비 등

전 산 실 설 비 점 검 일 지

200 년 월 일

점검항목		9:00	11:00	13:00	15:00	17:00	19:00	21:00	23:00	1:00	3:00	5:00	7:00
항온항습기	설정온도												
	현재온도												
	설정습도												
	현재습도												
	조작판 이벤트												
	냄새나 이상 소음												
누수	누수감지기												
	드레인												
UPS	입력전압												
	입력전류												
	출력전압												
	출력전류												
	항온항습												
	누수여부												
	소화기												
	정리정돈												
	조작판 이벤트												
	냄새나 이상 소음												
발전기	유량												
	소화기												
	정리정돈												
	누수나 누유												
점검자													

※ 출처: 전산실 관리지침 (NIA)

◇ 외부 집적정보통신시설(IDC)에 위탁 운영하는 경우 물리적 보호에 필요한 요구사항을 계약서에 반영하고 운영 상태를 주기적으로 검토하고 있는가?

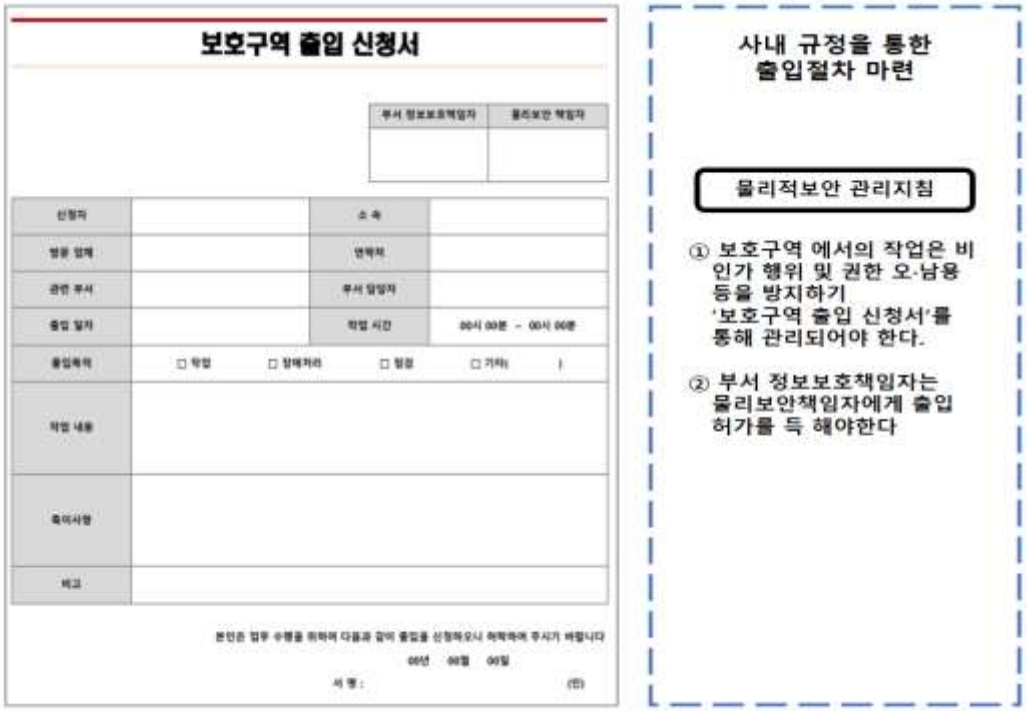
물리적 보호 보안 요구사항 계약서 반영 및 주기적 검토

① 정보보호 관련 법규 준수, 화재, 전력 이상 등 재해·재난 대비, 출입통제, 자산 반출입 통제, 영상감시 등 물리적 보안통제 적용 및 사고 발생 시 손해 배상에 관한 사항 등

② IDC의 책임보험 가입 여부(미가입 시 1천만 원 이하의 과태료 부과) 등

2.4.5 보호구역 내 작업

세부분야	2.4.5 보호구역 내 작업
인증 기준	보호구역 내에서의 비인가 행위 및 권한 오·남용 등을 방지하기 위한 작업 절차를 수립·이행하고, 작업 기록을 주기적으로 검토하여야 한다.
주요 확인사항	• 정보시스템 도입, 유지보수 등으로 보호구역 내 작업이 필요한 경우에 대한 공식적인 작업 신청 및 수행 절차를 수립·이행하고 있는가? • 보호구역 내 작업이 통제 절차에 따라 적절히 수행되었는지 여부를 확인하기 위하여 작업 기록을 주기적으로 검토하고 있는가?
기준 요약도	
운영 방안	**◇ 정보시스템 도입, 유지보수 등으로 보호구역 내 작업이 필요한 경우에 대한 공식적인 작업 신청 및 수행 절차를 수립·이행하고 있는가?** **(예시) 공식적인 작업 신청 및 수행관련 지침 수립** 「**물리적 보안관리 지침**」 제 ○○조 (보호구역 작업통제) ① 보호구역에서의 작업은 비인가 행위 및 권한 오·남용 등을 방지하기 위해 '보호구역 출입 신청서'를 통해 관리되어야 한다. ② 부서 정보보호 담당자는 물리보안 책임자에게 출입 허가를 득해야 한다.



※ 전산실 출입 신청 (이해를 돕기 위한 예시)

◇ 보호구역 내 작업이 통제 절차에 따라 적절히 수행되었는지 여부를 확인하기 위하여 작업 기록을 주기적으로 검토하고 있는가?

(예시) 주기적 검토 실시 및 검토여부 확인

「**물리적 보안관리 지침**」 제 ○○조 (보호구역 작업통제)

① 물리보안 책임자는 '보호구역 출입기록 관리대장'을 작성하고 분기별 1회 각 호에 따라 작업 기록을 검토해야 한다.

1. 작업 검토: 사전 승인 내역, 출입 기록, 작업 기록 등에 대한 정기적 검토 수행 등
2. 검토 방법: 출입 신청서와 출입 내역(관리대장, 시스템 로그 등) 일치성 등

보호구역 출입기록 관리대장

점검 일자 :

일시	출입시간	퇴소시간	작업내용	출입자			입회자			비고
				소속	이름	연락처	소속	이름	서명(인)	

※ 통제구역 출입대장 (이해를 돕기 위한 예시)

2.4.6 반출입 기기 통제

<table>
<tr><th>세부분야</th><th>2.4.6 반출입 기기 통제</th></tr>
<tr><td>인증
기준</td><td>보호구역 내 정보시스템, 모바일 기기, 저장매체 등에 대한 반출입 통제 절차를
수립·이행하고 주기적으로 검토하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 정보시스템, 모바일 기기, 저장매체 등을 보호구역에 반입하거나 반출하는 경우
정보 유출, 악성코드 감염 등 보안사고 예방을 위한 통제 절차를 수립·이행하고 있는가?
• 반출입 통제 절차에 따른 기록을 유지·관리하고, 절차 준수 여부를 확인할 수 있도록
반출입 이력을 주기적으로 점검하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 정보시스템, 모바일 기기, 저장매체 등을 보호구역에 반입하거나 반출하는 경우 정보 유출, 악성코드 감염 등 보안사고 예방을 위한 통제 절차를 수립·이행하고 있는가?

(예시) 반출입 기기 통제 절차 수립

「물리적 보안관리 지침」 제 ○○조 (기기 반출입 통제)
① 통제구역에서의 정보 유출, 악성코드 감염 등 보안 사고를 예방하기 위해 다음과 같이 기기 반출입을 통제하여야 한다.
1. 반출입 통제 대상: 정보시스템(서버, 네트워크 장비 등), 모바일 기기(노트북, 스마트패드, 스마트폰 등), 저장매체(HDD, SSD, USB메모리, 외장하드디스크, CD/DVD, 테이프 등) 등
2. 정보시스템 관리자는 반출입 통제 대상 기기에 대해 보안 점검(백신 설치, 악성코드 검사, 보안 업데이트, 매체 봉인, 자료 유출 여부 등)을 실시한 후 기기 반출입 허용</td></tr>
</table>

반 입 증

발행번호 :　　관리 회사명 :

품 명	규 격	단 위	수 량	비 고

반입회사명 :	차량번호 :		반입자 :	
반 입 사 유 :				
관리회사명 :	담당자		전화번호 :	
상기와 같이 반입을 허가함 200 년 월 일	결제	기 안	심 사	결 정

반 출 증

발행번호 :　　관리 회사명 :

품 명	규 격	단 위	수 량	비 고

반출회사명 :	차량번호 :		반출자 :	
반 출 사 유 :				
관리회사명 :	담당자		전화번호 :	
상기와 같이 반출을 허가함 200 년 월 일	결제	담 당	PM	감독자

※ 출처: 전산실 관리지침(NIA)

◇ 반출입 통제 절차에 따른 기록을 유지·관리하고, 절차 준수 여부를 확인할 수 있도록 반출입 이력을 주기적으로 점검하고 있는가?

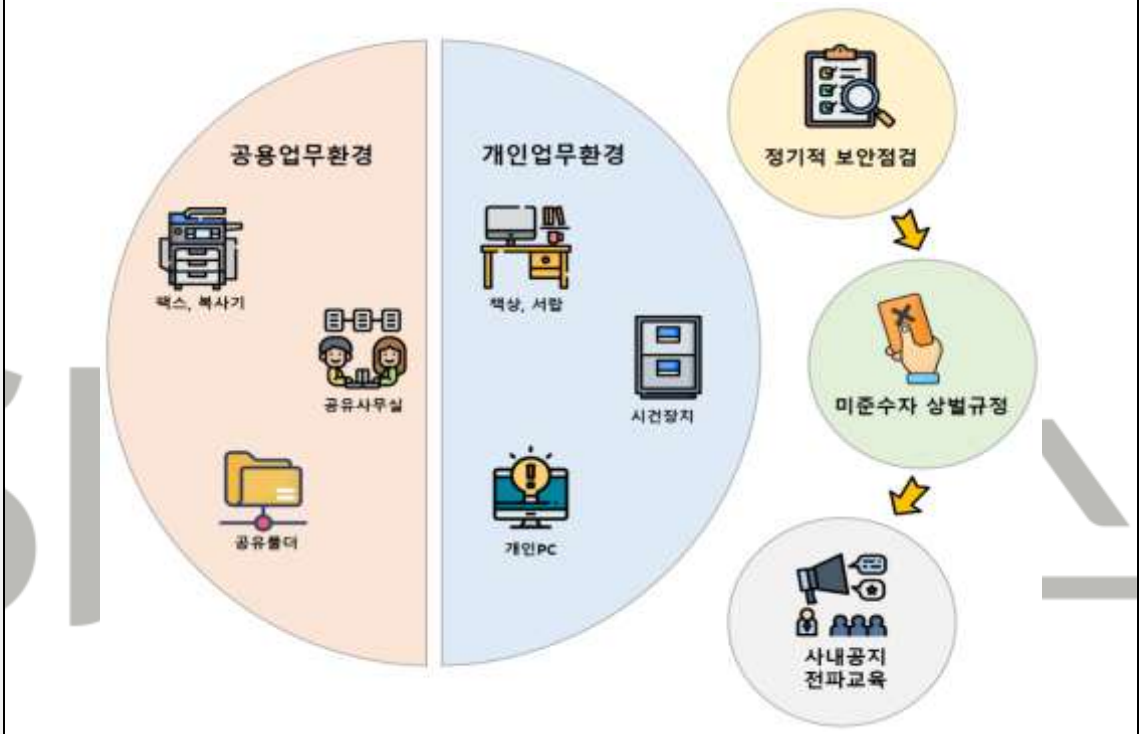
반출입 기기 이력 주기적 관리 검토

① 반출입 통제 절차에 따른 기록을 유지·관리하고, 절차 준수 여부를 확인할 수 있도록 반출입 이력을 주기적으로 점검

1. 보호구역 내 반출입 이력에 대한 기록 유지(반출입 관리대장, 반출입 통제시스템 로그 등)

② 반출입 이력을 주기적으로 점검하여 보호구역 내 반출입이 통제 절차에 따라 적절하게 수행되었는지 여부 검토

2.4.7 업무환경 보안

세부분야	2.4.7 업무환경 보안
인증 기준	공용으로 사용하는 사무용 기기(문서고, 공용 PC, 복합기, 파일서버 등) 및 개인 업무환경(업무용 PC, 책상 등)을 통하여 개인정보 및 중요정보가 비인가자에게 노출 또는 유출되지 않도록 클린데스크, 정기점검 등 업무환경 보호 대책을 수립·이행하여야 한다.
주요 확인사항	• 문서고, 공용 PC, 복합기, 파일서버 등 공용으로 사용하는 시설 및 사무용 기기에 대한 보호 대책을 수립·이행하고 있는가? • 업무용 PC, 책상, 서랍 등 개인업무 환경을 통한 개인정보 및 중요정보의 유·노출을 방지하기 위한 보호 대책을 수립·이행하고 있는가? • 개인정보가 포함된 종이 인쇄물 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 보호 조치를 하고 있는가? • 개인 및 공용 업무환경에서의 정보보호 준수 여부를 주기적으로 검토하고 있는가?
기준 요약도	
운영 방안	**◇ 문서고, 공용 PC, 복합기, 파일서버 등 공용으로 사용하는 시설 및 사무용 기기에 대한 보호 대책을 수립·이행하고 있는가?** **(예시) 공용 환경 보호 대책 수립** ① 접근통제 1. 문서고: 출입카드·비밀번호 잠금, CCTV 설치 2. 공용 PC·복합기: 사용자 인증(AD 연동·OTP), 자동 세션 잠금(이용 후 5분 이내) 3. 파일서버: 네트워크 접근 제어, 최소 권한 원칙으로 공유 폴더 권한 설정

② 데이터 보호

1. 문서고: 중요문서 잠금 캐비닛 보관, 방문자 기록 유지
2. 공용 PC: 로컬 저장 금지, USB 포트 비활성화 또는 제어 소프트웨어 적용
3. 복합기: 출력물 회수 대기함 설치, 출력물 암호화 전송 지원 기종 사용
4. 파일서버: 저장 데이터 암호화(AES-256), 백업본 분리 보관

③ 모니터링 및 로깅

1. 문서고 출입·문서 반출입 기록 관리
2. 공용 PC·파일서버 접속 로그 및 파일 접근 로그 1년 보관
3. 복합기 사용 로그(사용자·시간·문서 유형) 주기적 검토

◇ 업무용 PC, 책상, 서랍 등 개인업무 환경을 통한 개인정보 및 중요정보의 유·노출을 방지하기 위한 보호 대책을 수립·이행하고 있는가?

(예시) 업무환경 보안 보호 대책 수립

「**물리적 보안관리 지침**」 제 ◌◌조 (업무환경 보안점검)

① 업무환경 보안점검 시 '사무실 업무환경 보안점검표'를 활용하여 반기 1회 이상 수행하여야 한다.

② 업무환경 보안점검 결과 중대한 위반사실이 지적되었거나 평가 결과가 부진할 경우에는 「인사규정 시행지침」에 따라 징계할 수 있다.

사무실 업무환경 보안점검표

	개인 PC 보안관리	
1	ID/PWD를 공유하지 않으며, 책상 및 파티션 등에 패스워드가 노출되어 있는지 여부	☐
2	윈도우 패스워드 규정을 준수하여 패스워드를 설정 여부	☐
3	부팅 패스워드(CMOS)를 설정여부	☐
4	10분 이상 자리 이석 시, 화면보호기를 설정하고 있으며 재시작 시 로그인 여부	☐
...	....	...
	문서 보안	
1	보안등급이 부여된 문서를 보관하는 캐비닛, 서랍장 등에 시건 여부	☐
2	캐비닛 및 서랍장 등에 관리자(정/부)가 지정 여부	☐
3	업무 문서를 이면지로 사용 여부	☐
4	사무실에 파쇄기가 설치되어 있으며, 정상적으로 운영 여부	☐
5	휴가/교육 등으로 자리 이석 시, 업무 문서를 방치 여부	☐
...	....	...

※ 사무실 업무환경 보안점검표 (이해를 돕기 위한 예시)

◇ 개인정보가 포함된 종이 인쇄물 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 보호 조치를 하고 있는가?

개인정보가 포함된 종이 인쇄물 보안 조치

① 출력·복사물 보호 및 관리 정책, 규정, 지침 등 마련
② 출력·복사물 생산·관리 대장 마련 및 기록
③ 출력·복사물 운영·관리 부서 지정 및 운영
④ 출력·복사물 외부 반출 및 재생산 통제·신고·제한
⑤ 인쇄자, 인쇄일시 등 출력·복사물 기록 저장·관리
⑥ 종이 인쇄물에 대한 파기 절차, 파기 여부 확인 등을 포함하는 파기 계획 수립 및 주기적 점검
⑦ 복합기 보안, 출력물 워터마크 등 출력·복사물 보안 기술 적용 등

번호	서비스번호	이름	이메일	휴대폰번호	가입일	구매상품
1	1001	홍길동	hong@example.com	010-1234-5678	2023-01-15	상품A
2	1002	김철수	kim@example.com	010-2345-6789	2023-02-20	상품B
3	1003	이영희	lee@example.com	010-3456-7890	2023-03-10	상품A
4	1004	박영수	park@example.com	010-4567-8901	2023-04-05	상품C
5	1005	임영미	lim@example.com	010-5678-9012	2023-05-12	상품B
6	1006	최서영	choi@example.com	010-6789-0123	2023-06-08	상품A
7	1007	정희진	jung@example.com	010-7890-1234	2023-07-19	상품C
8	1008	신동호	shin@example.com	010-8901-2345	2023-08-25	상품B
9	1009	유지은	yoo@example.com	010-9012-3456	2023-09-30	상품A
10	1010	백승호	baek@example.com	010-0123-4567	2023-10-17	상품C

출력자 워터마크

출력자: AM03185 출력일자: 00년00월00일 00:00:00 출력사유:상품기획회의

※ 출력물 워터마크 출력 (이해를 돕기 위한 예시)

◇ 개인 및 공용 업무환경에서의 정보보호 준수 여부를 주기적으로 검토하고 있는가?

개인 및 공용 업무환경에서의 정보보호 준수 여부를 주기적으로 검토

① 개인 및 공용 업무환경에서의 정보보호 준수 여부를 주기적으로 검토하여야 한다.

1. 개인 및 공용 업무환경 보안규정 미준수자는 상벌규정에 따라 관리

사무실 업무환경 보안점검 결과보고

구분	직위	성명	일자	서명
승인	정보보호 최고책임자	OOO	2023-02-01	승인
기안	정보보호 담당자	OOO	2022-01-29	

※ 사무실 업무환경 보안점검 결과보고 (이해를 돕기 위한 예시)

2.5 인증 및 권한관리

2.5.1 사용자 계정 관리

세부분야	2.5.1 사용자 계정 관리
인증 기준	정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 사용자 등록·해지 및 접근권한 부여·변경·말소 절차를 수립·이행하고, 사용자 등록 및 권한 부여 시 사용자에게 보안 책임이 있음을 규정화하고 인식시켜야 한다.
주요 확인사항	• 정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자 계정 및 접근권한의 등록 · 변경 · 삭제에 관한 공식적인 절차를 수립·이행하고 있는가? • 정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자 계정 및 접근권한 생성·등록·변경 시 직무별 접근권한 분류 체계에 따라 업무상 필요한 최소한의 권한만을 부여하고 있는가? • 사용자에게 계정 및 접근권한을 부여하는 경우 해당 계정에 대한 보안 책임이 본인에게 있음을 명확히 인식시키고 있는가?
기준 요약도	
운영 방안	**◇ 정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자 계정 및 접근권한의 등록·변경·삭제에 관한 공식적인 절차를 수립·이행하고 있는가?** **(예시) 계정관리 절차 수립** 「**인적보안지침**」 제 ○○조 (접근권한 관리) ① 정보자산 접근권한은 최소권한 원칙 및 직무분장에 따라 필요 최소 범위 내에서 부여하며, 모든 계정 및 권한 부여, 변경, 삭제는 공식적인 승인 및 기록 절차를 거쳐야

한다.

② 접근권한 부여 절차는 다음 각 호로 구성한다.

1. 사용자 계정 및 권한은 부서장 승인, 권한관리책임자 검토 및 시스템관리자 실행 과정으로 등록한다.

2. 신규/변경/삭제 등 권한요구 시 계정신청서 등 관련 서류를 작성·제출하며, 승인 및 실행 이후 관련 내역을 관리대장에 기록한다.

3. 계정 생성 시 초기 비밀번호는 안전하게 전달하며, 사용자는 비밀번호를 즉시 변경한다.

③ 접근권한 변경은 업무, 인사, 직무 변경 등 공식 요청에 따라 승인·기록 후 변경한다. 긴급 상황 시 임시 권한 부여는 별도 승인 및 사후 정식 기록을 필수로 한다.

④ 접근권한의 삭제는 퇴사·전출·업무종료·장기 미사용 등 해당 사유 발생 시 인사팀 등 관련 부서 통지에 따라 실행하며, 계정 삭제 및 접근내역 관리대장에 기록한다.

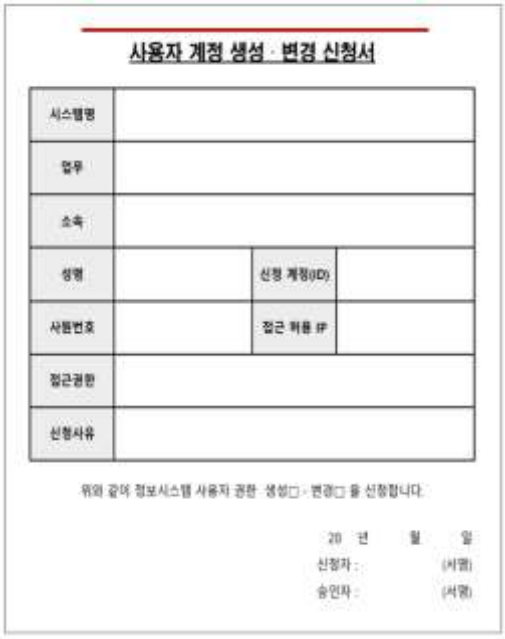
⑤ 접근권한 및 계정 사용 이력, 접속 로그, 변경 기록 등은 정보보호 관리대장에 최소 3년간 보관한다.

⑥ 분기 1회 이상 정기적으로 전체 계정 및 권한 부여의 적정성을 검토·보고하여, 불필요하거나 과다 부여된 권한은 즉시 축소·정리한다.

⑦ 관리자·개발자 등 특수 계정은 최소 인원에게만 부여하며 별도 승인을 거쳐 기록·관리한다

⑧ 외부업체 계정은 기간 및 접근 범위 제한, 보안서약서 징구 후, 사용 종료 즉시 삭제한다.

⑨ 본 지침에 의한 접근권한 부여자(사용자)는 개인정보·기밀정보 유출 및 오남용 방지 등 보안 책임을 분명히 인식하고 보안서약서를 작성한다.



사용자 계정 생성 · 변경 신청서

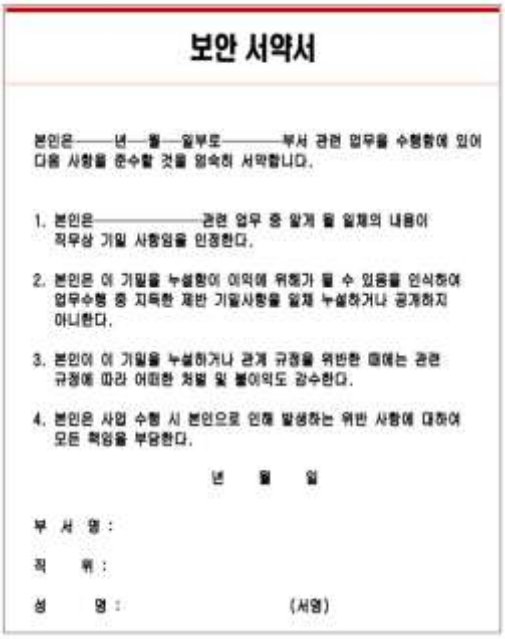
시스템명			
업무			
소속			
성명		신청 계정(ID)	
사원번호		접근 허용 IP	
접근권한			
신청사유			

위와 같이 정보시스템 사용자 권한 생성□ · 변경□ 을 신청합니다.

20 년 월 일

신청자 : (서명)

승인자 : (서명)



보안 서약서

본인은 ____년 ____월 ____일부로 ____부서 관련 업무를 수행함에 있어 다음 사항을 준수할 것을 엄숙히 서약합니다.

1. 본인은 ____관련 업무 중 알게 될 일체의 내용이 직무상 기밀 사항임을 인정한다.
2. 본인은 이 기밀을 누설함이 이익에 위해가 될 수 있음을 인식하여 업무수행 중 지득한 제반 기밀사항을 일체 누설하거나 공개하지 아니한다.
3. 본인이 이 기밀을 누설하거나 관계 규정을 위반한 때에는 관련 규정에 따라 어떠한 처벌 및 불이익도 감수한다.
4. 본인은 사업 수행 시 본인으로 인해 발생하는 위반 사항에 대하여 모든 책임을 부담한다.

년 월 일

부 서 명 :

직 위 :

성 명 : (서명)

※ 계정 발

◇ 정보시스템과 개인정보 및 중요정보에 접근할 수 있는 사용자 계정 및 접근권한 생성·등록·변경 시 직무별 접근권한 분류 체계에 따라 업무상 필요한 최소한의 권한만을 부여하고 있는가?

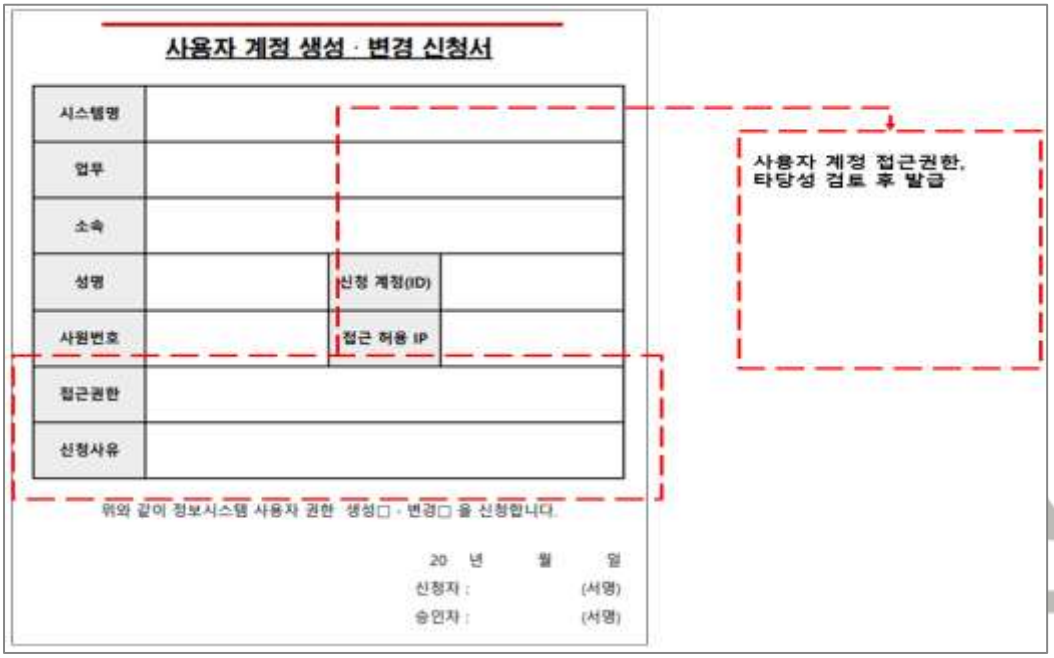
직무별 접근권한 분류 체계에 따라 업무에 필요한 최소한의 권한만을 부여

① 정보시스템 및 개인정보처리시스템에 대한 접근권한은 업무 수행 목적에 따라 최소한의 범위로 업무 담당자에게 차등 부여

② 중요정보 및 개인정보에 대한 접근권한은 알 필요(need-to-know), 할 필요(need-to-do)의 원칙에 따라 업무적으로 꼭 필요한 범위에 한하여 부여

③ 불필요하거나 과도하게 중요정보 또는 개인정보에 접근하지 못하도록 권한 세분화

④ 권한 부여 또는 변경 시 승인 절차 등을 통하여 적절성 검토 등



※ 사용자 계정 권한 신청서(이해를 돕기 위한 예시)

◇ 사용자에게 계정 및 접근권한을 부여하는 경우 해당 계정에 대한 보안 책임이 본인에게 있음을 명확히 인식시키고 있는가?

사용자가 부여받은 계정에 대해 다음과 같은 개인 책임을 명확히 인식하도록 교육

① 계정 소유권: 부여받은 계정은 개인 전용이며, 타인과 절대 공유 금지

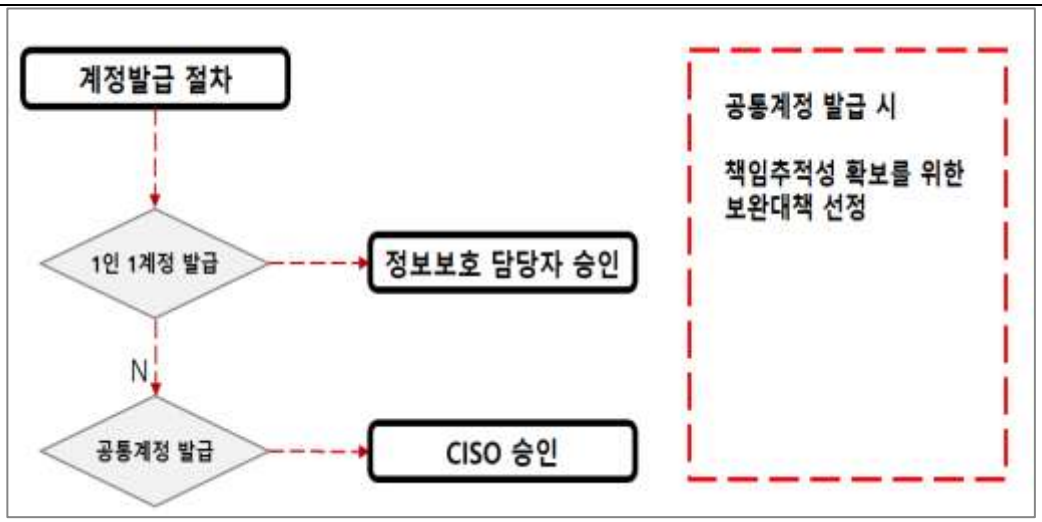
② 비밀번호 보안: 비밀번호 생성, 변경, 관리에 대한 전적인 책임

③ 접근 활동: 해당 계정으로 수행한 모든 활동에 대한 책임

④ 보안 수칙 준수: 조직의 정보보안 정책 및 지침 준수 의무

2.5.2 사용자 식별

세부분야	2.5.2 사용자 식별
인증 기준	사용자 계정은 사용자별로 유일하게 구분할 수 있도록 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 하며, 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하여 책임자의 승인 및 책임 추적성 확보 등 보완대책을 수립·이행하여야 한다.
주요 확인사항	• 정보시스템 및 개인정보처리시스템에서 사용자 및 개인정보취급자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자의 사용을 제한하고 있는가? • 불가피한 사유로 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 보완대책을 마련하여 책임자의 승인을 받고 있는가?
기준 요약도	
운영 방안	**◇ 정보시스템 및 개인정보처리시스템에서 사용자 및 개인정보취급자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자의 사용을 제한하고 있는가?** **책임 추적성 확보** ① 핵심 원칙 1. 1인 1계정 발급 원칙을 통해 사용자에 대한 책임추적성(Accountability)을 확보 2. 모든 사용자는 고유한 계정을 보유하며, 동일한 시스템 내에서 중복되는 ID 할당을 금지 ② 추측 불가능성 원칙에 따라 시스템 설치 후 제조사 기본계정(root, admin, administrator)을 필수적으로 변경하고, 순차적 번호나 단순 패턴 사용을 제한



※ 계정 발급 절차 (이해를 돕기 위한 예시)

◇ 불가피한 사유로 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 보완대책을 마련하여 책임자의 승인을 받고 있는가?

(예시) 불가피하게 공용계정 사용 시 보완대책 수립

「**인적보안지침**」 제 ◌◌조 (공용계정 관리)

① 업무상 불가피하게 공용계정을 사용하는 경우에는 그 사유와 타당성을 검토하고 책임추적성 확보 등 추가 보완대책을 마련하여 정보시스템 책임자의 승인을 받아야 한다.

1. 업무 분장상 정·부의 역할이 구분되어 관리자 계정을 공유하는 경우에도 사용자 계정을 별도로 부여하고 사용자 계정으로 로그인 후 관리자 계정으로 변경
2. 유지보수 업무 등을 위하여 임시적으로 계정을 공유한 경우 업무 종료 후 즉시 해당 계정의 비밀번호 변경
3. 업무상 불가피하게 공용계정 사용이 필요한 경우 그 사유와 타당성을 검토하여 책임자의 승인을 받고 책임 추적성을 보장할 추가 통제 방안 적용

2.5.3 사용자 인증

<table>
<tr><th>세부분야</th><th>2.5.3 사용자 인증</th></tr>
<tr><td>인증
기준</td><td>정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증 절차와 필요에 따라 강화된 인증 방식을 적용하여야 한다. 또한 로그인 횟수 제한, 불법 로그인 시도 경고 등 비인가자 접근 통제 방안을 수립·이행하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 정보시스템 및 개인정보처리시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 따라 통제하고 있는가?
• 정보통신망을 통하여 외부에서 개인정보처리시스템에 접속하려는 경우에는 법적 요구사항에 따라 안전한 인증수단 또는 안전한 접속수단을 적용하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 정보시스템 및 개인정보처리시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 따라 통제하고 있는가?

(예시) 안전한 사용자 인증 절차에 따른 접근통제
① 정보시스템 인증 방식을 다음 중 하나로 선택·구현.
1. 비밀번호
2. OTP, 모바일 OTP, 일회성 비밀번호
3. 전자 서명(인증서)
4. 생체인증
5. H/W, S/W 기반의 보안토큰 등
② 정보시스템의 비인가자 접근 통제를 위해 각 호의 사항을 적용.
1. 로그인 실패 횟수 5회 이상 제한</td></tr>
</table>

2. 접속 유지 시간 최소 10분 이상 제한

3. 동일 계정의 동시 접속 세션 수 제한

4. 불법 로그인 시도 등 경고

※ 출처: 임계값 설정 (SK쉴더스)

◇ 정보통신망을 통하여 외부에서 개인정보처리시스템에 접속하려는 경우에는 법적 요구사항에 따라 안전한 인증수단 또는 안전한 접속수단을 적용하고 있는가?

법적요구사항에 따라 안전한 인증수단 또는 안전한 접속수단을 적용

① 안전한 인증수단: 인증서(PKI), 보안토큰, 일회용 비밀번호(OTP) 등

② 안전한 접속수단: 가상사설망(VPN), 전용망 등

③ 법적 구분 적용

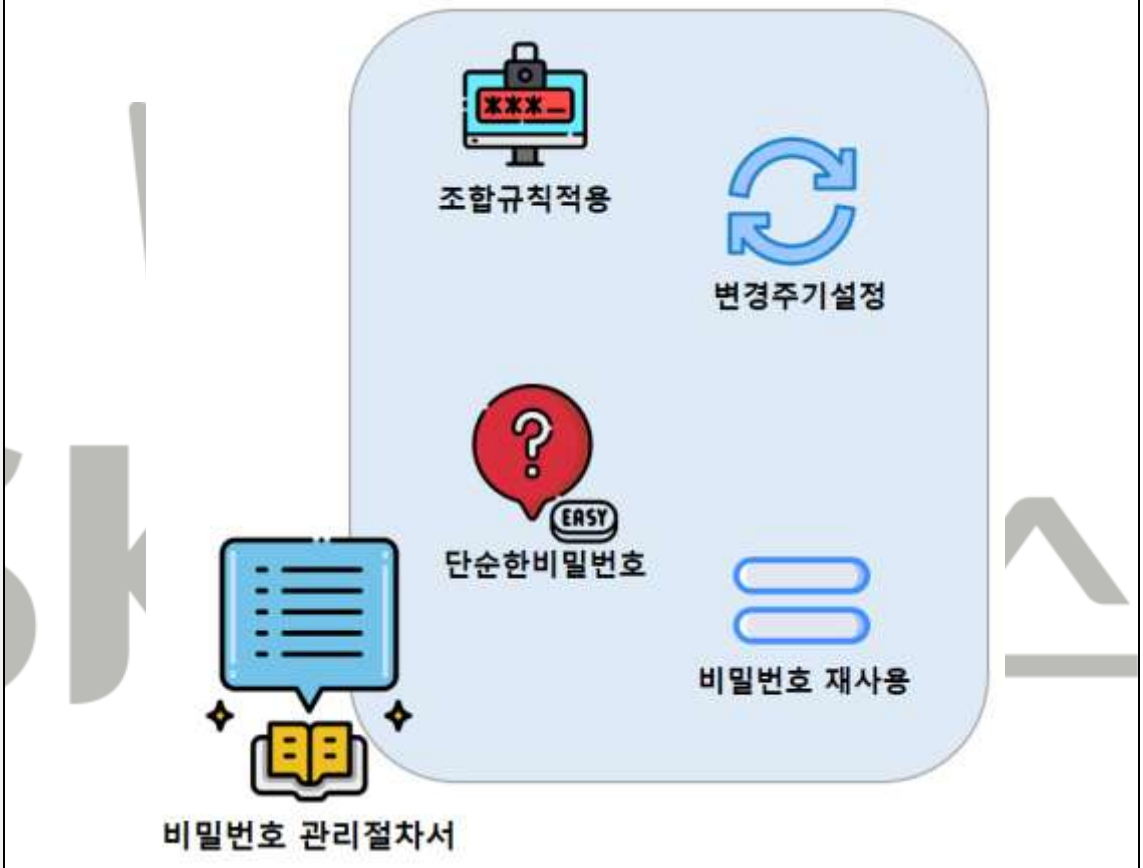
1. 이용자의 개인정보를 처리하는 시스템 : 안전한 인증수단 의무 적용

2. 이용자가 아닌 정보주체의 개인정보를 처리하는 시스템 : 안전한 접속수단 또는 안전한 인증수단 중 선택 적용 가능

※ 출처: OTP 인증 (SK쉴더스)


SK 쉴더스

2.5.4 비밀번호 관리

세부분야	2.5.4 비밀번호 관리
인증 기준	법적 요구사항, 외부 위협요인 등을 고려하여 정보시스템 사용자 및 고객, 회원 등 정보주체(이용자)가 사용하는 비밀번호 관리 절차를 수립·이행하여야 한다.
주요 확인사항	• 정보시스템에 대한 안전한 사용자 비밀번호 관리 절차 및 작성규칙을 수립·이행하고 있는가? • 정보주체(이용자)가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성규칙을 수립·이행하고 있는가? • 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하고 있는가?
기준 요약도	
운영 방안	**◇ 정보시스템에 대한 안전한 사용자 비밀번호 관리 절차 및 작성규칙을 수립·이행하고 있는가?** **(예시) 비밀번호 관리 절차 및 작성규칙 수립** 「**접근통제 관리지침**」 제 ○○조 (사용자 계정 관리) ① 계정 발급 시 임의 부여된 초기 패스워드는 사용 전 반드시 변경하여야 한다. ② 비밀번호는 숫자와 영문자, 특수문자 등을 혼합하여 9자리 이상으로 정하고, 분기별

1회 이상 주기적으로 변경 사용하여야 한다.

③ 침해사고 발생 또는 비밀번호의 노출 징후가 의심될 경우 지체 없이 비밀번호를 변경해야 한다.

※ 참고사항 : 2023년 9월 개정된 개인정보의 안전성 확보조치 기준에서 구체적인 비밀번호 작성규칙이 삭제되어 기업의 자율적 규정이 가능해짐

◇ 정보주체(이용자)가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성규칙을 수립·이행하고 있는가?

정보주체(이용자) 비밀번호 정책 수립

① 정보주체(이용자)가 안전한 비밀번호를 설정하여 사용할 수 있도록 작성규칙 수립

1. 사용자 및 개인정보취급자 비밀번호 작성규칙을 참고하되, 서비스의 특성 및 민감도 등을 고려하여 적절한 수준에서 비밀번호 작성규칙 적용
2. 비밀번호 분실, 도난 시 본인확인 등을 통한 안전한 재발급 절차 마련 등

② 금융분야의 경우 '전자금융감독규정. 제24조의3(이용자 비밀번호 관리)' 등 유관 법령에 규정된 내용 확인

◇ 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용 및 관리하고 있는가?

비밀번호 또는 인증수단 적용 시 안전한 보호 대책 적용 필요

① 인증수단은 개인정보처리자 스스로의 환경, 개인정보 보유 수, 정보주체에 미치는 영향 등을 종합적으로 고려하여 자율적으로 정하여 안전하게 적용

1. 비밀번호 인증: 문자열로 구성된 인증번호를 입력
2. 일회용 비밀번호(OTP) 인증: 한 번의 로그인 시도 또는 거래에 사용하기 위해 무작위로 생성되어 사용자에게 전송된 일회용 인증번호를 입력
3. 생체인증: 홍채, 지문 등의 생체정보를 입력하여 본인 여부를 확인
4. SMS 인증: 본인 명의의 휴대폰에서 문자로 받은 인증번호를 입력
5. 전화 인증: 본인 명의의 휴대폰에서 ARS 안내에 따라 본인 여부를 확인
6. 소셜 로그인: 포털사이트 등에서 제공하는 인증수단을 이용하여 본인 여부를 확인

② 비밀번호 등 인증정보의 분실 등을 이유로 재발급을 해야 할 때에는 정당한 사용자인지를 확인할 수 있는 수단(SMS, 이메일 등)을 활용하여 임시 인증정보를 부여하고 이용자가 확인 후 사이트에 접속하여 비밀번호 등 인증정보를 변경하여

	사용

2.5.5 특수 계정 및 권한 관리

세부분야	2.5.5 특수 계정 및 권한 관리
인증 기준	정보시스템 관리, 개인정보 및 중요정보 관리 등 특수 목적을 위하여 사용하는 계정 및 권한은 최소한으로 부여하고 별도로 식별하여 통제하여야 한다.
주요 확인사항	• 관리자 권한 등 특수 권한은 최소한의 인원에게만 부여될 수 있도록 공식적인 권한 신청 및 승인 절차를 수립·이행하고 있는가? • 특수 목적을 위하여 부여한 계정 및 권한을 식별하고 별도 목록으로 관리하는 등 통제 절차를 수립·이행하고 있는가?
기준 요약도	
운영 방안	**◇ 관리자 권한 등 특수 권한은 최소한의 인원에게만 부여될 수 있도록 공식적인 권한 신청 및 승인 절차를 수립·이행하고 있는가?** **(예시) 특수 권한 관리 절차 수립** 「**접근통제 관리지침**」 제 ○○조 (특수 계정 관리) ① 특수 계정·권한을 최소한의 업무 수행자에게만 부여할 수 있도록 하고

정보보호담당자가 정보보호 최고책임자의 승인을 득한 후 발급한다.

※ 특수 권한 계정 발급 신청 (이해를 돕기 위한 예시)

◇ 특수 목적을 위하여 부여한 계정 및 권한을 식별하고 별도 목록으로 관리하는 등 통제 절차를 수립·이행하고 있는가?

특수 권한의 통제 절차 수립 및 이행

① 계정 식별 및 분류

1. 시스템 관리자, 백업·복구, 모니터링, API 서비스 등 특수 목적 계정을 정의하고 별도 카테고리로 분류

② 권한부여 및 권한목록 작성·유지

1. 특수 목적 계정·권한 전용 목록(DB·스프레드시트 등)에 계정명, 목적, 소유자, 권한 범위, 발급일 등을 기록
2. 특수 목적 수행에 필요한 최소 권한만 부여하며, 일반 사용자 접근 금지
3. 긴급·일시적 목적 권한은 만료일 설정 후 자동 회수

③ 주기적 검토 및 갱신

1. 주기적 계정·권한 유효성 점검, 불필요 계정 비활성화 또는 삭제
2. 로그인·권한 변경 이력 실시간 수집, 이상 활동 탐지 시 경고 알림

2.5.6 접근권한 검토

세부분야	2.5.6 접근권한 검토
인증 기준	정보시스템과 개인정보 및 중요정보에 접근하는 사용자 계정의 등록·이용·삭제 및 접근권한의 부여·변경·삭제 이력을 남기고 주기적으로 검토하여 적정성 여부를 점검하여야 한다.
주요 확인사항	• 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근권한 생성 · 등록 · 부여 · 이용 · 변경 · 말소 등의 이력을 남기고 있는가? • 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근권한의 적정성 검토 기준, 검토 주체, 검토 방법, 주기 등을 수립하여 정기적 검토를 이행하고 있는가? • 접근권한 검토 결과 접근권한 과다 부여, 권한 부여 절차 미준수, 권한 오·남용 등 문제점이 발견된 경우 그에 따른 조치 절차를 수립·이행하고 있는가?
기준 요약도	
운영 방안	**◇ 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근권한 생성·등록·부여·이용·변경·말소 등의 이력을 남기고 있는가?** **(예시) 사용자 계정 및 접근권한 생성·등록·부여·이용·변경·말소 등의 이력 보관** 「**접근통제 관리지침**」 제 ○○조 (계정 접속기록 관리) ① 정보시스템 책임자는 책임 추적성 및 사고 발생 시 조사를 위해 각 호의 사항을 5년간 저장 및 관리해야 한다. 1. 계정 및 관리 구분(발급·변경·해지) 2. 신청 정보: 신청자, 신청 일자, 신청 목적, 사용 기간

3. 승인 정보: 승인자, 승인 일자

4. 등록 정보: 등록자, 등록 일자

② 정보시스템 책임자는 사용자 계정 및 접근권한에 대해 다음 각 호의 사항을 포함하여 분기 1회 이상 검토해야 한다.

※「개인정보보호법」에 따른 개인정보처리자: 최소 3년간 보관 필수

◇ 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근권한의 적정성 검토 기준, 검토 주체, 검토 방법, 주기 등을 수립하여 정기적 검토를 이행하고 있는가?

개인정보 및 중요정보에 대한 계정 및 접근권한 검토 분기 1회(권고) 실시

① 접근권한 부여의 적정성 검토

1. 공식적인 절차에 따른 접근권한 부여 여부
2. 접근권한 분류체계의 업무 목적 및 보안정책 부합 여부
3. 접근권한 승인자의 적절성
4. 직무변경 시 기존 권한 회수 후 신규 업무에 대한 적절한 권한 부여 여부
5. 업무 목적 외 과도한 접근권한 부여 여부
6. 특수 권한 부여·변경·발급 현황 및 적정성
7. 협력업체 등 외부자 계정·권한 발급 현황 및 적정성
8. 접근권한 신청·승인 내역과 실제 접근권한 부여 현황의 일치 여부
9. 장기 미접속자 계정 현황 및 삭제(또는 잠금) 여부
10. 휴직, 퇴직 시 지체 없이 계정 및 권한 회수 여부 등

◇ 접근권한 검토 결과 접근권한 과다 부여, 권한 부여 절차 미준수, 권한 오·남용 등 문제점이 발견된 경우 그에 따른 조치 절차를 수립·이행하고 있는가?

접근권한 과다·미준수·오·남용 사례 발견 시 대응 절차를 수립·운영

① 과다 권한 부여: 불필요 권한 회수, 영향도 분석 및 사용자 알림

② 절차 미준수: 해당 부서장·담당자에 경고, 재교육 시행, 반복 시 징계 절차

③ 권한 오·남용: 해당 계정 즉시 일시 중지, 사고조사팀 구성, 원인 분석 및 재발 방지 대책 수립

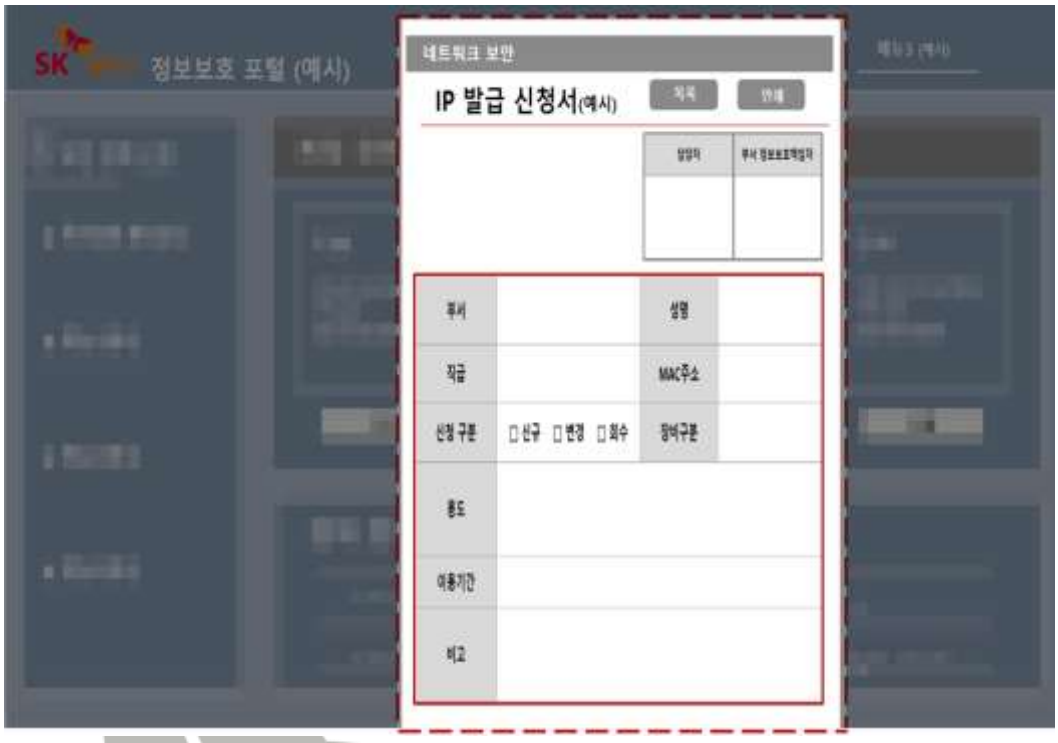
④ 이행 보고: 조치 결과를 포함한 분기별 감사보고서 작성·경영진 보고

2.6 접근통제

2.6.1 네트워크 접근

세부분야	2.6.1 네트워크 접근
인증 기준	네트워크에 대한 비인가 접근을 통제하기 위하여 IP 관리, 단말 인증 등 관리 절차를 수립·이행하고, 업무 목적 및 중요도에 따라 네트워크 분리(DMZ(Demilitarized Zone), 서버팜, 데이터베이스존, 개발존 등)와 접근통제를 적용하여야 한다.
주요 확인사항	• 조직의 네트워크에 접근할 수 있는 모든 경로를 식별하고 접근통제 정책에 따라 내부 네트워크는 인가된 사용자만이 접근할 수 있도록 통제하고 있는가? • 서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 각 영역 간 접근통제를 적용하고 있는가? • 네트워크 대역별 IP 주소 부여 기준을 마련하고 데이터베이스 서버 등 외부 연결이 필요하지 않은 경우 사설 IP로 할당하는 등의 대책을 적용하고 있는가? • 물리적으로 떨어진 IDC, 지사, 대리점 등과의 네트워크 연결 시 전송구간 보호 대책을 마련하고 있는가?
기준 요약도	
운영 방안	**◇ 조직의 네트워크에 접근할 수 있는 모든 경로를 식별하고 접근통제 정책에 따라 내부 네트워크는 인가된 사용자만이 접근할 수 있도록 통제하고 있는가?** **(예시) 네트워크 접근통제 관리 절차 수립·이행** 「**접근통제 관리지침**」 제 ○○조 (네트워크 접근) ① 사내 네트워크에 접근할 수 있는 모든 경로를 식별하고, 인가된 사용자만 접근할 수 있도록 통제해야 한다. ② IP 주소 발급은 'IP 발급 신청서' 작성 부서 정보보호 책임자의 승인을 득한 후 발급한다.

③ 네트워크 담당자는 'IP 관리대장'에 현황을 기록·관리하고, 분기 1회 최신화해야 한다.



※ IP 발급 신청서 (이해를 돕기 위한 예시)

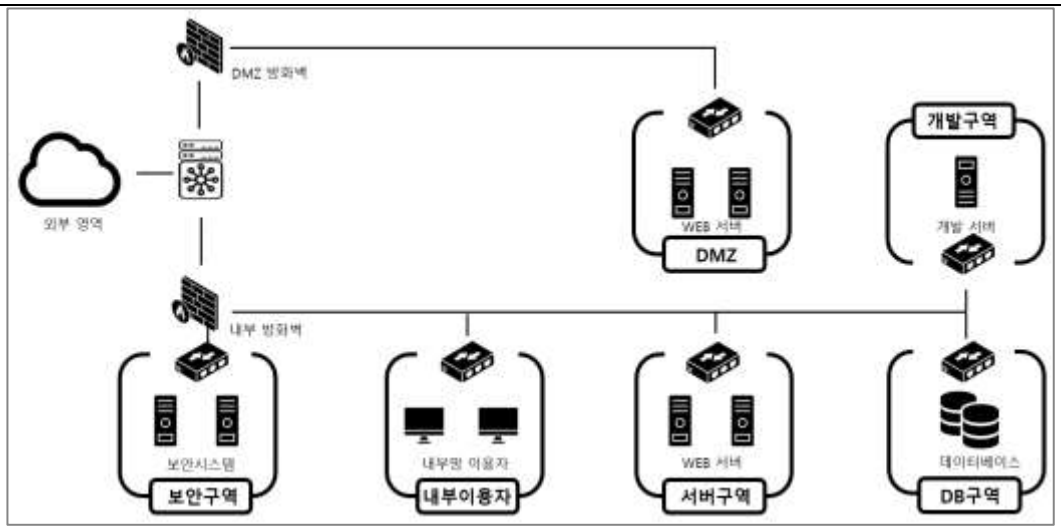
◇ 서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 각 영역 간 접근통제를 적용하고 있는가?

(예시) 네트워크 영역 분리

「**접근통제 관리지침**」 제 ○○조 (네트워크 접근)

① 서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 각 영역 간 접근을 통제하여야 한다.

1. DMZ, 서버팜, 데이터베이스, 운영 환경, 개발 환경, 외부자 영역, 공개망 등



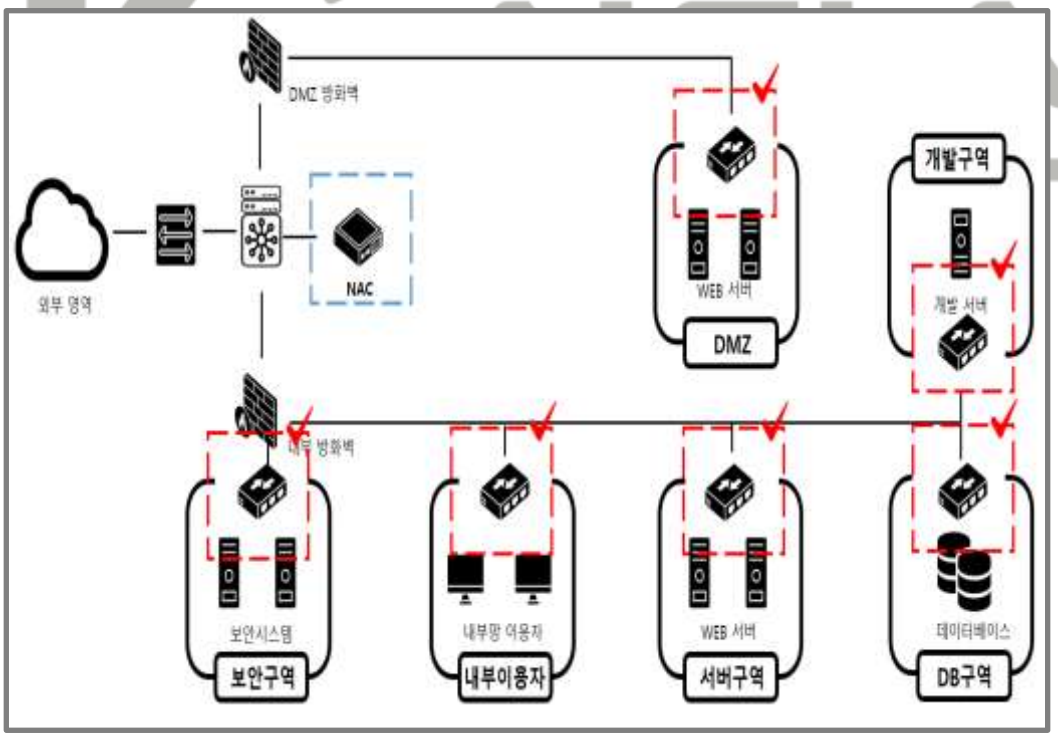
※ 네트워크 구성도 (이해를 돕기 위한 예시)

◇ 네트워크 대역별 IP 주소 부여 기준을 마련하고 데이터베이스 서버 등 외부 연결이 필요하지 않은 경우 사설 IP로 할당하는 등의 대책을 적용하고 있는가?

(예시) 사설 IP 할당 기준 수립

「**접근통제 관리지침**」 제 ○○조 (네트워크 접근)

① 내부 네트워크는 대역별 IP 주소 부여 기준을 마련하여 데이터베이스 서버 등 중요 시스템이 외부와 연결되지 않도록 사설 IP를 할당해야 한다.



※ 네트워크 사설 IP 적용 (이해를 돕기 위한 예시)

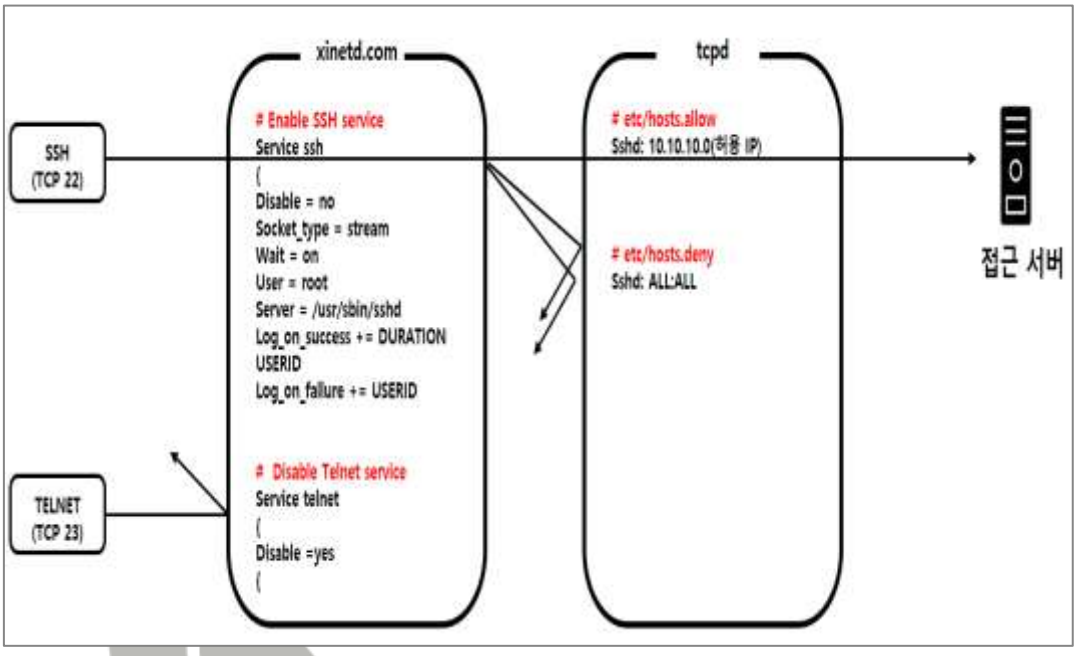
	◇ 물리적으로 떨어진 IDC, 지사, 대리점 등과의 네트워크 연결 시 전송구간 보호 대책을 마련하고 있는가? **(예시) 전송구간 보호대책 구성** ① VPN 사용 1. 지점·IDC·대리점 간 트래픽에 대해 IPsec VPN 또는 SSL VPN을 적용하여 전송구간을 전면 암호화 2. 관리망 및 운영망은 별도 VPN 프로파일로 분리 운용 ② 전용회선 사용 1. 공용 인터넷 대신 전용회선을 사용하여 물리적·논리적 분리 2. 전용 백업회선 구축으로 이중화 ③ 강화된 인증 및 상호인증 1. VPN 연결 시 디바이스 인증서(PKI) 및 사용자 다중인증(MFA) 적용 2. 지점 장비 간 상호인증(서버–서버)으로 중간자 공격 방지

2.6.2 정보시스템 접근

세부분야	2.6.2 정보시스템 접근
인증 기준	서버, 네트워크시스템 등 정보시스템에 접근을 허용하는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 통제하여야 한다.
주요 확인사항	• 서버, 네트워크시스템, 보안시스템 등 정보시스템별 운영체제(OS)에 접근이 허용되는 사용자, 접근 가능 위치, 접근 수단 등을 정의하여 통제하고 있는가? • 정보시스템에 접속 후 일정 시간 업무처리를 하지 않는 경우 자동으로 시스템 접속이 차단되도록 하고 있는가? • 정보시스템의 사용 목적과 관계없는 서비스를 제거하고 있는가? • 주요 서비스를 제공하는 정보시스템은 독립된 서버로 운영하고 있는가?
기준 요약도	
운영 방안	**◇ 서버, 네트워크시스템, 보안시스템 등 정보시스템별 운영체제(OS)에 접근이 허용되는 사용자, 접근 가능 위치, 접근 수단 등을 정의하여 통제하고 있는가?** **(예시) 정보시스템 접근통제 절차 수립** 「**접근통제 관리지침**」 제 ○○조 (정보시스템 접근) ① 서버·네트워크시스템·보안시스템 등 정보시스템별 운영체제(OS)에 대한 접근을 다음 각 호를 포함하여 통제해야 한다. 1. 계정 및 권한 신청·승인 절차 2. 사용자별로 개별 계정 부여 및 공용 계정 사용 제한 3. 계정 사용 현황에 대한 정기 검토 및 현행화 관리 4. 접속 위치 제한 5. 관리자 등 특수 권한에 대한 강화된 인증 수단(인증서, OTP 등) 적용

6. 안전한 접근 수단 적용(SFTP, SSH, SSL 등)

7. 동일 네트워크 영역 내 서버 간 접속에 대한 접근통제 조치



※ 접근제어 설정 (이해를 돕기 위한 예시)

◇ 정보시스템에 접속 후 일정 시간 업무처리를 하지 않는 경우 자동으로 시스템 접속이 차단되도록 하고 있는가?

정보시스템 세션 타임아웃 설정

① 정보시스템 특성, 업무 환경, 위험의 크기, 법적 요구사항 등을 고려하여 세션 유지시간 설정

1. 최대 접속가능 시간은 통상적인 수준(10분~60분 이내)에서 정할 수 있음

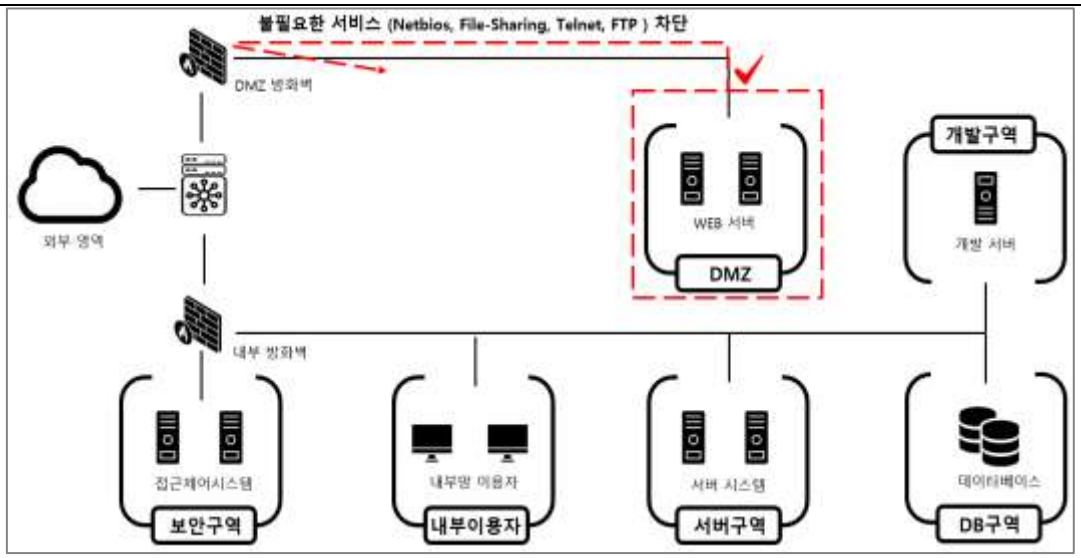
2. 개인정보처리시스템 정기 점검 등 특별한 상황에서 장시간 접속이 필요한 때에는 사유 및 접속기간 등 그 기록을 보관·관리하고, 작업 종료 등에 따라 장시간 접속이 불필요해진 경우에는 다시 원래의 시간으로 복원

◇ 정보시스템의 사용 목적과 관계없는 서비스를 제거하고 있는가?

불필요한 서비스 또는 포트 제거

① 안전하지 않은 서비스, 프로토콜, 데몬에 대해서는 추가 보안기능 구현

② NetBIOS, File-Sharing, Telnet, FTP 등과 같은 안전하지 않은 서비스를 보호하기 위하여 SSH, SFTP, IPSec VPN 등과 같은 안전한 기술 사용



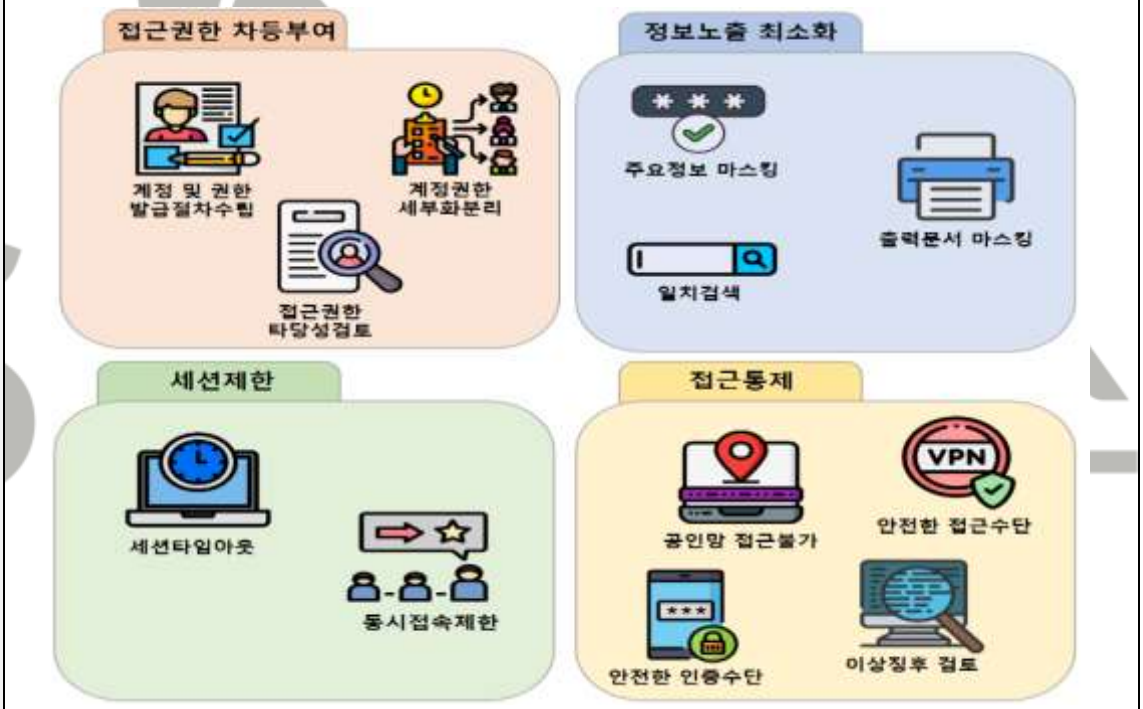
※ 불필요한 아웃바운드 서비스 오픈 (이해를 돕기 위한 예시))

◇ 주요 서비스를 제공하는 정보시스템은 독립된 서버로 운영하고 있는가?

주요 정보시스템 독립 서버 운영

① 외부에 직접 서비스를 제공하거나 민감한 정보를 보관·처리하고 있는 웹서버, 데이터베이스 서버, 응용 프로그램 등은 공용 장비로 사용하지 않고 독립된 서버 사용

2.6.3 응용프로그램 접근

세부분야	2.6.3 응용프로그램 접근
인증 기준	사용자별 업무 및 접근 정보의 중요도 등에 따라 응용프로그램 접근권한을 제한하고, 불필요한 정보 또는 중요정보 노출을 최소화할 수 있도록 기준을 수립하여 적용하여야 한다.
주요 확인사항	• 중요정보 접근을 통제하기 위하여 사용자의 업무에 따라 응용프로그램 접근권한을 차등 부여하고 있는가? • 일정 시간 동안 입력이 없는 세션은 자동 차단하고, 동일 사용자의 동시 세션 수를 제한하고 있는가? • 관리자 전용 응용프로그램(관리자 웹페이지, 관리콘솔 등)은 비인가자가 접근할 수 없도록 접근을 통제하고 있는가? • 개인정보 및 중요정보의 표시제한 보호조치의 일관성을 확보할 수 있도록 관련 기준을 수립하여 적용하고 있는가? • 개인정보 및 중요정보의 불필요한 노출(조회, 화면 표시, 인쇄, 다운로드 등)을 최소화할 수 있도록 응용프로그램을 구현하여 운영하고 있는가?
기준 요약도	
운영 방안	**◇ 중요정보 접근을 통제하기 위하여 사용자의 업무에 따라 응용프로그램 접근권한을 차등 부여하고 있는가?** **최소 권한 원칙에 따라 접근권한 부여** ① 업무별 응용프로그램 접근권한 차등 부여 1. 역할(Role)·직무(Task) 기반 권한 별 매트릭스 수립 2. 업무분석 결과에 따라 조회·입력·수정·삭제 권한 세분화

3. 신규 사용자·업무 변경 시 권한 신청·승인 절차 적용

4. 최소권한 원칙(Least Privilege) 방식으로 주기적 권한 검토

000업무시스템 상세 권한부여 현황

직책	설명	권한 세부 내역				
		A 화면	B화면	C화면	D화면	다운로드
슈퍼 관리자	- 시스템 계정생성 권한부여	부여	부여	부여	부여	미부여
책임자	- 사업을 총괄 관리 하는 담당자	부여	부여	부여	미부여	부여
관리자	- 일부 업무를 관리하는 담당자	부여	부여	미부여	미부여	부여
취급자	- 업무를 수행하는 사용자	부여	미부여	미부여	미부여	미부여

※ 권한 상세 부여 현황 (이해를 돕기 위한 예시)

◇ 일정 시간 동안 입력이 없는 세션은 자동 차단하고, 동일 사용자의 동시 세션 수를 제한하고 있는가?

응용프로그램 세션 관리

① 세션 타임아웃: 일정시간 미동작 시 자동 로그아웃 또는 화면 잠금

② 동시 세션 제한: 기준에 따른 세션 허용, 초과 시 기존 세션 종료 또는 신규 접속 차단

※ 출처: 세션 타임아웃 (SK쉴더스)

◇ 관리자 전용 응용프로그램(관리자 웹페이지, 관리콘솔 등)은 비인가자가 접근할 수 없도록 접근을 통제하고 있는가?

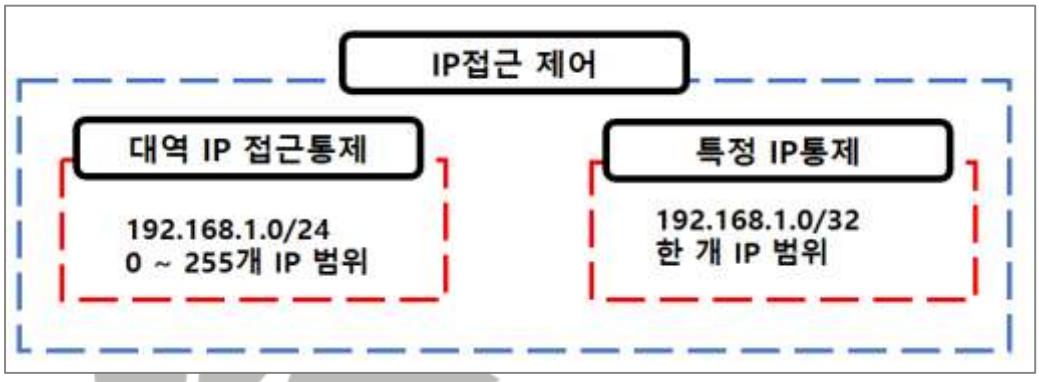
관리자 전용 응용프로그램 접근통제

① 관리자 전용 응용프로그램의 외부 공개 차단 및 IP 주소 등을 통한 접근제한 조치

② 불가피하게 외부 공개가 필요한 경우 안전한 인증 수단(OTP 등) 또는 안전한 접속 수단(VPN 등) 적용

③ 관리자(사용자), 개인정보취급자의 접속 로그 및 이벤트 로그에 대한 정기적 모니터링

④ 이상징후 발견 시 세부 조사, 내부 보고 등 사전에 정의된 절차에 따라 이행



※ IP 범위 설정 (이해를 돕기 위한 예시)

◇ 개인정보 및 중요정보의 표시제한 보호조치의 일관성을 확보할 수 있도록 관련 기준을 수립하여 적용하고 있는가?

일관성 있는 마스킹 처리

① 개인정보·중요정보 표시제한 기준 수립

1. 민감도 등급(Level) 정의(예: 일반·민감)

2. 등급별 표시 허용 범위 문서화

- 일반: 화면표시·출력 가능

- 민감: 마스킹(****) 후 부분 표시

3. 개발·테스트 환경에서도 동일 기준 적용

② 일관성 있는 기준 수립

1. 다수의 개인정보처리시스템 등에서 개인정보를 각기 다른 방식으로 마스킹 할 때에는 개인정보취급자가 개인정보 집합을 구성할 수 있으므로 동일한 기준으로 표시제한 조치

구분	A 시스템	B 시스템
이름	홍*동	홍길*
전화번호	010-****-5678	010-1234-****
이메일	ho**@asd.com	**ng@asd.com

※ 일관성 없는 표시제한 (이해를 돕기 위한 예시)

◇ 개인정보 및 중요정보의 불필요한 노출(조회, 화면 표시, 인쇄, 다운로드 등)을 최소화할 수 있도록 응용프로그램을 구현하여 운영하고 있는가?

(예시) 불필요한 노출 최소화

① 용도 특정 및 출력항목 최소화

② Like 검색 제한

③ 과도 정보 필터링

④ 복합 검색조건 활용

⑤ 출력 전 확인 알림 등

구분	(예시) 보험사	(예시) 물류회사
용도 특정 및 출력항목 최소화	대출심사 시스템 : 고객명·대출금액·신용등급만 표시, 주민등록번호·주소는 숨김 처리	배송 예약 시스템 : 고객명·예약일·배송주소만 표시, 상세주소는 비노출
업무형태별 최소 출력	보험상담 시스템 : 통화 중인 고객 전화번호·최근 상담이력만 표시, 추가 개인정보는 별도 동의 후 표시	물류창고 출입 시스템 : 직원 이름·출입 시간만 표시, 부서·연락처는 숨김 처리
유사검색(Like검색) 제한	회원 이메일 검색 : 이메일 일치 검색 시 조회가능	배송관리 시스템 : 고객명, 주문번호 등 다수조건 검색만 허용, 단일 조건 검색 시 오류 메시지 표시
출력 전 확인 알림	인쇄 버튼 클릭 시 "출력용도: 내부결재" 선택 후 인쇄 가능, 목적 미선택 시 기능 비활성화	배송확인서 출력 시 "용도" 선택 시만 출력, 미선택 시 비활성화

※ 개인정보 및 중요정보 불필요한 노출 최소화 (이해를 돕기 위한 예시)

2.6.4 데이터베이스 접근

<table>
<tr><th>세부분야</th><th>2.6.4 데이터베이스 접근</th></tr>
<tr><td>인증
기준</td><td>테이블 목록 등 데이터베이스 내에서 저장·관리되고 있는 정보를 식별하고, 정보의 중요도와 응용프로그램 및 사용자 유형 등에 따른 접근통제 정책을 수립·이행하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 데이터베이스의 테이블 목록 등 저장·관리되고 있는 정보를 식별하고 있는가?
• 데이터베이스 내 정보에 접근이 필요한 응용프로그램, 정보시스템(서버) 및 사용자를 명확히 식별하고 접근통제 정책에 따라 통제하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 데이터베이스의 테이블 목록 등 저장·관리되고 있는 정보를 식별하고 있는가?

데이터베이스 현황 정기적 현행화
① 데이터베이스 테이블 목록 및 컬럼 기록 변경 현행화
000 시스템 테이블 정의서
※ 테이블명세서(이해를 돕기 위한 예시)

◇ 데이터베이스 내 정보에 접근이 필요한 응용프로그램, 정보시스템(서버) 및</td></tr>
</table>

사용자를 명확히 식별하고 접근통제 정책에 따라 통제하고 있는가?

데이터베이스 접근권한 차등 부여

① 테이블, 뷰, 컬럼, 쿼리 등 사용 명령어 권한 차등 부여

② 지정된 IP 접근 설정을 통해 비인가 접근제한 (IP 통제, 접근제어 솔루션 적용)

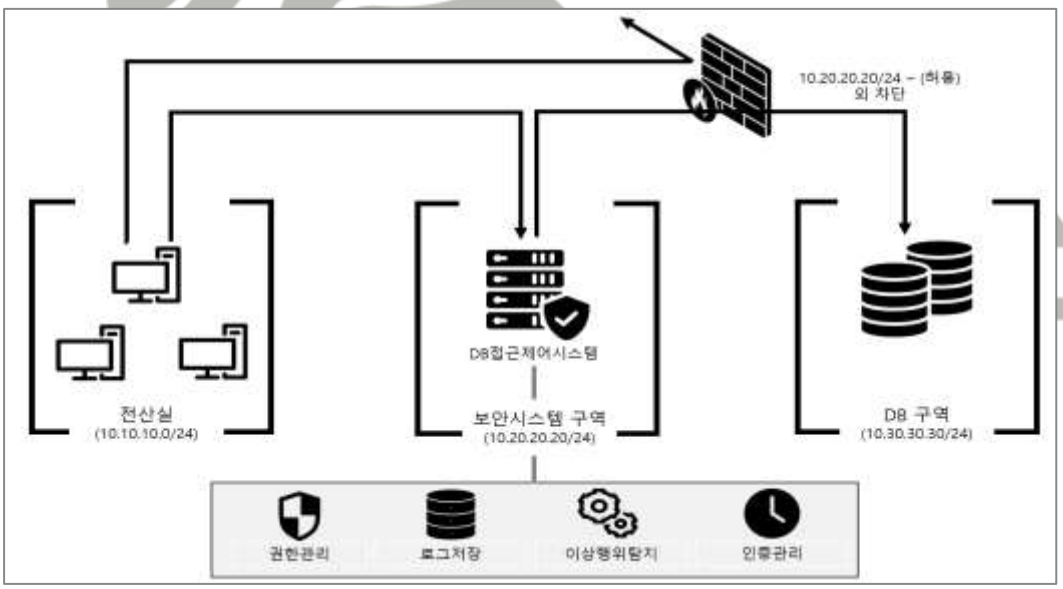
권한 명령어	설명	예시
SELECT	SELECT 권한 부여	GRANT SELECT ON mydatabase.mytable TO '권한 부여 ID';
INSERT	INSERT 권한 부여	GRANT INSERT ON mydatabase.mytable TO '권한 부여 ID';
UPDATE	UPDATE 권한 부여	GRANT UPDATE ON mydatabase.mytable TO '권한 부여 ID';
DELETE	DELETE 권한 부여	GRANT DELETE ON mydatabase.mytable TO '권한 부여 ID';
ALL PRIVILEGES	모든 권한 부여	GRANT ALL PRIVILEGES ON mydatabase.mytable TO '권한 부여 ID';
CREATE	CREATE 권한 부여	GRANT CREATE ON mydatabase.* TO '권한 부여 ID';
DROP	DROP 권한 부여	GRANT DROP ON mydatabase.* TO '권한 부여 ID';
INDEX	INDEX 권한 부여	GRANT INDEX ON mydatabase.mytable TO '권한 부여 ID';
REFERENCES	REFERENCES 권한 부여	GRANT REFERENCES ON mydatabase.mytable TO '권한 부여 ID';
ALTER	ALTER 권한 부여	GRANT ALTER ON mydatabase.mytable TO '권한 부여 ID';

※ 권한 부여 명령어 (이해를 돕기 위한 예시)

접근제어 시스템을 이용한 통제

① 비인가자 접근제어

② 우회 접속 차단



※ 데이터베이스 접근제어 시스템 (이해를 돕기 위한 예시)

2.6.5 무선 네트워크 접근

세부분야	2.6.5 무선 네트워크 접근
인증 기준	무선 네트워크를 사용하는 경우 사용자 인증, 송수신 데이터 암호화, AP 통제 등 무선 네트워크 보호 대책을 적용하여야 한다. 또한 AD Hoc 접속, 비인가 AP 사용 등 비인가 무선 네트워크 접속으로부터 보호 대책을 수립·이행하여야 한다.
주요 확인사항	• 무선 네트워크를 업무적으로 사용하는 경우 무선 AP 및 네트워크 구간 보안을 위하여 인증, 송수신 데이터 암호화 등 보호 대책을 수립·이행하고 있는가? • 인가된 임직원만이 무선 네트워크를 사용할 수 있도록 사용 신청 및 해지 절차를 수립 · 이행하고 있는가? • AD Hoc 접속 및 조직 내 허가받지 않은 무선 AP 탐지 · 차단 등 비인가된 무선 네트워크에 대한 보호 대책을 수립·이행하고 있는가?
기준 요약도	
운영 방안	**◇ 무선 네트워크를 업무적으로 사용하는 경우 무선 AP 및 네트워크 구간 보안을 위하여 인증, 송수신 데이터 암호화 등 보호 대책을 수립·이행하고 있는가?** **무선 네트워크 보호 대책 수립** 「**접근통제 관리지침**」 제 ○○조 (AP관리) ① 무선랜을 사용하여 업무 자료를 전송하는 경우에는 각 호에 해당하는 보호 대책을 수립해야 한다. 1. 네트워크 이름(SSID, Service Set Identifier) 브로드캐스팅 중지 2. 추측이 어려운 복잡한 SSID 사용 3. WPA2 이상(256비트 이상)의 암호체계를 사용하여 소통자료 암호화 - AP가 제공하는 WEP 키 중 128bit 이상의 키를 사용하도록 하고 WEP키를 주기적으로 변경하거나 Dynamic WEP Key 혹은 TKIP 등을 사용하여 데이터 암호화를 실시한다.

4. MAC 주소 및 IP 필터링 설정, DHCP 사용 금지 RADIUS (Remote Authentication Dial-In User Service)인증 사용

5. 그 밖에 무선단말기·중계기(AP) 등 무선랜 구성요소별 분실·탈취·훼손·오용 등에 대비한 관리적·물리적 보안대책

② 무선랜 및 AP를 사용하고자 하는 경우에는 무선LAN 설치 의뢰서를 작성하여 네트워크 담당자에게 신청하고, 네트워크 담당자는 무선랜/AP 사용대장에 기록·관리한다.

무선 AP 관리대장

운영담당자	운영책임자

장비명	관리번호 (시리얼번호)	장소/사용자	목적	기간	SSID	인증방식 (WPA/PSK)	네트워크키 (128bit)	신청자

※ 무선AP 관리대장 (이해를 돕기 위한 예시)

◇ 인가된 임직원만이 무선 네트워크를 사용할 수 있도록 사용 신청 및 해지 절차를 수립 · 이행하고 있는가?

사용 신청 및 해지 절차 수립

① 무선 네트워크 사용 권한 신청 및 승인 절차(사용자 및 접속단말 등록 등)

② 퇴직, 기간 만료 등의 사유로 무선 네트워크 사용이 필요하지 않은 경우 접근권한 해지 절차

③ 외부인에게 제공하는 무선 네트워크는 임직원이 사용하는 무선 네트워크와 분리

◇ AD Hoc 접속 및 조직 내 허가받지 않은 무선 AP 탐지 · 차단 등 비인가된 무선 네트워크에 대한 보호 대책을 수립·이행하고 있는가?

(예시) 비인가된 무선 네트워크에 대한 보호대책 수립·이행

① 무선 침입 탐지·방지 시스템(WIPS) 도입

1. 실시간 스캔: 주기적 및 상시 무선 주파수 스캐닝으로 Ad Hoc 네트워크 및 무단 AP 탐지

2. 서명 기반 탐지: SSID 변조, MAC 스푸핑, 비표준 채널 사용 패턴 식별

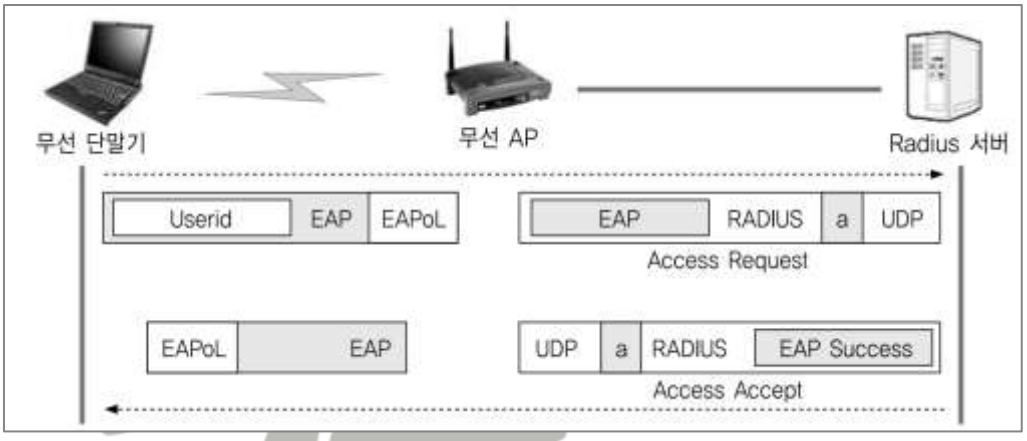
3. 행위 기반 탐지: 비인가 디바이스의 트래픽 패턴 분석 및 이상행위 탐지

② 차단 및 격리 조치

1. Rogue AP 차단: 무단 AP SSID 및 BSSID 자동 블랙리스트 등록 및 통신 차단
2. Ad Hoc 네트워크 차단: 엔드포인트에서 Ad Hoc 모드 비활성화 정책 강제 적용
3. 네트워크 접근제어(NAC): 미인가 디바이스 식별 시 VLAN 격리 또는 포트 차단

③ 정책 및 절차 수립

1. 무선 네트워크 보안 정책: 허가된 AP 목록(화이트리스트) 관리, 등록 절차 문서화
2. 무선망 구축·변경 요청 프로세스: 신규 AP 설치 시 담당자 승인 필수
3. Ad Hoc 사용 금지: 운영 정책에 명시하고 사용자·관리자 교육 실시



※ 출처: 금융부분 무선랜 보안가이드 (KISA)

2.6.6 원격접근 통제

세부분야	2.6.6 원격접근 통제
인증 기준	보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지하고, 재택근무·장애 대응·원격협업 등 불가피한 사유로 원격 접근을 허용하는 경우 책임자 승인, 접근 단말 지정, 접근 허용 범위 및 기간 설정, 강화된 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등 보호 대책을 수립·이행하여야 한다.
주요 확인사항	• 인터넷과 같은 외부 네트워크를 통한 정보시스템 원격운영은 원칙적으로 금지하고 장애 대응 등 부득이하게 허용하는 경우 보완대책을 마련하고 있는가? • 내부 네트워크를 통하여 원격으로 정보시스템을 운영하는 경우 특정 단말에 한해서만 접근을 허용하고 있는가? • 재택근무, 원격협업, 스마트워크 등과 같은 원격 업무 수행 시 중요정보 유출, 해킹 등 침해사고 예방을 위한 보호 대책을 수립·이행하고 있는가? • 개인정보처리시스템의 관리, 운영, 개발, 보안 등을 목적으로 원격으로 개인정보처리 시스템에 접속하는 단말기는 관리용 단말기로 지정하고 임의조작 및 목적 외 사용 금지 등 안전조치를 적용하고 있는가?
기준 요약도	
운영 방안	**◇ 인터넷과 같은 외부 네트워크를 통한 정보시스템 원격운영은 원칙적으로 금지하고 장애 대응 등 부득이하게 허용하는 경우 보완대책을 마련하고 있는가?** **외부 네트워크를 통한 접근 시 보호 대책**

「**접근통제 관리지침**」 제 ○○조 (외부 네트워크 통제)

① 외부에서 원격으로 정보시스템을 유지보수 하는 것을 원칙적으로 금지하여야 하며 부득이한 경우에는 '원격연결 요청서'를 작성하여 정보시스템 책임자의 승인을 득한 후 일시적인 원격접속을 허용한다.

② 정보시스템 책임자는 원격접속 작업을 관리 감독하며, 작업기록 및 내용을 분기별 1회 점검한다.


원격연결 신청서

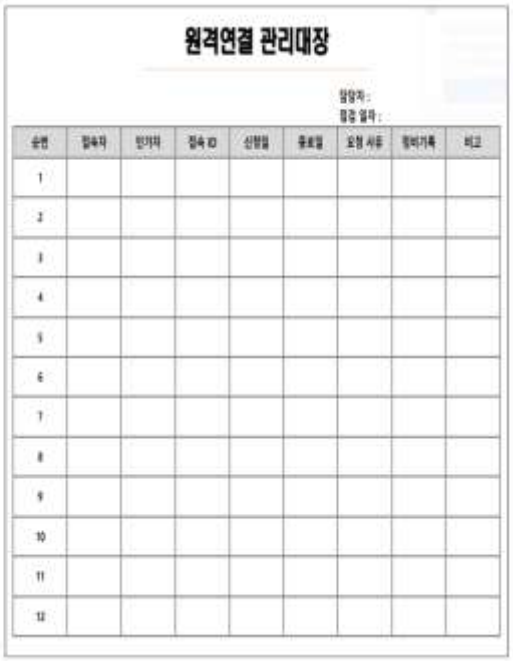
부서 담당자	정보시스템 책임자

신청자		부서	
직급		이용 기간	
요청 사유			

본건은 업무 수행을 위하여 외부 감독 원격 연결을 신청하오니 허락하여 주시기 바랍니다.

년 월 일

신청인: (인)


원격연결 관리대장

담당자:
점검 일자:

순번	접속자	인가자	접속 ID	신청일	종료일	요청 사유	정비기록	비고
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								

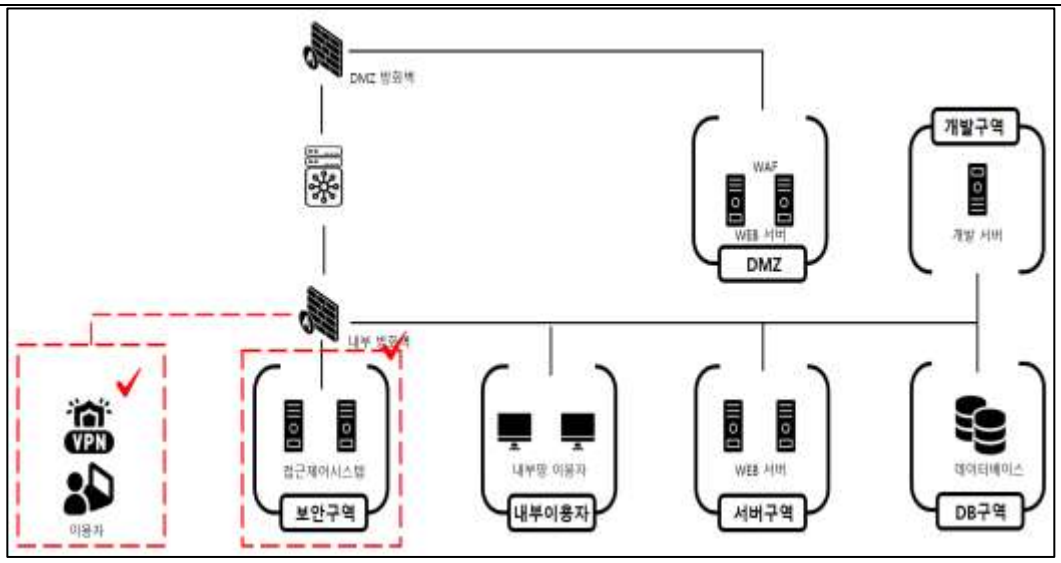
※ 원격연결 신청서 (이해를 돕기 위한 예시)

◇ 내부 네트워크를 통하여 원격으로 정보시스템을 운영하는 경우 특정 단말에 한해서만 접근을 허용하고 있는가?

원격 시스템 우회 접속 차단

① 접속 가능한 단말을 IP 주소, MAC주소 등으로 제한

② 정상적인 원격접속 경로를 우회한 접속 경로 차단 등



※ VPN을 통한 내부 접근 (이해를 돕기 위한 예시)

◇ 재택근무, 원격협업, 스마트워크 등과 같은 원격업무 수행 시 중요정보 유출, 해킹 등 침해사고 예방을 위한 보호 대책을 수립·이행하고 있는가?

(예시) 재택근무, 원격협업, 스마트워크 등 보호 대책 수립·이행

「**접근통제 관리지침**」 제 ○○조 (원격근무 보안관리)

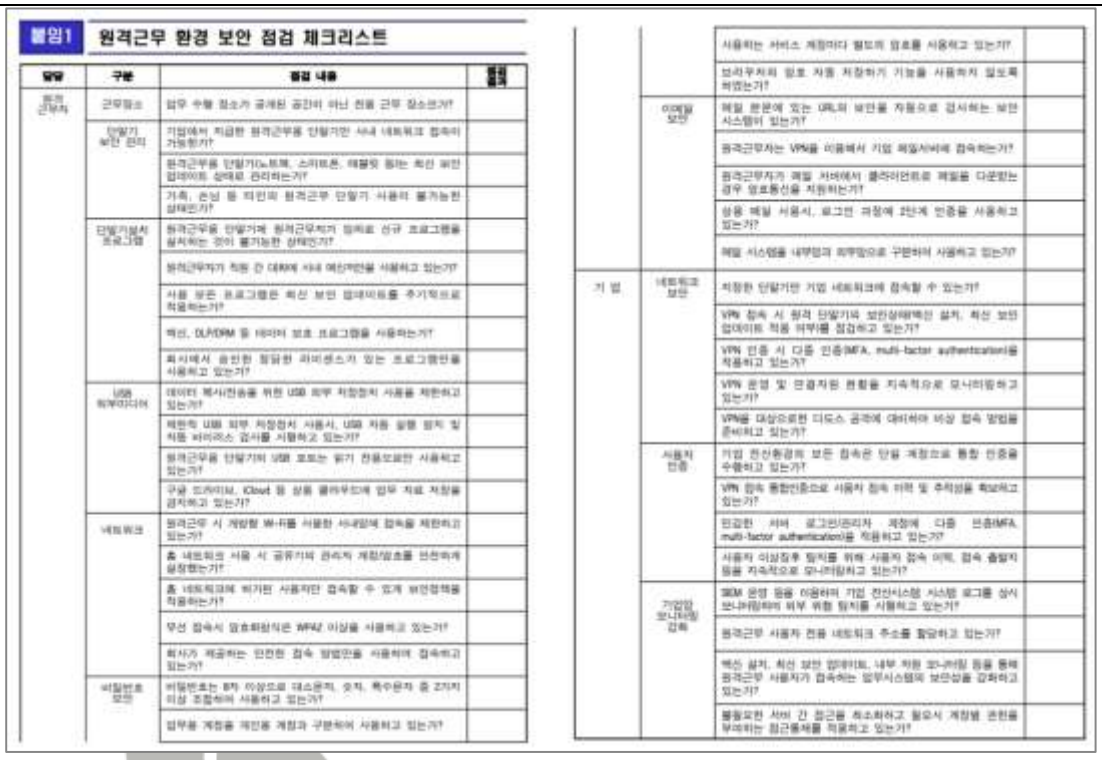
① 원격근무를 지원하기 위한 정보시스템을 도입·운영할 경우 기술적·관리적·물리적 보안대책을 수립하여 시행하여야 한다.

1. 주기적인 원격근무 보안점검을 수행하여 원격근무 보호 대책 확인

원격 근무환경 운영관리 매뉴얼

순번	내용
1	개요
2	근무형태 분류
3	관리적 보호대책
4	기술적 보호대책
5	물리적 보호대책
별첨	원격근무 보안점검 체크리스트

※ 원격 근무환경 운영관리 매뉴얼 (이해를 돕기 위한 예시)



붙임1 원격근무 환경 보안 점검 체크리스트

업무	구분	점검 내용	점검 결과
원격 근무자	근무장소	업무 수행 장소가 공개된 공간이 아닌 전용 근무 장소인가?	
	단말기 보안 관리	기업에서 지급한 원격근무용 단말기만 사내 네트워크 접속이 가능한가?	
		원격근무용 단말기(노트북, 스마트폰, 태블릿 등)는 최신 보안 업데이트 상태로 관리하는가?	
		기록, 손상 등 외인에 의한 원격근무 단말기 사용이 불가능한 상태인가?	
	단말기용서 프로그램	원격근무용 단말기에 원격근무자가 임의로 신규 프로그램을 설치하는 것이 불가능한 상태인가?	
		원격근무자가 적용 간 CMM에 사내 예산제한을 사용하고 있는가?	
		사용 모든 프로그램은 최신 보안 업데이트를 주기적으로 적용하는가?	
		백신, DLP/DRM 등 데이터 보호 프로그램을 사용하는가?	
		회사에서 승인한 정당한 라이센스가 있는 프로그램만을 사용하고 있는가?	
	USB 저장매체	데이터 복사(전송)를 위한 USB 외부 저장장치 사용을 제한하고 있는가?	
		제한적 USB 외부 저장장치 사용시, USB 자동 실행 방지 및 악성 바이러스 검사를 시행하고 있는가?	
		원격근무용 단말기의 USB 또는 읽기 전용으로만 사용하고 있는가?	
		구글 드라이브, iCloud 등 상용 클라우드에 업무 자료 저장을 금지하고 있는가?	
	네트워크	원격근무 시 개인망 Wi-Fi를 사용한 사내망에 접속을 제한하고 있는가?	
		홈 네트워크의 사용 시 공유기의 관리자 계정/암호를 반드시 재설정했는가?	
		홈 네트워크에 허가된 사용자만 접속할 수 있게 비인증책을 적용하는가?	
		무선 접속시 암호화방식은 WPA2 이상을 사용하고 있는가?	
		회사가 제공하는 인증된 접속 방법만을 사용하여 접속하고 있는가?	
	비밀번호 보안	비밀번호는 8자 이상으로 대소문자, 숫자, 특수문자 중 2가지 이상 조합하여 사용하고 있는가?	
		업무용 계정을 개인용 계정과 구분하여 사용하고 있는가?	
		사용하는 서비스 계정마다 별도의 암호를 사용하고 있는가?	
		브라우저의 암호 자동 저장하기 기능을 사용하지 않도록 하였는가?	
	이메일 보안	메일 본문에 있는 URL의 보안을 자동으로 검사하는 보안 시스템이 있는가?	
		원격근무자는 VPN을 이용해서 기업 메일서버에 접속하는가?	
		원격근무자가 메일 서버에서 클라이언트로 메일을 다운받는 경우 암호통신을 지원하는가?	
		상용 메일 사용시, 로그인 과정에 2단계 인증을 사용하고 있는가?	
		메일 시스템을 내부망과 외부망으로 구분하여 사용하고 있는가?	
기 업	네트워크 보안	지정한 단말기만 기업 네트워크에 접속할 수 있는가?	
		VPN 접속 시 원격 단말기의 보안성(백신 설치, 최신 보안 업데이트 적용 여부)를 점검하고 있는가?	
		VPN 인증 시 다중 인증(MFA, multi-factor authentication)을 적용하고 있는가?	
		VPN 운영 및 관리자의 현황을 지속적으로 모니터링하고 있는가?	
		VPN을 대상으로한 디도스 공격에 대비하여 비상 접속 방법을 준비하고 있는가?	
	사용자 인증	기업 전산환경의 모든 접속은 단일 계정으로 통합 인증을 수행하고 있는가?	
		VPN 접속 통합인증으로 사용자 접속 이력 및 추적성을 확보하고 있는가?	
		인증한 서버 로그인/관리자 계정에 다중 인증(MFA, multi-factor authentication)을 적용하고 있는가?	
		사용자 이상징후 탐지를 위해 사용자 접속 이력, 접속 출입지 등을 지속적으로 모니터링하고 있는가?	
	기업망 모니터링 강화	SIEM 운영 등을 이용하여 기업 전산시스템 시스템 로그를 상시 모니터링하여 비부 위협 탐지를 시행하고 있는가?	
		원격근무 사용자 전용 네트워크 주소를 할당하고 있는가?	
		백신 설치, 최신 보안 업데이트, 내부 악성 모니터링 등을 통해 원격근무 사용자가 접속하는 업무시스템의 보안성을 강화하고 있는가?	
		불필요한 서버 간 접근을 최소화하고 필요시 계정별 권한을 부여하는 접근통제를 적용하고 있는가?	

※ 출처: 비대면 업무환경 도입 운영을 위한 보안가이드 (과학기술정보통신부·KISA)

◇ 개인정보처리시스템의 관리, 운영, 개발, 보안 등을 목적으로 원격으로 개인정보처리시스템에 접속하는 단말기는 관리용 단말기로 지정하고 임의조작 및 목적 외 사용 금지 등 안전조치를 적용하고 있는가?

(예시) 원격으로 개인정보처리시스템에 접속하는 단말기 보호 대책 구현

① 관리용 단말기 지정

1. 원격 접속 전용 단말기는 별도 자산번호를 부여하여 '관리용 단말기'로 등록
2. 일반 업무용 PC·모바일과 물리적·논리적으로 분리

② 임의 조작 금지

1. 관리용 단말기에는 USB 저장장치·외장 디스크 자동 마운트 차단
2. 불필요한 서비스(블루투스, 원격데스크탑 등) 비활성화

③ 접근 제어

1. 단말기 로그인에 MFA(비밀번호 + OTP 또는 인증서) 적용
2. 원격 VPN 또는 전용망 접속 전용 계정만 허용, 관리자 승인 로그 보관

④ 보안 설정 강화

1. OS 및 원격 접속 클라이언트는 최신 보안패치 유지
2. 실행파일 화이트리스트 기반 Application Control 구성

⑤ 모니터링 및 로그 관리

1. 단말기 접속 시도·성공·종료 로그 중앙시스템 전송·저장

	2. 비인가 소프트웨어 설치 시도 탐지 및 즉시 차단 알림 ⑥ 목적 외 사용 통제 1. 관리용 단말기에서는 승인된 원격관리 툴(RDP, SSH, VDI 등) 외 접속 금지 2. 업무 범위 외 시스템 및 인터넷 사이트 접근 차단 ⑦ 주기적 점검 1. 분기별 보안설정 일치 여부 및 패치 상태 점검 2. 변경 관리 절차에 따라 승인되지 않은 설정 변경 시 자동 복원

2.6.7 인터넷 접속 통제

세부분야	2.6.7 인터넷 접속 통제
인증 기준	인터넷을 통한 정보 유출, 악성코드 감염, 내부망 침투 등을 예방하기 위하여 주요 정보시스템, 주요 직무 수행 및 개인정보 취급 단말기 등에 대한 인터넷 접속 또는 서비스(P2P, 웹하드, 메신저 등)를 제한하는 등 인터넷 접속 통제 정책을 수립·이행하여야 한다.
주요 확인사항	• 주요 직무 수행 및 개인정보 취급 단말기 등 업무용 PC의 인터넷 접속에 대한 통제 정책을 수립·이행하고 있는가? • 주요 정보시스템(DB 서버 등)에서 불필요한 외부 인터넷 접속을 통제하고 있는가? • 관련 법령에 따라 인터넷망 차단 의무가 부과된 경우 망분리 대상자를 식별하여 안전한 방식으로 인터넷망 차단 조치를 적용하고 있는가?
기준 요약도	
운영 방안	**◇ 주요 직무 수행 및 개인정보 취급 단말기 등 업무용 PC의 인터넷 접속에 대한 통제 정책을 수립·이행하고 있는가?** **인터넷 접속 통제 정책 수립** ① 업무용 PC 인터넷 접속 통제 정책 수립 1. 주요 직무(개인정보 취급, 재무, 개발 등)에 따른 업무용 PC 인터넷 접속 허용 범위를 정의 ② 통제 방식: 승인된 업무 사이트·애플리케이션만 접속 허용, 그 외 차단 ③ 브라우저 보안 설정: 다운로드 파일·스크립트 실행 제한, 외부 링크 차단 플러그인 적용

④ 에이전트 설치: DLP(Data Loss Prevention) 에이전트로 웹 트래픽 모니터링 및 차단

⑤ 모니터링: 인터넷 접속 로그 실시간 수집, 이상 패턴(대량 업로드, 불법 사이트 접속)

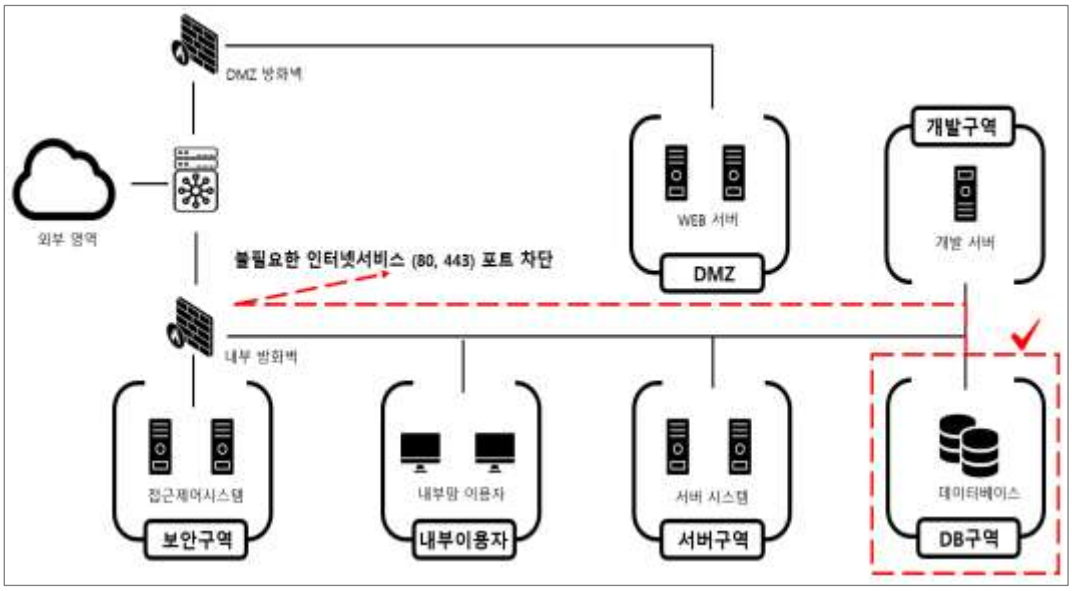
◇ 주요 정보시스템(DB 서버 등)에서 불필요한 외부 인터넷 접속을 통제하고 있는가?

주요 정보시스템 외부 인터넷 차단

① 악성코드 유입, 정보 유출, 역방향 접속 등이 차단되도록 내부 서버(데이터베이스 서버, 파일서버 등)에서 외부 인터넷 접속 제한

1. 네트워크 ACL: DB서버·응용서버의 아웃바운드 트래픽을 허용된 IP·포트만 개방
2. 프록시 게이트웨이: 외부 요청 필요 시 중앙 프록시 경유, 인증·로깅 후 허용
3. 호스트 방화벽: 서버 차원에서 외부 접속 포트(HTTP, SSH 등) 최소화 및 차단

② 불가피한 사유가 있는 경우 위험분석을 통하여 보호 대책을 마련하고 책임자의 승인 후 허용



※ DB서버의 불필요한 인터넷 차단 (이해를 돕기 위한 예시)

◇ 관련 법령에 따라 인터넷 차단 의무가 부과된 경우 망분리 대상자를 식별하여 안전한 방식으로 인터넷 차단 조치를 적용하고 있는가?

망분리 또는 인터넷 차단 조치

① 개인정보처리자 기준

1. 전년도 말 직전 3개월간 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만 명 이상인 개인정보처리자

- 개인정보처리시스템에서 개인정보를 다운로드, 파기, 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터
- 단, 개인정보처리시스템에서 개인정보를 다운로드 및 파기하는 컴퓨터 등의 경우 내부 관리계획에 따른 위험 분석을 실시하여, 위험을 감소시킬 수 있는 보호조치 등 적절한 통제대책을 적용한 경우에는 해당 컴퓨터 등을 인터넷망 차단 조치 대상에서 제외(민감정보, 고유식별정보 등 암호화 대상 정보 처리 시 차단조치 필요)
- 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성·운영하는 경우에는 해당 서비스에 대한 접속 외에는 인터넷을 차단하는 조치 적용

② 금융분야 기준

1. 전자금융감독규정 제15조(해킹 등 방지대책) 준용
- 물리적 망분리: 내부 업무용시스템과 외부 인터넷망 완전 분리
- 전산실 내 정보처리시스템과 운영·개발·보안 목적 단말기의 물리적 분리 등

2. 금융분야 망분리 규제 개선 로드맵
- 2024년 금융위원회는 망분리 규제 개선 로드맵을 발표
- 생성형 AI와 클라우드 기반 서비스(SaaS)의 활용 범위를 확대하고, 금융 회사들이 자율적으로 보안 체계를 강화할 수 있도록 지원할 예정
- 규제 완화는 단계적 개선(생성형 AI 활용 허용, SaaS 활용 범위 확대 등) 추진

※ 참고사항 : 개인정보의 안전성 확보조치 기준(2025.10.31)

① 기존 규정 :

1. 개인정보를 다운로드·파기하거나 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등에 대한 전면적 인터넷망 차단

② 개정 규정 :

1. 위험 분석 기반 차등 적용: 내부관리계획에 따른 위험 분석 실시 후 적절한 통제대책 적용 시 개인정보를 다운로드 또는 파기할 수 있는 개인정보취급자를 인터넷망 차단에서 예외 허용
2. 위험을 저감할 수 있는 보호조치 적용 시 선별적 인터넷망 접속 가능

③ 적용 방법

1. 개인정보 처리환경을 고려한 자율적 위험 평가
2. 위험도에 따른 차등 보안조치 적용
- 위험을 감소시킬 수 있는 보호조치를 적용한 경우, 하기 예시를 고려하여야 함

구분	보호조치 예시
1. 개인정보 파일을 다운로드 할 수 있는 개인정보취급자의 컴퓨터 등	◇ 개인정보처리시스템 접속 시 안전한 인증수단 적용 ◇ 개인정보 파일 저장 시 안전한 암호 알고리즘으로 암호화 ◇ 개인정보 다운로드 건수 제한 ◇ 개인정보 다운로드 권한을 가진 개인정보취급자 최소화 ◇ 개인정보 출력시 마스킹, 안심번호 등 표시제한 조치 적용
2. 개인정보 파일을 파기할 수 있는 개인정보취급자의 컴퓨터 등	◇ 개인정보 파기 권한을 가진 개인정보취급자 최소화 ◇ 개인정보 파기시 관리자 등으로부터 별도 승인을 받도록 설정
※ "예시"는 개인정보처리자가 개인정보에 대한 접근을 통제하기 위해 필요한 조치를 마련하는 과정에서 '필요한 조치'에 해당하는지를 판단할 때 적용해야 하는 안전조치 사례로, 실제 사례에서는 구체적 사실관계에 따라 필요한 부분을 선별적으로 적용할 수 있음	

※ 출처: 개인정보의 안전성 확보조치 기준 안내서(개인정보보호위원회,KISA)

2.7 암호화 적용

2.7.1 암호정책 적용

세부분야	2.7.1 암호정책 적용
인증 기준	개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고 개인정보 및 주요정보의 저장·전송·전달 시 암호화를 적용하여야 한다.
주요 확인사항	• 개인정보 및 주요정보의 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 등이 포함된 암호정책을 수립하고 있는가? • 암호정책에 따라 개인정보 및 주요정보의 저장, 전송, 전달 시 암호화를 수행하고 있는가?
기준 요약도	
운영 방안	**◇ 개인정보 및 주요정보의 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 등이 포함된 암호정책을 수립하고 있는가?** **법적 요구사항을 반영한 암호화 정책 수립** 「**암호관리 매뉴얼**」 제 ○○조 (암호화 기술 선택 기준) ① 데이터 암호화 시에는 법적 요구사항 등을 고려한 안전한 암호화 알고리즘 및 보안 강도를 선택하야 한다. 시스템 관리 및 기술적 한계 등으로 적용이 불가능한 경우 정보보호 책임자의 승인을 받아 예외로 할 수 있다. 1. 대칭키 암호 알고리즘: SEED, ARIA-128/192/256, AES-128/192/256, HIGHT, LEA 2. 공개키 암호 알고리즘: RSAES-OAEP, RSAES-PKCS1 3. 일방향 암호 알고리즘: SHA-256/384/512

<table>
<tr><th colspan="2" rowspan="2">구분</th><th colspan="2">개인정보 보호법에 따른 암호화 대상</th></tr>
<tr><th>이용자가 아닌 정보주체의 개인정보</th><th>이용자의 개인정보</th></tr>
<tr><td rowspan="2">정보통신망을 통한 송·수신 시</td><td>정보통신망</td><td colspan="2">인증정보(비밀번호, 생체인식정보 등)</td></tr>
<tr><td>인터넷망</td><td colspan="2">개인정보
※ 단, 종전의 개인정보의 안전성 확보조치 기준 적용대상의 경우 2024.9.15 시행</td></tr>
<tr><td rowspan="4">저장 시</td><td rowspan="2">저장 위치 무관</td><td colspan="2">인증정보(비밀번호, 생체인식정보 등)
※ 단, 비밀번호는 일방향암호화</td></tr>
<tr><td colspan="2">주민등록번호
※ 법 제24조의2 제2항에 따라 암호화</td></tr>
<tr><td>인터넷구간, DMZ</td><td>고유식별정보</td><td rowspan="2">주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 생체인식정보
※ 저장 위치 무관</td></tr>
<tr><td>내부망</td><td>※ 단, 주민등록번호 외의 고유식별정보를 내부망에 저장하는 경우 개인정보영향평가의 결과 또는 위험도 분석에 따른 결과에 따라 암호화의 적용여부 및 적용범위를 정하여 시행 가능</td></tr>
<tr><td colspan="2">개인정보취급자 컴퓨터, 모바일기기, 보조저장매체 등에 저장 시</td><td>고유식별정보, 생체인식정보</td><td>개인정보</td></tr>
</table>

※ 개인정보보호법 기준 법적 암호화 대상

※ 연계정보 처리 시 고려사항

① 「**연계정보의 생성·처리 등에 관한 기준**」제11조(연계정보 이용기관의 안전조치)에 따른 연계정보 암호화 조치

1. 연계정보를 안전하게 저장.전송할 수 있는 암호화 기술 적용에 관한 사항

- 연계정보를 정보통신망을 통하여 인터넷망 구간으로 송.수신하는 경우 안전한 암호알고리즘으로 암호화

- 10만 명 이상의 이용자 연계정보를 보유한 대기업.중견기업.법 제44조의5제1항 제1호에 해당하는 공공기관 등 또는 100만 명 이상의 이용자 연계정보를 보유한 중소기업.단체는 연계정보를 안전한 알고리즘으로 암호화하여 저장

② 연계정보 저장 시 암호화 규정은 예산 확보, 준비 기간 등을 고려하여 2027.05.01부터 시행

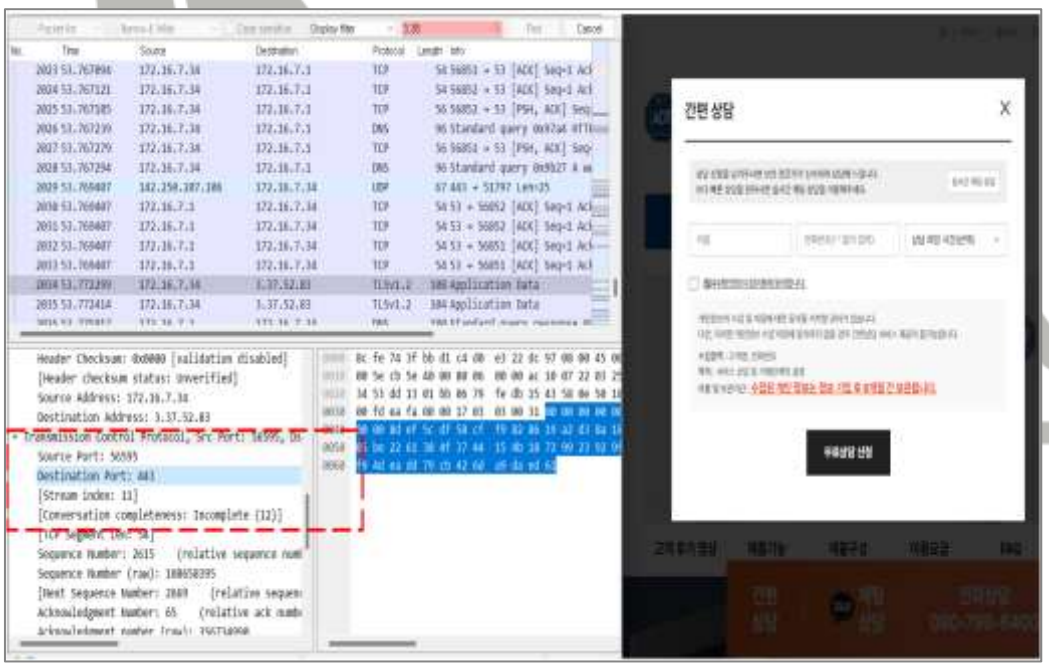
◇ 암호정책에 따라 개인정보 및 주요정보의 저장, 전송, 전달 시 암호화를 수행하고 있는가?

개인정보 및 중요정보의 저장, 전송, 전달 시 암호화

「**암호관리 매뉴얼**」 제○○조 (암호화 기술 적용 대상)

① 이용자 데이터의 무결성을 보장하기 위해 개인정보 및 중요정보의 저장, 전송, 전달 시 암호화를 수행하여야 한다.

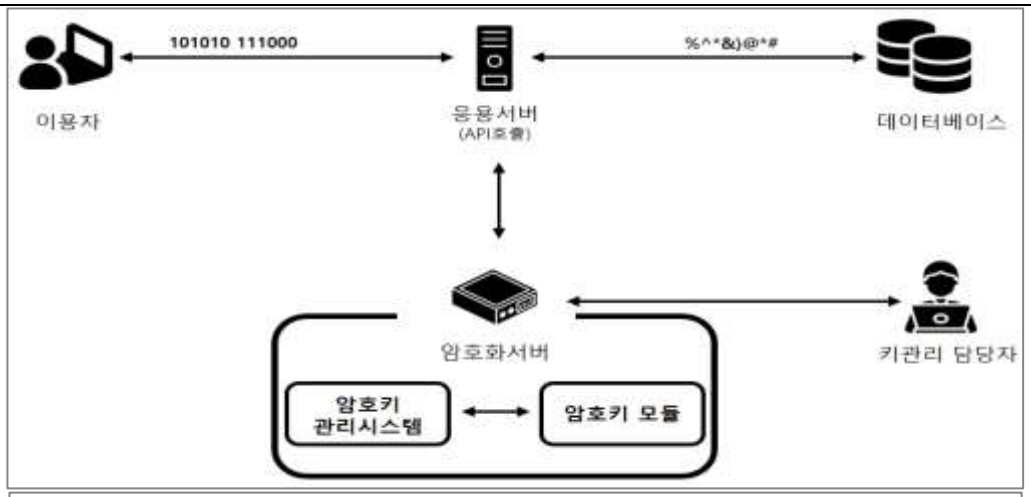
1. 정보통신망을 통한 전송
2. 보조저장매체로 전달
3. 개인정보처리시스템 저장
4. 업무용 컴퓨터 및 모바일 기기 저장



※ 중요 개인정보 전송구간 암호화 (이해를 돕기 위한 예시)

2.7.2 암호키 관리

세부분야	2.7.2 암호키 관리
인증 기준	암호키의 안전한 생성·이용·보관·배포·파기를 위한 관리 절차를 수립·이행하고, 필요시 복구 방안을 마련하여야 한다.
주요 확인사항	• 암호키 생성, 이용, 보관, 배포, 변경, 복구, 파기 등에 관한 절차를 수립·이행하고 있는가? • 암호키는 필요시 복구가 가능하도록 별도의 안전한 장소에 보관하고 암호키 사용에 관한 접근권한을 최소화하고 있는가?
기준 요약도	
운영 방안	**◇ 암호키 생성, 이용, 보관, 배포, 변경, 복구, 파기 등에 관한 절차를 수립·이행하고 있는가?** **(예시) 암호키 관리 절차 수립** 「**암호관리 매뉴얼**」 제 ○○조 (암호키 관리) ① 암호화 키는 기밀 데이터를 암호화할 경우 정보보호 책임자의 승인을 받아 생성하고 '암호화 키 관리 대장'에 기록한다. ② 접근이 인가되지 않은 사용자는 암호화 키를 사용할 수 없도록 통제구역 등에 안전하게 관리해야 한다. ③ 암호화 키는 노출 위협을 최소화하기 위해 1년마다 변경해야 한다. 단, 정보보호 책임자가 암호화 키 변경이 필요하다고 판단될 경우 변경할 수 있다. ④ 암호화 키는 사용 용도가 종료되거나 사용 주기가 만료된 경우 폐기한다. 암호화 키는 부서 정보보호담당자가 폐기하고 '암호화 키 관리 대장'에 기록한다.



암호 키 관리대장

순번	일자		용도	암호키 저장위치	부서 및 사용자	부서 정보보호 담당자
1	키생성					
	키폐기					
	키복구					
2	키생성					
	키폐기					
	키복구					
3	키생성					
	키폐기					
	키복구					

※ 암호 키 관리 (이해를 돕기 위한 예시)

◇ 암호키는 필요시 복구가 가능하도록 별도의 안전한 장소에 보관하고 암호키 사용에 관한 접근권한을 최소화하고 있는가?

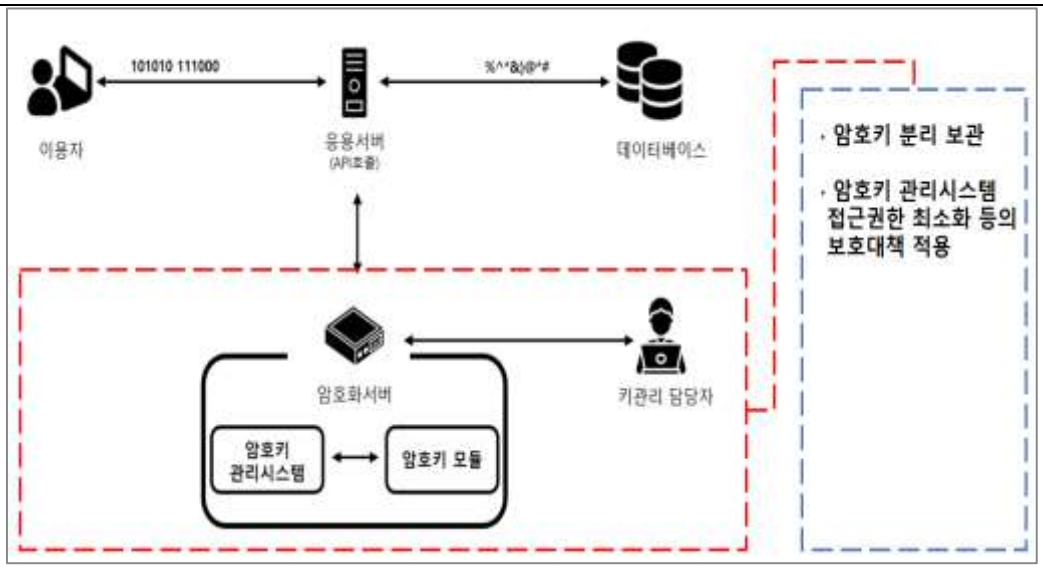
암호키 접근 제어

① 암호키는 필요시 복구가 가능하도록 별도의 안전한 장소에 보관하고 암호키 사용에 관한 접근권한을 최소화하여야 한다.

1. 암호키는 별도 매체(모듈/파일 포함)에서 관리
2. 암호키를 별도 물리서버에 백업
3. 데이터베이스 적용 시 암호키 노출 금지
4. 암/복호화 시스템을 통해 관리자 개입없이 배포 설정
5. 소스에 암호키를 하드코딩 하지 않도록 설정
6. 암호키 네트워크로 전송 시 암호화 등

② 암호키 손상 시 시스템 또는 암호화된 정보의 복구를 위하여 암호키는 별도의 매체에 저장한 후 안전한 장소에 보관(암호키 관리 시스템, 물리적으로 분리된 곳 등)

1. 암호키에 대한 접근권한 최소화 및 접근 모니터링



※ 암호 키 분리 보관 및 보호 대책 구현 (이해를 돕기 위한 예시)

2.8 정보시스템 도입 및 개발 보안

2.8.1 보안 요구사항 정의

세부분야	2.8.1 보안 요구사항 정의
인증 기준	정보시스템의 도입·개발·변경 시 정보보호 및 개인정보보호 관련 법적 요구사항, 최신 보안취약점, 안전한 코딩 방법 등 보안 요구사항을 정의하고 적용하여야 한다.
주요 확인사항	• 정보시스템을 신규로 도입·개발 또는 변경하는 경우 정보보호 및 개인정보보호 측면의 타당성 검토 및 인수 절차를 수립·이행하고 있는가? • 정보시스템을 신규로 도입·개발 또는 변경하는 경우 법적 요구사항, 최신 취약점 등을 포함한 보안 요구사항을 명확히 정의하고 설계 단계에서부터 반영하고 있는가? • 정보시스템의 안전한 구현을 위한 코딩 표준을 수립하여 적용하고 있는가?
기준 요약도	
운영 방안	**◇ 정보시스템을 신규로 도입·개발 또는 변경하는 경우 정보보호 및 개인정보보호 측면의 타당성 검토 및 인수 절차를 수립·이행하고 있는가?** **보안 요구사항 타당성 검토 및 인수 절차를 수립·이행** ① 새로운 정보시스템(서버, 네트워크 장비, 상용 소프트웨어 패키지) 및 보안시스템 도입 시 도입 타당성 분석 등의 내용이 포함된 도입 계획 수립 1. 현재 시스템 자원의 이용률, 사용량, 능력 한계에 대한 분석 2. 성능, 안정성, 보안성, 신뢰성 및 기존 시스템과의 호환성, 상호 운용성 요건 3. 개인정보처리시스템에 해당될 경우 개인정보보호법(개인정보의 안전성 확보조치

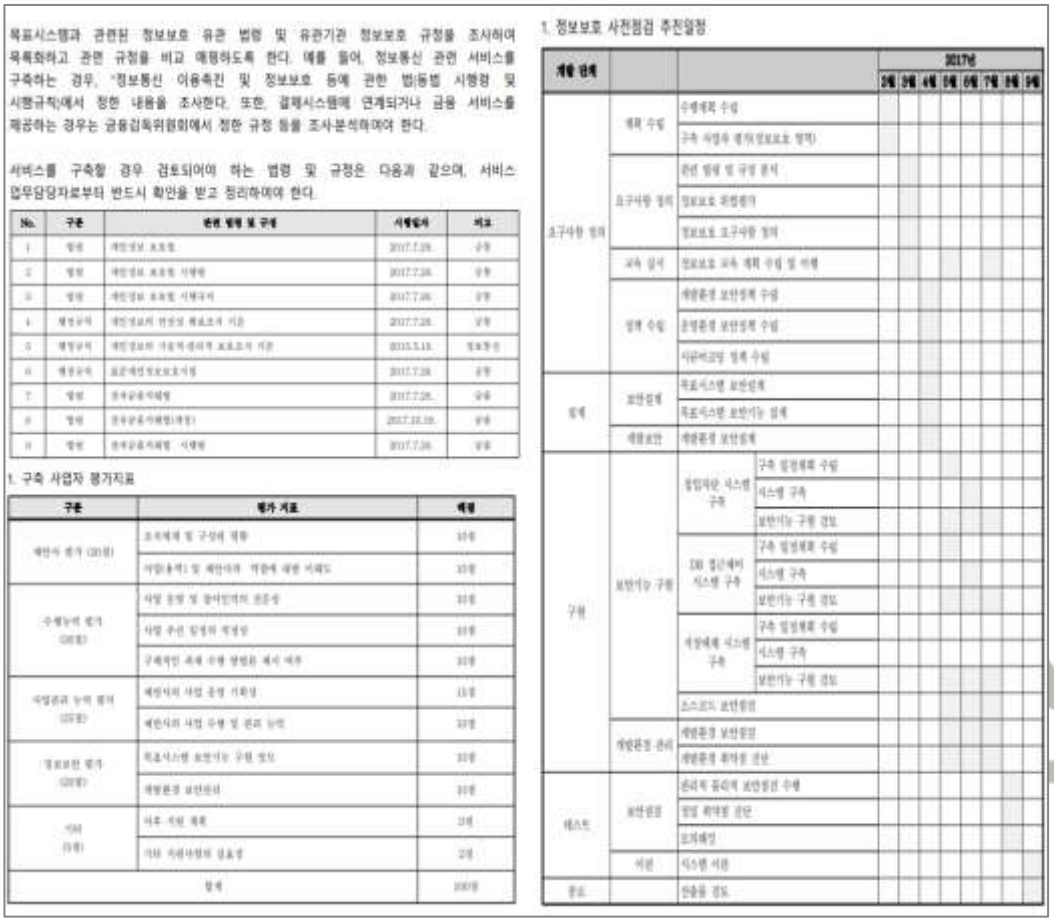
기준, 개인정보의 기술적·관리적 보호조치 기준 고시 포함) 등에서 요구하는 법적 요구사항 준수

② 정보보호 및 개인정보보호 측면의 요구사항을 제안요청서(RFP)에 반영하고 업체 또는 제품 선정 시 기준으로 활용

③ 정보시스템 인수 여부를 판단하기 위한 시스템 인수기준 수립

1. 도입 계획 수립 시 정의된 성능, 보안성, 법적 요구사항 등을 반영한 인수 승인 기준 수립

2. 시스템 도입 과정에서 인수기준을 준수하도록 구매계약서 등에 반영

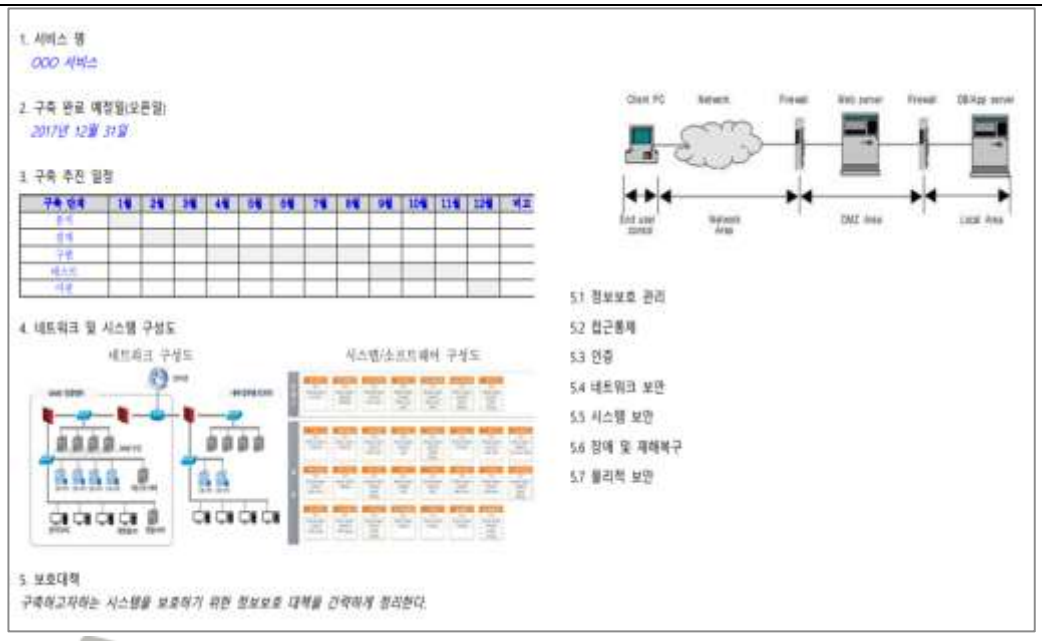


※ 출처: 정보보호 사전점검 해설서 (KISA)

◇ 정보시스템을 신규로 도입·개발 또는 변경하는 경우 법적 요구사항, 최신 취약점 등을 포함한 보안 요구사항을 명확히 정의하고 설계 단계에서부터 반영하고 있는가?

정보시스템 도입·개발 시 설계 단계에서 보안 요구사항 반영

① 목표 시스템을 구축·개발·기획 단계에서 기본적인 정보보호 요건을 정의하고, 요구사항을 제안 요청서에 반영

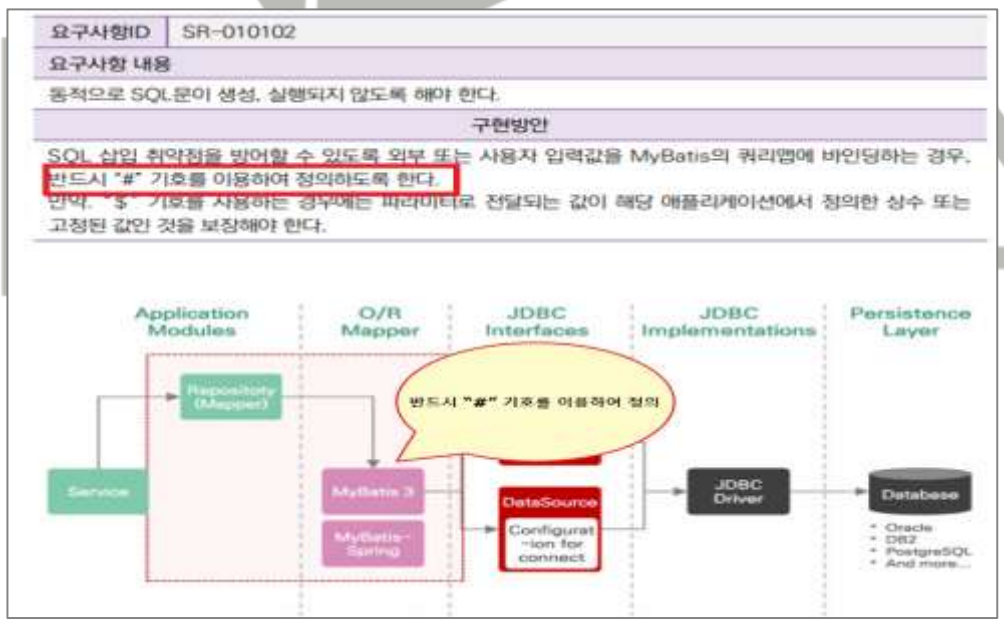


※ 출처: 정보보호 사전점검 해설서 (KISA)

◇ 정보시스템의 안전한 구현을 위한 코딩 표준을 수립하여 적용하고 있는가?

개발 단계에서부터 안전한 코딩 표준 적용

① 분석·설계 단계에서 안전한 코딩 표준 및 규약을 마련하여 보안 요구항목 적용




```
<select id="selectUser" parameterType="userVO"
 resultMap="userVO"> select * from users where id = #{userId}
</select>
```

※ 출처: 소프트웨어 보안약점 진단가이드 (행정안전부·KISA)

2.8.2 보안 요구사항 검토 및 시험

세부분야	2.8.2 보안 요구사항 검토 및 시험
인증 기준	사전 정의된 보안 요구사항에 따라 정보시스템이 도입 또는 구현되었는지를 검토하기 위하여 법적 요구사항 준수, 최신 보안취약점 점검, 안전한 코딩 구현, 개인정보 영향평가 등의 검토 기준과 절차를 수립·이행하고, 발견된 문제점에 대한 개선 조치를 수행하여야 한다.
주요 확인사항	• 정보시스템의 도입, 개발, 변경 시 분석 및 설계 단계에서 정의한 보안 요구사항이 효과적으로 적용되었는지를 확인하기 위한 시험을 수행하고 있는가? • 정보시스템이 안전한 코딩 기준 등에 따라 안전하게 개발되었는지를 확인하기 위한 취약점 점검이 수행되고 있는가? • 시험 및 취약점 점검 과정에서 발견된 문제점이 신속하게 개선될 수 있도록 개선 계획 수립, 이행점검 등의 절차를 이행하고 있는가? • 공공기관은 관련 법령에 따라 개인정보처리시스템 신규 개발 및 변경 시 분석·설계 단계에서 영향평가기관을 통하여 영향평가를 수행하고 그 결과를 개발 및 변경 시 반영하고 있는가?
기준 요약도	
운영 방안	**◇ 정보시스템의 도입, 개발, 변경 시 분석 및 설계 단계에서 정의한 보안 요구사항이 효과적으로 적용되었는지를 확인하기 위한 시험을 수행하고 있는가?** **정보시스템을 인수하기 전 사전 정의한 인수기준과의 적합성 여부를 테스트** ① 정보시스템 인수 전 인수기준 적합성 여부를 확인하기 위한 시험 수행 1. 정보시스템이 사전에 정의한 보안 요구사항을 만족하여 개발·변경 및 도입되었는지 확인하기 위한 인수기준 및 절차 수립 2. 정보시스템을 인수하기 전에 사전 정의한 인수기준과의 적합성 여부를 테스트 등을

통하여 확인한 후 인수 여부를 결정

3. 시스템 보안 설정, 불필요한 디폴트 계정 제거 여부, 최신 보안취약점 패치 여부 등 확인 필요

② 개발·변경 및 구현된 기능이 사전에 정의된 보안 요구사항을 충족하는지 시험 수행

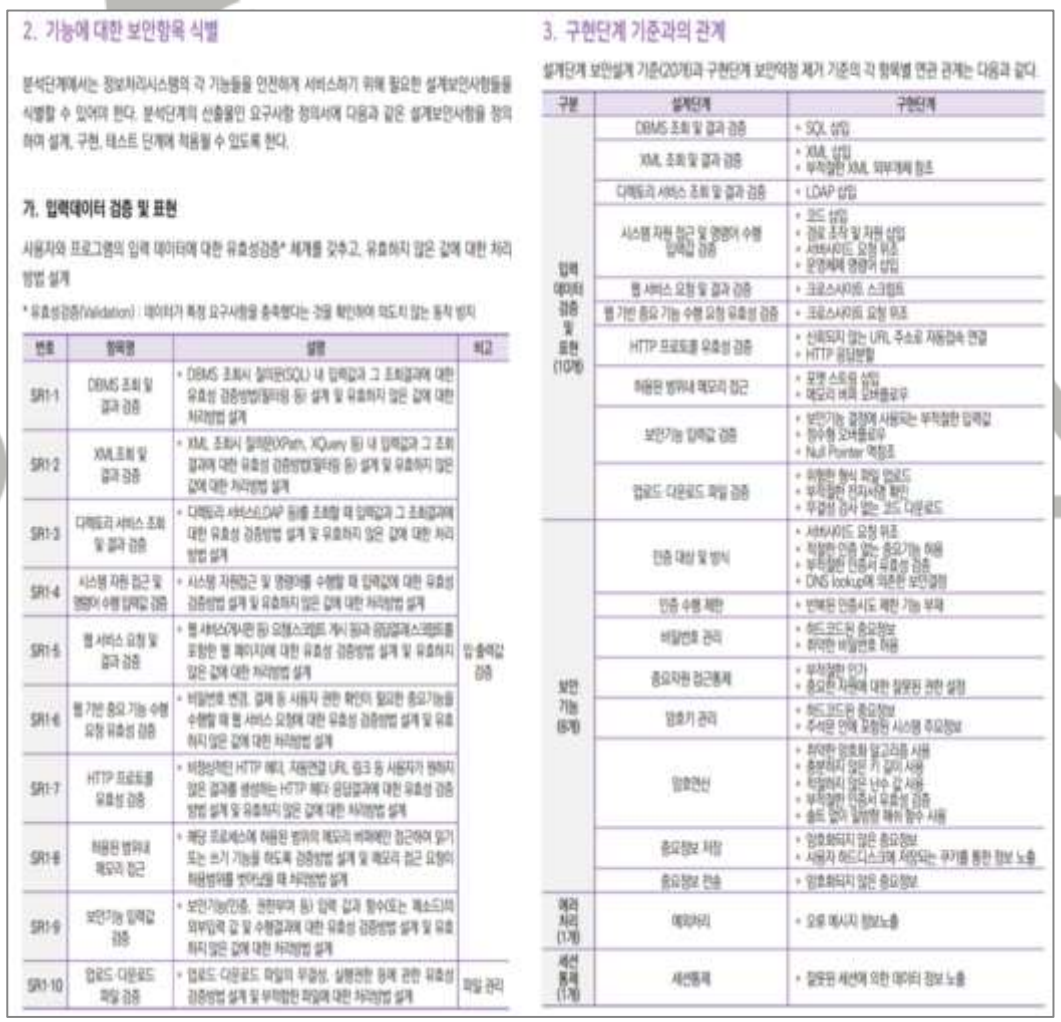
1. 시험 계획서, 체크리스트, 시험 결과서 등에 반영

◇ 정보시스템이 안전한 코딩 기준 등에 따라 안전하게 개발되었는지를 확인하기 위한 취약점 점검이 수행되고 있는가?

안전한 코딩 점검

① 시스템이 안전한 코딩 표준에 따라 구현하는지 소스코드 검증

② 코딩이 완료된 프로그램은 운영 환경과 동일한 환경에서 취약점 점검도구 또는 모의 진단을 통한 취약점 노출 여부 점검



2. 기능에 대한 보안항목 식별

분석단계에서는 정보처리시스템의 각 기능들을 안전하게 서비스하기 위해 필요한 설계보안사항들을 식별할 수 있어야 한다. 분석단계의 산출물인 요구사항 정의서에 다음과 같은 설계보안사항을 정의하여 설계, 구현, 테스트 단계에 적용될 수 있도록 한다.

가. 입력데이터 검증 및 표현

사용자와 프로그램의 입력 데이터에 대한 유효성검증* 체계를 갖추고, 유효하지 않은 값에 대한 처리 방법 설계

* 유효성검증(Validation) : 데이터가 특정 요구사항을 충족했다는 것을 확인하여 악도적 않는 동작 방지

번호	항목명	설명	비고
SR1-1	DBMS 조회 및 결과 검증	• DBMS 조회시 질의문(SQL) 내 입력값과 그 조회결과에 대한 유효성 검증방법(필터링 등) 설계 및 유효하지 않은 값에 대한 처리방법 설계	입출력값 검증
SR1-2	XML조회 및 결과 검증	• XML 조회시 질의문(XPath, XQuery 등) 내 입력값과 그 조회결과에 대한 유효성 검증방법(필터링 등) 설계 및 유효하지 않은 값에 대한 처리방법 설계	
SR1-3	디렉토리 서비스 조회 및 결과 검증	• 디렉토리 서비스(LDAP 등)를 조회할 때 입력값과 그 조회결과에 대한 유효성 검증방법 설계 및 유효하지 않은 값에 대한 처리 방법 설계	
SR1-4	시스템 자원 접근 및 명령어 수행 입력값 검증	• 시스템 자원접근 및 명령어를 수행할 때 입력값에 대한 유효성 검증방법 설계 및 유효하지 않은 값에 대한 처리방법 설계	
SR1-5	웹 서비스 요청 및 결과 검증	• 웹 서버스(게시판 등) 오픈소스(모듈, 게시 등)과 관련(패스워드를 포함한 웹 페이지에 대한 유효성 검증방법 설계 및 유효하지 않은 값에 대한 처리방법 설계	
SR1-6	웹 기반 중요 기능 수행 요청 유효성 검증	• 비밀번호 변경, 결제 등 사용자 권한 확인이 필요한 중요기능을 수행할 때 웹 서비스 요청에 대한 유효성 검증방법 설계 및 유효하지 않은 값에 대한 처리방법 설계	
SR1-7	HTTP 프로토콜 유효성 검증	• 비정상적인 HTTP 헤더, 자동연결 URL, 링크 등 사용자가 원하지 않은 결과를 생성하는 HTTP 헤더 응답결과에 대한 유효성 검증 방법 설계 및 유효하지 않은 값에 대한 처리방법 설계	
SR1-8	허용된 범위내 폐도의 접근	• 해당 프로세스에 허용된 범위의 폐도의 비허용한 접근여부 및/또는 쓰기 기능을 허도록 검증방법 설계 및 폐도의 접근 요청이 허용범위를 벗어났을 때 처리방법 설계	
SR1-9	보안기능 입력값 검증	• 보안기능(인증, 권한부여 등) 입력 값과 함수(또는 메소드)의 외부입력 값 및 수행결과에 대한 유효성 검증방법 설계 및 유효하지 않은 값에 대한 처리방법 설계	
SR1-10	업로드·다운로드 파일 검증	• 업로드·다운로드 파일의 무결성, 실행권한 등에 관한 유효성 검증방법 설계 및 부적합한 파일에 대한 처리방법 설계	파일 관리

3. 구현단계 기준과의 관계

설계단계 보안설계 기준(20개)과 구현단계 보안약점 제거 기준의 각 항목별 연관 관계는 다음과 같다.

구분	설계단계	구현단계
입력데이터 검증 및 표현 (10개)	DBMS 조회 및 결과 검증	• SQL 삽입
	XML 조회 및 결과 검증	• XML 삽입 • 부적절한 XML 외부개체 참조
	디렉토리 서비스 조회 및 결과 검증	• LDAP 삽입
	시스템 자원 접근 및 명령어 수행 입력값 검증	• 코드 삽입 • 경로 조작 및 자원 삽입 • 서버사이드 요청 위조 • 운영체제 명령어 삽입
	웹 서비스 요청 및 결과 검증	• 크로스사이트 스크립트
	웹 기반 중요 기능 수행 요청 유효성 검증	• 크로스사이트 요청 위조
	HTTP 프로토콜 유효성 검증	• 신뢰되지 않는 URL 주소로 자동접속 연결 • HTTP 응답분할
	허용된 범위내 폐도의 접근	• 포맷 스트링 삽입 • 폐도의 버퍼 오버플로우
	보안기능 입력값 검증	• 보안기능 결정에 사용되는 부적절한 입력값 • 정수형 오버플로우 • Null Pointer 역참조
	업로드·다운로드 파일 검증	• 위험한 형식 파일 업로드 • 부적절한 전자서명 확인 • 무결성 검사 없는 코드 다운로드
보안기능 (6개)	인증 대상 및 방식	• 서버사이드 요청 위조 • 적절한 인증 없는 중요기능 허용 • 부적절한 인증서 유효성 검증 • DNS lookup에 의존한 보안결정
	인증 수행 제한	• 반복된 인증시도 제한 기능 부재
	비밀번호 관리	• 하드코드된 중요정보 • 취약한 비밀번호 허용
	중요자원 접근통제	• 부적절한 인가 • 중요한 자원에 대한 잘못된 권한 설정
	암호키 관리	• 하드코드된 중요정보 • 주석문 안에 포함된 시스템 주요정보
	암호연산	• 취약한 암호화 알고리즘 사용 • 충분하지 않은 키 길이 사용 • 적절하지 않은 난수 값 사용 • 부적절한 인증서 유효성 검증 • 솔트 없이 일방향 해시 함수 사용
	중요정보 저장	• 암호화되지 않은 중요정보 • 사용자 하드디스크에 저장되는 쿠키를 통한 정보 노출
	중요정보 전송	• 암호화되지 않은 중요정보
예외처리 (1개)	예외처리	• 오류 메시지 정보노출
세션통제 (1개)	세션통제	• 잘못된 세션에 의한 데이터 정보 노출

※ 출처: 소프트웨어 보안약점 진단가이드 (행정안전부·KISA)

◇ 시험 및 취약점 점검 과정에서 발견된 문제점이 신속하게 개선될 수 있도록 개선 계획 수립, 이행점검 등의 절차를 이행하고 있는가?

도출 취약점 개선 계획 수립

① 발견된 문제점은 시스템 오픈 전에 개선될 수 있도록 개선 계획 수립, 내부 보고, 이행점검 등의 절차 수립·이행

② 불가피한 사유로 시스템 오픈 전에 개선이 어려울 경우에는 이에 따른 영향도 평가, 보완대책, 내부보고 등 위험을 줄일 수 있는 대책 마련

◇ 공공기관은 관련 법령에 따라 개인정보처리시스템 신규 개발 및 변경 시 분석·설계 단계에서 영향평가기관을 통하여 영향평가를 수행하고 그 결과를 개발 및 변경 시 반영하고 있는가?

영향평가 의무 대상

① 민감정보 또는 고유식별정보의 처리가 수반되는 경우 5만 명 이상의 개인정보파일

② 다른 개인정보파일과 연계하려는 경우로서 50만 명 이상의 개인정보파일

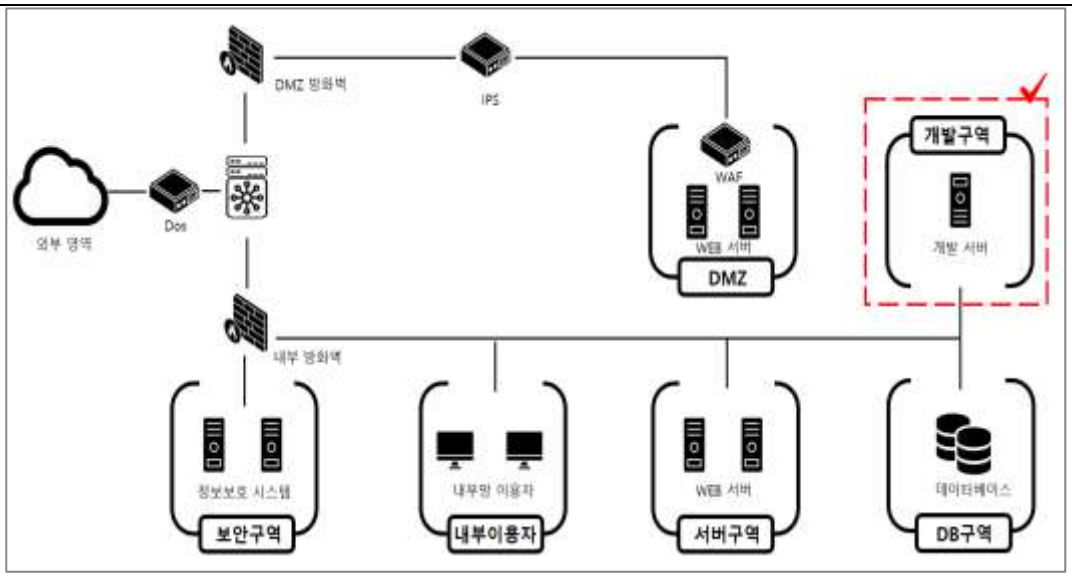
③ 100만 명 이상의 정보주체에 관한 개인정보파일

④ 영향평가를 받은 후 개인정보파일의 운용체계를 변경하는 경우 변경된 부분에 대해서는 영향평가를 실시

※ 출처: 개인정보 영향평가 수행안내서 (개인정보보호위원회·KISA)

2.8.3 시험과 운영 환경 분리

세부분야	2.8.3 시험과 운영 환경 분리
인증 기준	개발 및 시험 시스템은 운영 시스템에 대한 비인가 접근 및 변경의 위험을 감소시키기 위하여 원칙적으로 분리하여야 한다.
주요 확인사항	• 정보시스템의 개발 및 시험 시스템을 운영 시스템과 분리하고 있는가? • 불가피한 사유로 개발과 운영 환경의 분리가 어려운 경우 상호 검토, 상급자 모니터링, 변경 승인, 책임 추적성 확보 등의 보안대책을 마련하고 있는가?
기준 요약도	
운영 방안	**◇ 정보시스템의 개발 및 시험 시스템을 운영 시스템과 분리하고 있는가?** **(예시) 개발보안에 대한 정책 및 절차** 「**개발보안 지침**」 제 ○○조 (개발 환경 분리) ① 개발/시험 환경과 운영 환경을 분리하기 어려운 경우 다음 사항을 포함한 보안대책을 수립한다. 1. 개발/시험으로 인하여 영향을 받는 부분에 대한 범위 산정 2. 개발/시험의 오류로 인하여 발생할 수 있는 장애의 유형 및 복구 대책 3. 장애 발생 시 대응을 위한 상세한 시험 절차 수립 4. 개발/시험 중 서비스 운영의 정상 여부를 지속적으로 모니터링하기 위한 대책 5. 운영 환경에서 개발/시험을 수행하기 전에 정보보호 책임자 등으로부터의 승인 6. 운영 데이터가 시험 데이터로 사용되는 경우 운영 데이터 보호를 위한 대책



※ 개발 환경 분리 (이해를 돕기 위한 예시)

◇ 불가피한 사유로 개발과 운영 환경의 분리가 어려운 경우 상호 검토, 상급자 모니터링, 변경 승인, 책임 추적성 확보 등의 보안대책을 마련하고 있는가?

개발과 운영 환경의 분리가 어려울 경우 보완 통제 수단 적용

① 직무자 간 상호 검토

② 변경 승인

③ 상급자의 모니터링 및 감사

④ 백업 및 복구 방안, 책임 추적성 확보 등

2.8.4 시험 데이터 보안

세부분야	2.8.4 시험 데이터 보안
인증 기준	시스템 시험 과정에서 운영 데이터의 유출을 예방하기 위하여 시험 데이터의 생성과 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립·이행하여야 한다.
주요 확인사항	• 정보시스템의 개발 및 시험 과정에서 실제 운영 데이터의 사용을 제한하고 있는가? • 불가피하게 운영 데이터를 시험 환경에서 사용할 경우 책임자 승인, 접근 및 유출 모니터링, 시험 후 데이터 삭제 등의 통제 절차를 수립·이행하고 있는가?
기준 요약도	
운영 방안	**◇ 정보시스템의 개발 및 시험 과정에서 실제 운영 데이터의 사용을 제한하고 있는가?** **시험용 데이터 사용** 「**개발보안 지침**」 제 ○○조 (테스트 데이터 관리) ① 테스트를 위하여 실 데이터를 이용하고자 할 경우에는 '테스트 데이터 사용 요청서'를 작성하여 정보보호 관리자의 승인을 득해야 한다. ② 테스트 데이터에 사용자의 중요정보가 포함될 경우 제공받은 실 데이터를 익명화하여 테스트 데이터로 변환한 후 사용한다. 단, 실데이터를 변환하지 않고 테스트를 할 경우에는 정보보호 관리자의 승인을 득해야 한다.

※ 테스트 데이터 사용 신청서 (이해를 돕기 위한 예시)

◇ 불가피하게 운영 데이터를 시험 환경에서 사용할 경우 책임자 승인, 접근 및 유출 모니터링, 시험 후 데이터 삭제 등의 통제 절차를 수립·이행하고 있는가?

운영 데이터 사용 시 통제 절차 수립

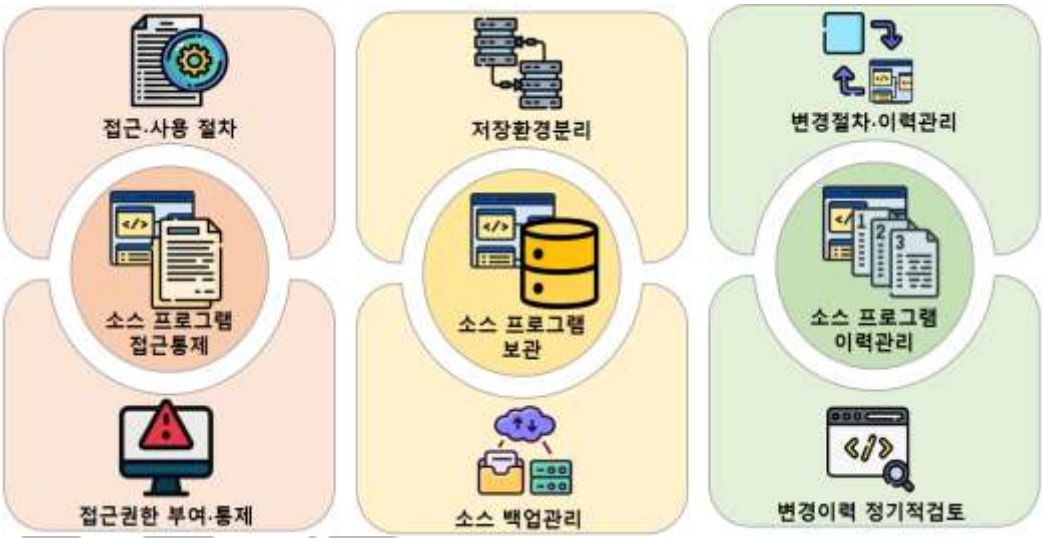
① 운영 데이터 사용승인 절차 마련: 데이터 중요도에 따른 보고 및 승인체계 정의 등

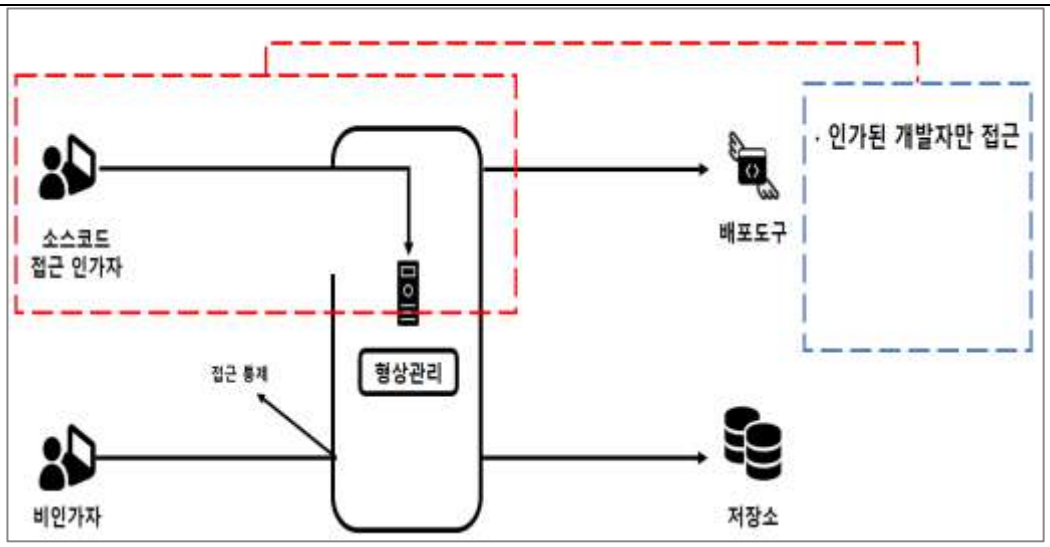
② 시험 기한 만료 후 데이터 폐기 절차 마련 및 이행

③ 운영 데이터 사용에 대한 시험 환경에서의 접근통제 대책 적용

④ 운영 데이터 복제·사용에 대한 모니터링 및 정기검토 수행 등

2.8.5 소스 프로그램 관리

세부분야	2.8.5 소스 프로그램 관리
인증 기준	소스 프로그램은 인가된 사용자만이 접근할 수 있도록 관리하고, 운영 환경에 보관하지 않는 것을 원칙으로 하여야 한다.
주요 확인사항	• 비인가자에 의한 소스 프로그램 접근을 통제하기 위한 절차를 수립·이행하고 있는가? • 소스 프로그램은 장애 등 비상시를 대비하여 운영 환경이 아닌 곳에 안전하게 보관하고 있는가? • 소스 프로그램에 대한 변경 이력을 관리하고 있는가?
기준 요약도	
운영 방안	**◇ 비인가자에 의한 소스 프로그램 접근을 통제하기 위한 절차를 수립·이행 하고 있는가?** **소스 프로그램 접근 통제 절차 수립** 「**개발보안 관리지침**」 제 ○○조 (소스 프로그램 관리) ① 소스 프로그램은 인가된 사용자만이 접근할 수 있도록 관리하고 비인가자의 소스 프로그램 접근을 다음과 같이 통제하여야 한다. 1. 소스코드가 보관된 서버에 대한 접근통제 적용 2. 소스 프로그램 접근 시 인가자만 접근 가능하도록 접근권한 부여 3. SW개발과정 형상관리 도구: CVN·SVN·Git



※ 형상관리시스템 접근제어 (이해를 돕기 위한 예시)

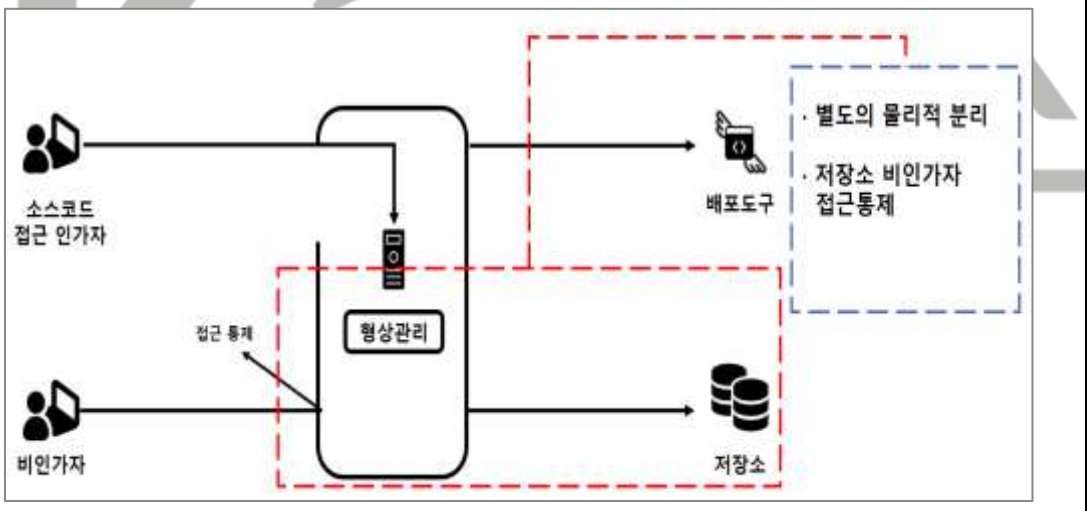
◇ 소스 프로그램은 장애 등 비상시를 대비하여 운영 환경이 아닌 곳에 안전하게 보관하고 있는가?

소스 프로그램 백업 관리

① 최신 소스 프로그램 및 이전 소스 프로그램에 대한 백업 보관

② 운영 환경이 아닌 별도의 환경에 저장·관리

③ 소스 프로그램 백업본에 대한 비인가자의 접근 통제



※ 소스 프로그램 별도 분리 공간 저장 보관관리 (이해를 돕기 위한 예시)

◇ 소스 프로그램에 대한 변경 이력을 관리하고 있는가?

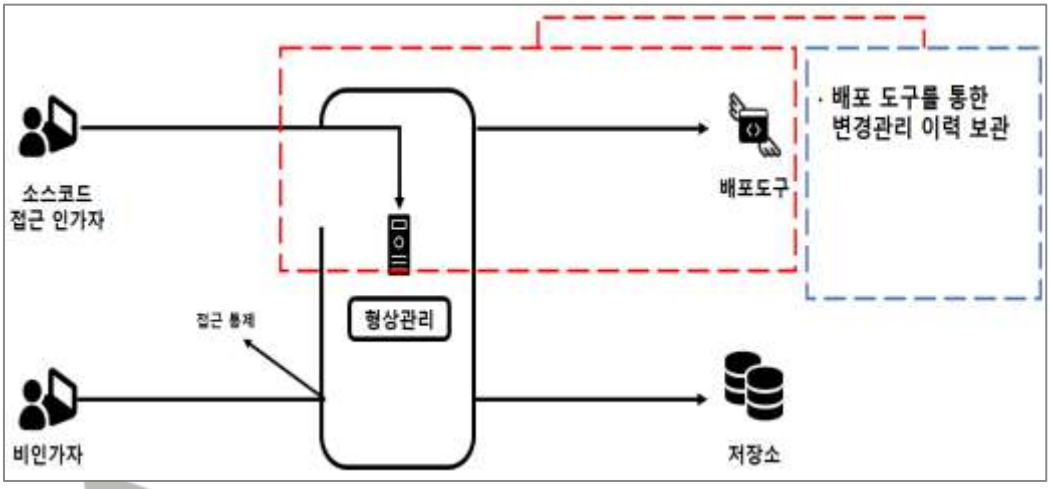
소스코드 배포 및 변경 이력 관리

① 소스 프로그램 변경 절차 수립: 승인 및 작업 절차, 버전 관리 방안 등

② 소스 프로그램 변경 이력 관리: 변경·구현·이관 일자, 변경 요청사유, 담당자 등

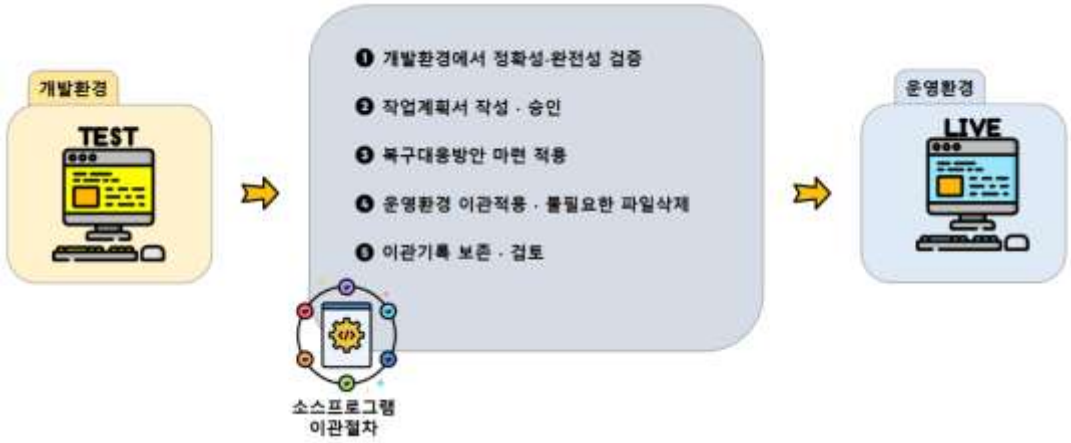
③ 소스 프로그램 변경에 따른 시스템 관련 문서(설계서 등)에 대한 변경 통제 수행

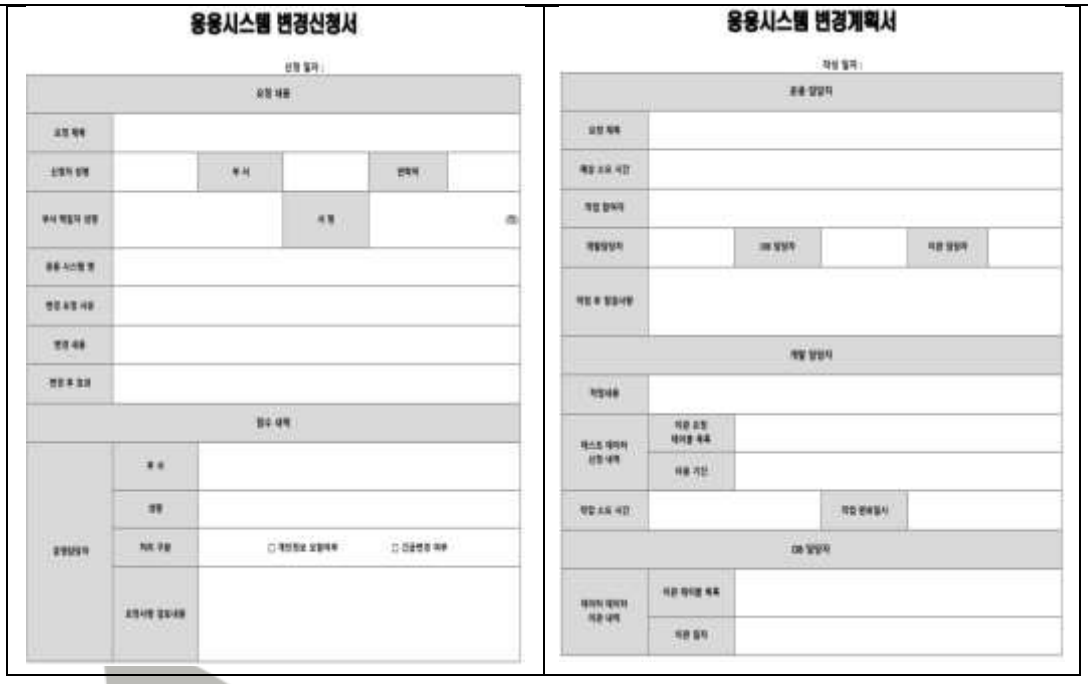
④ 소스 프로그램 변경 이력 및 변경 통제 수행 내역에 대한 정기적인 검토 수행



※ 소스 프로그램 변경관리 이력 보관 (이해를 돕기 위한 예시)

2.8.6 운영 환경 이관

세부분야	2.8.6 운영 환경 이관
인증 기준	신규 도입·개발 또는 변경된 시스템을 운영 환경으로 이관할 때는 통제된 절차를 따라야 하고, 실행 코드는 시험 및 사용자 인수 절차에 따라 실행되어야 한다.
주요 확인사항	• 신규 도입·개발 및 변경된 시스템을 운영 환경으로 안전하게 이관하기 위한 통제 절차를 수립·이행하고 있는가? • 운영 환경으로 이관 시 발생할 수 있는 문제에 대한 대응 방안을 마련하고 있는가? • 운영 환경에는 서비스 실행에 필요한 파일만을 설치하고 있는가?
기준 요약도	
운영 방안	**◇ 신규 도입·개발 및 변경된 시스템을 운영 환경으로 안전하게 이관하기 위한 통제 절차를 수립·이행하고 있는가?** **운영 환경 이전 계획 수립** 「**개발보안 관리지침**」 제 ○○조 (응용시스템 변경관리) ① 응용시스템의 변경 사항이 발생한 경우 '응용시스템 변경 요청서'를 작성하여 담당 정보시스템 책임자에게 변경 요청을 해야 한다. ② 담당 정보시스템 책임자는 변경 요청서의 타당성을 검토한 후 '응용시스템 변경 계획서'를 작성하여 반영한다. 단, 긴급한 상황 하에서 승인 절차를 생략하고 응용시스템을 변경한 경우 사후 승인을 득해야 한다.



※ 응용프로그램 변경신청서 및 변경계획서 (이해를 돕기 위한 예시)

◇ 운영 환경으로 이관 시 발생할 수 있는 문제에 대한 대응 방안을 마련하고 있는가?

운영 환경 이관 문제 발생 시 대응 절차 수립

① 운영 환경으로 정보시스템 이관이 원활하게 이루어지지 않았을 경우 Rollback 방안

② 이전 버전의 시스템 보관 방안(소프트웨어, 종속프로그램, 구성파일, 파라미터 등)

◇ 운영 환경에는 서비스 실행에 필요한 파일만을 설치하고 있는가?

불필요한 테스트 소스 파일 삭제

① 운영 환경에는 승인되지 않은 개발도구(편집기 등), 소스 프로그램 및 백업본, 업무 문서 등 서비스 실행에 불필요한 파일이 존재하지 않도록 관리

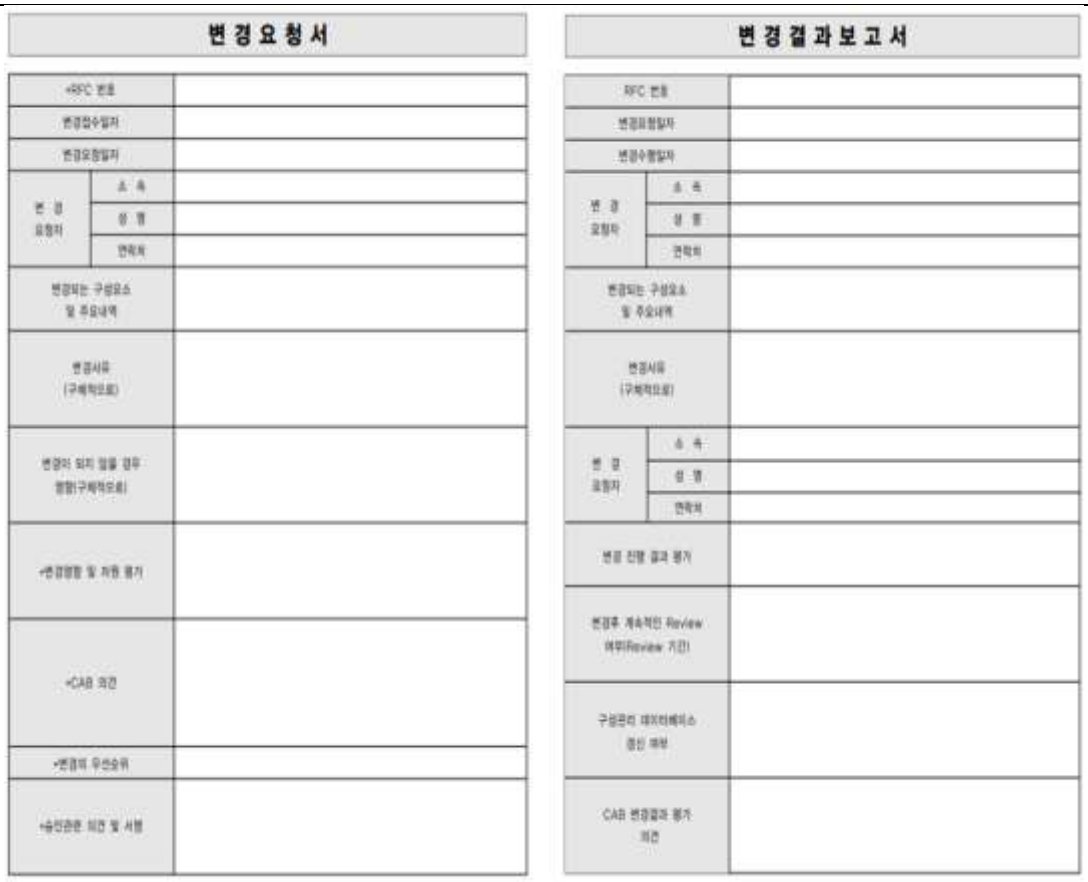
2.9 시스템 및 서비스 운영관리

2.9.1 변경관리

<table>
<tr><th>세부분야</th><th>2.9.1 변경관리</th></tr>
<tr><td>인증
기준</td><td>정보시스템 관련 자산의 모든 변경 내역을 관리할 수 있도록 절차를 수립·이행하고, 변경 전 시스템의 성능 및 보안에 미치는 영향을 분석하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 정보시스템 관련 자산(하드웨어, 운영체제, 상용 소프트웨어 패키지 등) 변경에 관한 절차를 수립·이행하고 있는가?
• 정보시스템 관련 자산 변경을 수행하기 전 성능 및 보안에 미치는 영향을 분석하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 정보시스템 관련 자산(하드웨어, 운영체제, 상용 소프트웨어 패키지 등) 변경에 관한 절차를 수립·이행하고 있는가?

(예시) 변경관리 절차 수립

「접근통제 관리지침」 제 ○○조 (변경관리 대상)
① 정보시스템 책임자는 다음 각 호의 변경 작업 수행 시 '변경 요청서'를 작성하고 정보보호 최고책임자의 승인을 득한 후 변경 작업을 실시한다.
1. 정보시스템 구성 추가·증설·변경·교체·재개
2. 시스템 설정 변경·환경 설정 변경 추가
3. 데이터 및 파일 백업·복구·전환·변경 작업
4. 정보시스템 장애·성능 향상 등 기타 작업
② 변경 작업 완료 후 5일 이내로 '변경 결과보고서'를 작성하여 정보보호 최고책임자의 승인을 득한 후 기록 관리한다.</td></tr>
</table>



변 경 요 청 서

•RFC 번호		
변경접수일자		
변경요청일자		
변 경 요청자	소 속	
	성 명	
	연락처	
변경되는 구성요소 및 주요내역		
변경사유 (구체적으로)		
변경이 되지 않을 경우 영향(구체적으로)		
•변경영향 및 자원 평가		
•CAB 의견		
•변경의 우선순위		
•승인관련 의견 및 서명		

변 경 결 과 보 고 서

RFC 번호		
변경요청일자		
변경수행일자		
변 경 요청자	소 속	
	성 명	
	연락처	
변경되는 구성요소 및 주요내역		
변경사유 (구체적으로)		
변 경 요청자	소 속	
	성 명	
	연락처	
변경 진행 결과 평가		
변경후 계속적인 Review 여부(Review 기간)		
구성관리 데이터베이스 갱신 여부		
CAB 변경결과 평가 의견		

※ 출처 : 변경요청서 및 변경결과보고서(NIA)

◇ 정보시스템 관련 자산 변경을 수행하기 전 성능 및 보안에 미치는 영향을 분석하고 있는가?

변경관리 영향도 분석

① 정보시스템 관련 정보자산 변경이 필요한 경우 변경에 따른 보안, 성능, 업무 등에 미치는 영향을 분석 (방화벽 등 보안시스템 정책 변경 필요성, 정책 변경 시 문제점 및 영향도 등)

② 변경에 따른 영향을 최소화할 수 있도록 변경관리 이행

③ 변경 실패에 따른 복구 방안 사전에 고려

변경관리 점검 체크리스트

점검일시		점검자	
점검대상 업무기관		업무기관 관리책임자명	

Y : Yes / N : No / P : Partially Yes / NA : Not Applicable

점 검 항 목	Y/N/P/NA	부적합 건수
1. 변경 사항에 대한 이해 당사자들이 전부 참석한 CAB 회의를 통해 변경이 승인이 되었는가 ?		
2. 변경 사항에 대해 충분한 시험을 실시하였는가?		
3. 변경 사항에 대해 구성정보 데이터베이스는 갱신이 되었는가?		
4. 변경관리 절차를 따르지 않고 변경이 수행된 경우는 없는가?		
5. 변경 업무에 대한 효율이 변경 관리자의 통제를 통해 적절히 진행되고 있는가?		
6. 긴급변경 시행에 대해서 사전에 정의되고 계속 추가 되고 있는가?		
7. 문제관리 및 구성관리 프로세스와 원활하게 연계 되고 있는가?		
8. 변경 절차서를 데이터에 입무에 혼란이 발생되지 않도록 필요한 사항이 사전에 준비가 되었는가?		

구성관리 점검 체크리스트

점검일시		점검자	
점검대상 업무기관		업무기관 관리책임자명	

Y : Yes / N : No / P : Partially Yes / NA : Not Applicable

점 검 항 목	Y/N/P/NA	부적합 건수
1. 구성요소중 부적합하게 등록되거나 미등록된 구성요소은 없는가 ?		
2. 구성관리 데이터베이스의 실제 구성요소의 상태가 갱신되지 않거나 불필요한 구성요소는 없는가?		
3. 변경관리 절차를 따르지 않고 구성변경이 수행된 경우는 없는가?		
4. 구성베이스라인의 최초 업무시점과 대규모 변경 등 구성된 시점에서 설정되었는가?		
5. 구성요소의 변경에 따라, 관련된 상위 및 하위 구성요소가 적절하게 갱신되었는가?		
6. 구성요소에 대한 변경, 장애, 문제이력이 적절하게 기록되었는가?		
7. 구성관리 데이터베이스와 DSL의 백업 계획에 따라 백업이 수행되고 있는가?		
8. 구성관리 데이터베이스, DSL, DHL에 대한 접근권한 할당 및 통제가 부적절한 사례는 없는가?		

※ 출처: 구성 및 변경관리 지침 (NIA)

2.9.2 성능 및 장애관리

세부분야	2.9.2 성능 및 장애관리
인증 기준	정보시스템의 가용성 보장을 위하여 성능 및 용량 요구사항을 정의하고 현황을 지속적으로 모니터링하여야 하며, 장애 발생 시 효과적으로 대응하기 위한 탐지·기록·분석·복구·보고 등의 절차를 수립·관리하여야 한다.
주요 확인사항	• 정보시스템의 가용성 보장을 위하여 성능 및 용량을 지속적으로 모니터링할 수 있는 절차를 수립·이행하고 있는가? • 정보시스템 성능 및 용량 요구사항(임계치)을 초과하는 경우에 대한 대응 절차를 수립·이행하고 있는가? • 정보시스템 장애를 즉시 인지하고 대응하기 위한 절차를 수립·이행하고 있는가? • 장애 발생 시 절차에 따라 조치하고 장애 조치 보고서 등을 통하여 장애 조치 내역을 기록하여 관리하고 있는가? • 심각도가 높은 장애의 경우 원인 분석을 통한 재발방지 대책을 마련하고 있는가?
기준 요약도	
운영 방안	**◇ 정보시스템의 가용성 보장을 위하여 성능 및 용량을 지속적으로 모니터링할 수 있는 절차를 수립·이행하고 있는가?** **(예시) 정보시스템 가용성 보장 모니터링 절차 수립** 「**접근통제 관리지침**」 제 ○○조 (시스템 성능관리 및 유지보수) ① 성능관리 대상은 1등급 정보시스템으로 정한다. ② 정보시스템 책임자는 각 호의 임계값에 따라 월 1회 이상 모니터링 활동을 수행하고 '정보시스템 성능점검 관리대장'에 기록 관리해야 한다. 1. CPU 사용률 임계치: 80% ~ 85% 이상일 경우 지속적인 모니터링 2. 메모리 사용률 임계치: 80% ~ 85% 이상일 경우 지속적인 모니터링 3. 디스크 사용률 임계치: 70% ~ 75% 이상일 경우 지속적인 모니터링

③ 부서 정보보호 책임자는 성능점검 결과를 반기 1회 이상 정보보호 최고책임자에게 보고해야 한다.

정보시스템 성능점검 관리대장

정보시스템 성능점검 관리대장 (반기)

※ 성능점검 관리대장 (이해를 돕기 위한 예시)

◇ 정보시스템 성능 및 용량 요구사항(임계치)을 초과하는 경우에 대한 대응 절차를 수립·이행하고 있는가?

지속적인 임계값 초과 위험 발생 모니터링 및 변경 계획 수립

① 정보시스템의 성능 및 용량 현황을 지속적으로 모니터링하여 요구사항(임계치)을 초과하는 경우 조치 방안(예: 정보시스템, 메모리, 저장장치 증설 등)을 수립·이행

성능분석/조정 요청서

성능개선 결과보고서

※ 출처: 성능관리지침 (NIA)

◇ 정보시스템 장애를 즉시 인지하고 대응하기 위한 절차를 수립·이행하고 있는가?

정보시스템 장애 대응 절차 수립

① 장애 유형 및 심각도 정의

② 장애 유형 및 심각도별 보고 절차

③ 장애 유형별 탐지 방법 수립

④ 장애 대응 및 복구에 관한 책임과 역할 정의

⑤ 장애 기록 및 분석

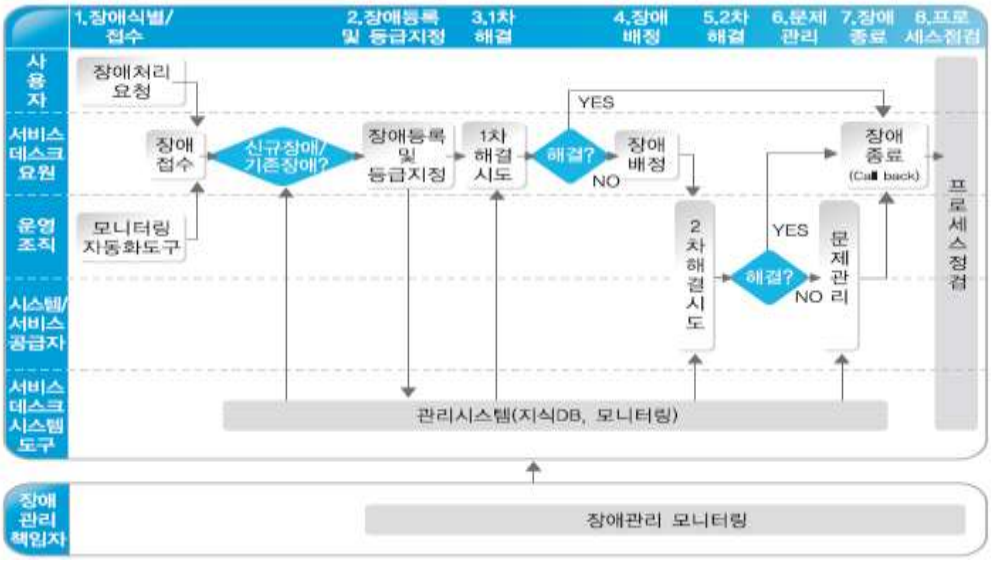
⑥ 대고객 서비스인 경우 고객 안내 절차

⑦ 비상연락체계(유지보수업체, 정보시스템 제조사) 등

장애 유형 및 심각도(예시)

장애 등급	영향도	긴급도	보고체계
Level 1	· 즉각적인 조치가 필요한 긴급 상황으로, 인명 피해, 대규모 재산 손실, 법적 문제 등이 발생할 수 있는 경우	- 즉각적 해결	- 10분 이내 즉시보고
Level 2	· 빠른 조치가 필요한 상황으로, 중요한 비즈니스 프로세스나 서비스 중단 등으로 인한 큰 손실이 예상되는 경우	- 가능한 신속해결	- 30분 이내 보고
Level 3	· 적극적인 대응이 필요한 상황으로, 일부 비즈니스 프로세스나 서비스 중단 등으로 인한 손실이 예상되는 경우	- 대응시간을 가지며 해결	- 60분 이내 보고
Level 4	· 일반적인 대응이 가능한 상황으로, 손실이 예상되지 않지만 빠른 조치가 필요한 경우	- 장애처리조직 별도 해결	- 장애처리조직에서 관리
Level 5	· 보통의 업무 운영에서 발생하는 문제로, 대부분의 경우	- 보고없이 해결	- 보고 없이 해결

※ 장애 유형 및 심각도 (이해를 돕기 위한 예시)



※ 출처: 정보시스템 장애관리 지침 (NIA)

◇ 장애 발생 시 절차에 따라 조치하고 장애 조치 보고서 등을 통하여 장애 조치 내역을 기록하여 관리하고 있는가?

정보시스템 장애 조치 기록 관리

① 장애 일시

② 장애 심각도

③ 담당자, 책임자명

④ 장애 내용

⑤ 장애 원인, 조치 내용, 복구 내용, 재발방지 대책 등

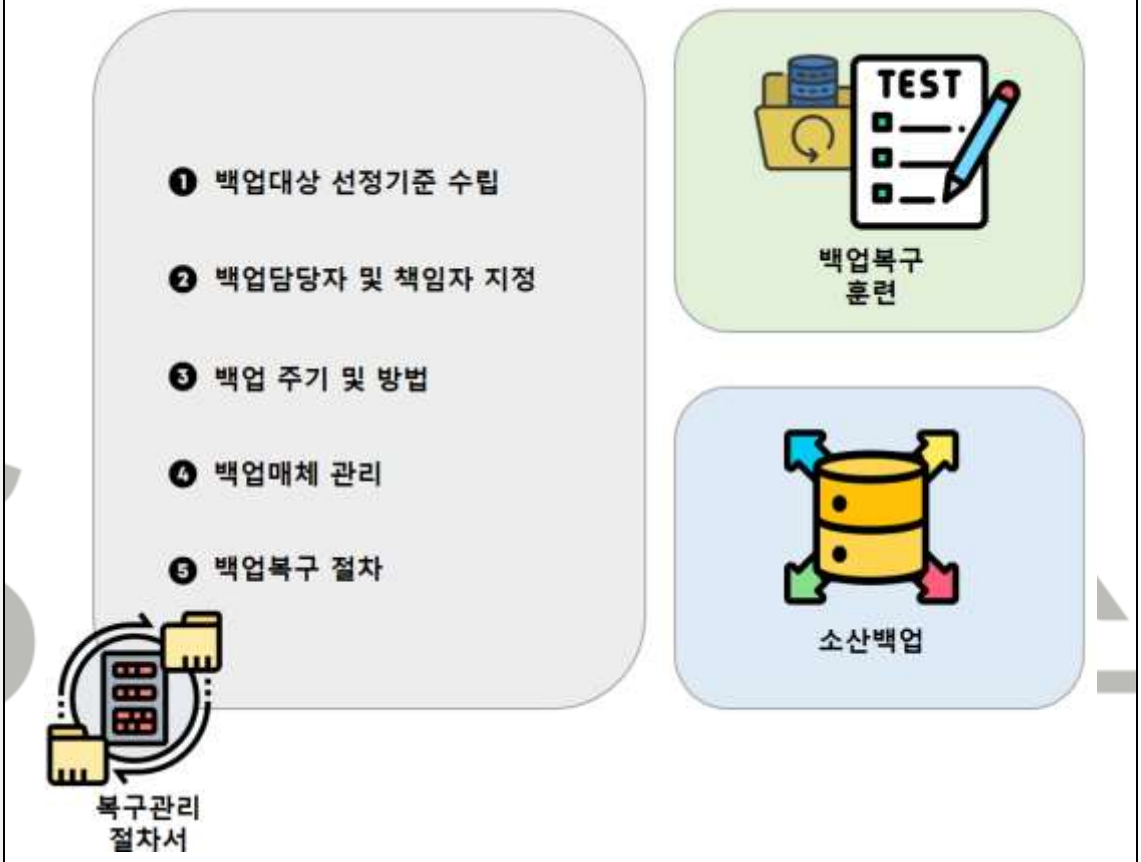
※ 출처: 정보시스템 장애관리 지침 (NIA)

◇ 심각도가 높은 장애의 경우 원인 분석을 통한 재발방지 대책을 마련하고 있는가?

원인 분석을 통하여 재발방지 대책 마련

① 일상 업무가 중단되는 장애, 과다한 비용(피해)을 초래한 장애, 반복적으로 발생하는 장애 등과 같은 심각한 장애의 경우 원인을 규명하고 재발을 방지하기 위한 대책을 수립·이행하여야 함.

2.9.3 백업 및 복구관리

세부분야	2.9.3 백업 및 복구관리
인증 기준	정보시스템의 가용성과 데이터 무결성을 유지하기 위하여 백업 대상, 주기, 방법, 보관 장소, 보관 기간, 소산 등의 절차를 수립·이행하여야 한다. 아울러 사고 발생 시 적시에 복구할 수 있도록 관리하여야 한다.
주요 확인사항	• 백업 대상, 주기, 방법, 절차 등이 포함된 백업 및 복구 절차를 수립·이행하고 있는가? • 백업된 정보의 완전성과 정확성, 복구 절차의 적절성을 확인하기 위하여 정기적으로 복구 테스트를 실시하고 있는가? • 중요정보가 저장된 백업매체의 경우 재해·재난에 대처할 수 있도록 백업매체를 물리적으로 떨어진 장소에 소산하고 있는가?
기준 요약도	
운영 방안	**◇ 백업 대상, 주기, 방법, 절차 등이 포함된 백업 및 복구 절차를 수립·이행하고 있는가?** **(예시) 백업 및 복구 절차를 수립·이행** 「**업무연속성 관리지침**」 제 ○○조 (백업 복구 계획) ① 백업 대상은 데이터 파손 시 복구 필요성이 있는 주요 데이터로, 각 호와 같은 정보들을 백업한다.

1. 각종 서버에 저장된 운영체제, 시스템프로그램, 업무개발 소스 및 DATA 등

② 백업 담당자 및 책임자 지정

③ 백업 대상 별 백업 주기 및 보존기한 정의

정보시스템 백업 스케줄 관리

서버명	백업대상	시스템 중요도	백업주기	백업 보관기간	백업방식
AAA 시스템	- 저장된 운영체제, 시스템프로그램, 업무개발 소스 및 DATA	1등급	1 일	1 주일	자동백업 시스템
BBB 시스템	- 저장된 운영체제, 시스템프로그램, 업무개발 소스 및 DATA	2등급	3 일	1 주일	자동백업 시스템
CCC 시스템	- 저장된 운영체제, 시스템프로그램, 업무개발 소스 및 DATA	3등급	1 주일	1 개월	자동백업 시스템
...	...	...	...	...	...

※ 정보시스템 백업 스케줄 관리 (이해를 돕기 위한 예시)

④ 백업 방법 및 절차

⑤ 백업매체 관리

⑥ 백업 복구 절차

1. 정보시스템 재해 및 장애 발생 시 데이터가 손실 또는 훼손된 경우 최신 데이터로 빠르게 복구해야 한다.

2. 사용자 부주의 또는 업무 착오 등으로 인한 데이터 훼손 시 '자료 복구 신청서'를 작성하여 백업 운영자에게 신청하고 백업 운영자는 이를 근거로 자료를 복구한다.

백 업 신 청 서

신청부서	
담 당	검 토

1. 일반 사항

신청일자					
신청자 성명		전화		부서명	

2.백업정보

구 분	내 용		
서버명 (IP주소 명기)			
백업 주기 (해당항목 'Y')	OS ( ) 데이터베이스 ( ) 사용자 일반파일 ( ) 기타 ( )		
백업 주기 (해당항목 'Y')	일간 ( ) 주간 ( ) 월간 ( ) 연간 ( ) 수시 ( )		
백업본 보관기간			
백업 대상 위치			
백업 전체 용량			
백업 희망시간	시작시간		완료시간
특기사항			

*신청서 접수정보

접수일시		접수자 성명	
백업 적용일자			
백업 장치		백업 소프트웨어	
특기사항			

※ 검토란은 승인자의 성명을 기입하여 결재가 가능함.

복 구 신 청 서

신청부서	
담 당	검 토

1. 일반 사항

신청일자					
신청자 성명		전화		부서명	

2.복구 정보

구 분	내 용
서 버 명	
복구 목적	
복구 대상명	
전체 파일크기	
대상파일 백업일자	
*복구 불가시 대체백업일자	
복구 위치	
복구 완료 희망시간	
특기사항	

*백업완료정보

접수 일시			
작업자 성명		작업소요시간	
복구 결과			

※ 검토란은 승인자의 성명을 기입하여 결재가 가능함.

※ 출처: 정보시스템 백업지침 (NIA)

◇ 백업된 정보의 완전성과 정확성, 복구 절차의 적절성을 확인하기 위하여 정기적으로 복구 테스트를 실시하고 있는가?

복구 테스트 훈련

① 복구 테스트 계획(복구 테스트 주기 및 시점, 담당자, 방법 등)

② 복구 테스트 시나리오 수립

③ 복구 테스트 실시 및 결과 보고

④ 복구 테스트 결과 문제점 발견 시 개선 계획 수립 및 이행

◇ 중요정보가 저장된 백업매체의 경우 재해·재난에 대처할 수 있도록 백업매체를 물리적으로 떨어진 장소에 소산하고 있는가?

(예시) 주기적 소산백업 지침 수립

「**업무연속성 관리지침**」 제 ○○조 (백업 관리)

① 백업은 정보통신실의 완전 소실인 경우에도 복구 가능한 수준으로 이루어져야 하며,

소산은 6개월마다 실시할 수 있다.

소산 백업 관리대장

소산 대상	소산 장소	소산 수행일	보존 기간	담당자	확인자

※ 소산 백업 관리대장 (이해를 돕기 위한 예시)

2.9.4 로그 및 접속기록 관리

세부분야	2.9.4 로그 및 접속기록 관리
인증 기준	서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 사용자 접속기록, 시스템로그, 권한 부여 내역 등의 로그 유형, 보존 기간, 보존 방법 등을 정하고 위·변조, 도난, 분실되지 않도록 안전하게 보존·관리하여야 한다.
주요 확인사항	• 서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 로그 관리 절차를 수립하고 이에 따라 필요한 로그를 생성하여 보관하고 있는가? • 정보시스템의 로그 기록은 위·변조 및 도난, 분실되지 않도록 안전하게 보관하고 로그 기록에 대한 접근권한은 최소화하여 부여하고 있는가? • 개인정보처리시스템에 대한 접속기록은 법적 요구사항을 준수할 수 있도록 필요한 항목을 모두 포함하여 일정기간 안전하게 보관하고 있는가?
기준 요약도	
운영 방안	**◇ 서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 로그 관리 절차를 수립하고 이에 따라 필요한 로그를 생성하여 보관하고 있는가?** **(예시) 로그 기록 관리 절차 수립** 「**정보시스템 운영보안 지침**」 제 ○○조 (로그 기록 관리) ① 정보시스템 관리자는 보존이 필요한 로그 유형 및 대상 시스템을 식별하고, 정보시스템의 로그를 각 호의 항목을 포함하여 저장 및 관리해야 한다. 1. 이벤트 로그: 시스템 시작, 종료, 상태, 에러코드 등 2. 네트워크 이벤트로그: IP 할당, 주요 구간 트래픽 로그 등 3. 보안 시스템: 관리자 접속, 보안 정책(룰셋) 변경 내역 등 4. 정보시스템 감사 로그: 사용자 접속기록, 인증 성공·실패, 파일 접근, 계정

발급·변경·해지 내역, 접근권한 부여·변경·말소 내역 등

5. 개인정보처리시스템 접속 로그: 접속 계정, 접속일시(시·분·초), 접속지IP, 수행 업무

linux 서버	
wtmp	사용자 로그인 정보
syslog	OS 및 응용프로그램의 주요 동작 내역
secure	OS 및 응용프로그램의 주요 동작 내역(Linux)
sulog	su 명령에 의한 결과를 기록
authlog	시스템 내 인증관련 이벤트 기록(Solaris)
messages	각종 메시지들을 기록
btmp	5회 이상의 로그인 실패에 대한 기록(Linux, HP-UX)
loginlog	n회 이상의 로그인 실패에 대한 기록(Solaris)

Window 서버	
응용 프로그램로그	응용 프로그램에 의해 발생된 이벤트 기록, 파일에러 기록
보안로그	보안 감사 레코드
	보안 로그는 감사정책을 설정하여야 기록됨
	보안로그는 관리자만 볼 수 있음
시스템 오류 로그	시스템 구성요소가 발생시킨 이벤트를 기록함
	드라이버나 다른 시스템 구성 요소를 읽어 들이지 못했을 경우 기록함

※ 시스템 로그 보관 (이해를 돕기 위한 예시)

◇ 정보시스템의 로그 기록은 위·변조 및 도난, 분실되지 않도록 안전하게 보관하고 로그 기록에 대한 접근권한은 최소화하여 부여하고 있는가?

로그 접근권한 최소화

① 로그 기록은 스토리지 등 별도 저장 장치를 사용하여 백업하고, 로그 기록에 대한 접근권한 부여는 최소화하여 비인가자에 의한 로그 기록 위·변조 및 삭제 등이 발생하지 않도록 하여야 함.

◇ 개인정보처리시스템에 대한 접속기록은 법적 요구사항을 준수할 수 있도록 필요한 항목을 모두 포함하여 일정기간 안전하게 보관하고 있는가?

개인정보처리시스템의 접속 및 작업기록 법적 요구사항에 맞게 기록

① 개인정보처리시스템 접속기록에 반드시 포함되어야 할 항목

접속기록 작성 예시

1) 계정 : 개인정보처리시스템에 접속한 자(개인정보취급자 등)의 계정정보

2) 접속일시 : 접속한 시점 또는 업무를 수행한 시점(년-월-일, 시:분:초)

3) 접속지 정보: 개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버 IP

4) 처리한 정보주체 정보 : 누구의 개인정보를 처리하였는지 알 수 있는 정보

※ 과도한 개인정보가 저장되지 않도록 개인의 식별정보(ID, 학번, 사번 등)를 활용하여 기록

※ 대량의 개인정보를 처리하는 경우 검색조건문(쿼리)으로 대체 가능

5) 수행업무 : 개인정보취급자가 개인정보처리시스템을 이용하여 개인정보를 처리한 내용

※ 검색, 열람, 조회, 입력, 수정, 삭제, 출력, 다운로드 등

접속기록 항목 작성 예시

개인정보 취급자 계정	접속일시	접속지 정보	처리한 정보주체의 정보	수행업무
A0001	2020-02-25, 17:00:00.	192.168.100.1	kdhong	개인정보 수정

※ 위 항목은 반드시 기록하여야 하며, 처리하는 업무환경에 따라 책임추적성 확보에 필요한 항목은 추가로 기록하여야 함

※ 출처: 개발자 대상 개인정보 보호조치 적용 가이드 (개인정보보호위원회·KISA)

2.9.5 로그 및 접속기록 점검

세부분야	2.9.5 로그 및 접속기록 점검
주요 확인사항	정보시스템의 정상적인 사용을 보장하고 사용자 오·남용(비인가접속, 과다조회 등)을 방지하기 위하여 접근 및 사용에 대한 로그 검토 기준을 수립하여 주기적으로 점검하며, 문제 발생 시 사후 조치를 적시에 수행하여야 한다.
기준 요약도	• 정보시스템 관련 오류, 오·남용(비인가접속, 과다조회 등), 부정행위 등 이상징후를 인지할 수 있도록 로그 검토 주기, 대상, 방법 등을 포함한 로그 검토 및 모니터링 절차를 수립·이행하고 있는가? • 로그 검토 및 모니터링 결과를 책임자에게 보고하고 이상징후 발견 시 절차에 따라 대응하고 있는가? • 개인정보처리시스템의 접속기록은 관련 법령에서 정한 주기에 따라 정기적으로 점검하고 있는가?
운영 방안	
점검 방법	**◇ 정보시스템 관련 오류, 오·남용(비인가접속, 과다조회 등), 부정행위 등 이상징후를 인지할 수 있도록 로그 검토 주기, 대상, 방법 등을 포함한 로그 검토 및 모니터링 절차를 수립·이행하고 있는가?** **로그 검토 절차** ① 검토 주기 ② 검토 대상 ③ 검토 기준 및 방법 ④ 검토 담당자 및 책임자 ⑤ 이상징후 발견 시 대응 절차 등

개인정보처리시스템 접속기록 검토 (예시)

접속 기록 ID	사용자 이름	소속 부서	직급	접속 일시	접속 정보 IP 주소	접속 상태	응용프로그램 시스템명	행위	소명확인
A1B2C3D4	홍길동	인사부	대리	2024-05-26	192.168.1.100	로그인 완료	인사정보시스템	주말 로그인	소명확인 완료
E5F6G7H8	김철수	영업부	과장	2024-05-26	192.168.1.105	로그인 완료	고객관리시스템	업무 외 시간 로그인	소명확인 완료
I9J0K1L2	이영희	IT부	부장	2024-05-27	192.168.1.110	로그인 완료	서버관리시스템	주말 로그인	소명확인 완료
M3N4O5P6	박지민	마케팅부	수석	2024-05-27	192.168.1.115	로그인 완료	마케팅데이터베이스시스템	과다 다운로드	소명확인 완료
Q7R8S9T0	최영호	개발부	임원	2024-05-28	192.168.1.120	로그인 완료	개발프로젝트관리시스템	업무 외 시간 로그인	소명확인 완료

※ 로그 검토 기록 체크리스트 (이해를 돕기 위한 예시)

◇ 로그 검토 및 모니터링 결과를 책임자에게 보고하고 이상징후 발견 시 절차에 따라 대응하고 있는가?

이상징후 검토 결과 대응

① 로그 검토 및 모니터링 기준에 따라 검토를 수행한 후 이상징후 발견 여부 등 그 결과를 관련 책임자에게 보고

② 이상징후 발견 시 정보 유출, 해킹, 오·남용, 부정행위 등 발생 여부를 확인하기 위한 절차를 수립하고 절차에 따라 대응

③ 개인정보를 다운로드한 것이 확인된 경우 내부관리계획 등 로그검토 기준에서 정하는 바에 따라 그 사유를 확인하고, 개인정보의 오·남용이나 유출 목적으로 다운로드한 것이 확인되었다면 지체 없이

④ 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등의 필요한 조치 이행

◇ 개인정보처리시스템의 접속기록은 관련 법령에서 정한 주기에 따라 정기적으로 점검하고 있는가?

개인정보처리시스템 접속기록 주기적 검토

① 법령에 따른 개인정보처리시스템 접속기록 점검 주기:

1. 개인정보의 다운로드가 확인된 경우에는 내부 관리계획 등으로 정하는 바에 따라 그 사유를 반드시 확인하여야 함

※ 개인정보처리시스템 접속기록 점검 주기

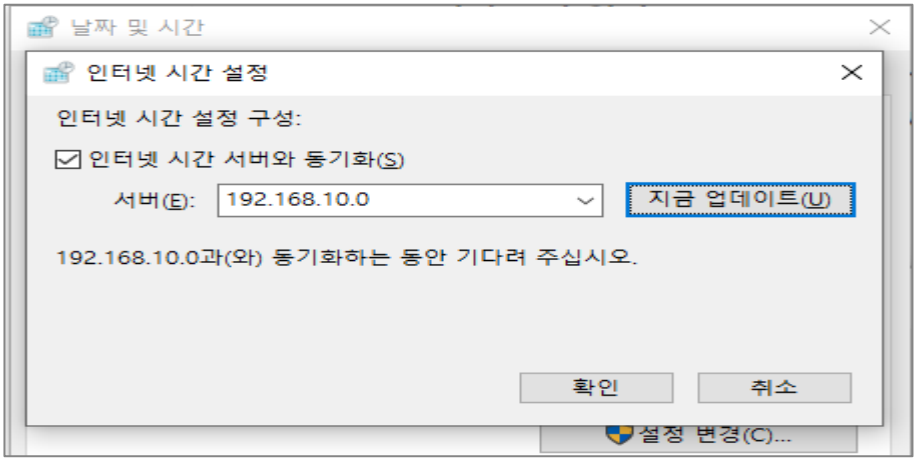
1. 개인정보의 안전성 확보조치 기준 개정(2025.10.31)으로, 기존 월 1회 점검에서 내부관리계획에 따른 점검주기로 개정됨

	□ **제8조(접속기록의 보관 및 점검)** ① 개인정보처리자는 개인정보처리시스템에 접속한 자(다만, 정보주체는 제외한다)의 접속기록을 1년 이상 보관·관리하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 2년 이상 보관·관리하여야 한다. 1. 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우 2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우 3. 개인정보처리자로서 「전기통신사업법」 제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우 ② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보취급자의 개인정보처리시스템에 대한 접속기록 및 개인정보 다운로드 상황을 확인하고 점검하는 주기·방법·사후조치절차 등을 내부 관리계획으로 정하고 이행하여야 한다. ③ 개인정보처리자는 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하기 위한 조치를 하여야 한다. ※ 출처: 개인정보의 안전성 확보조치 기준 (법제처)

2.9.6 시간 동기화

<table>
<tr><th>세부분야</th><th>2.9.6 시간 동기화</th></tr>
<tr><td>인증
기준</td><td>로그 및 접속기록의 정확성을 보장하고 신뢰성 있는 로그 분석을 위하여 관련 정보시스템의 시각을 표준시각으로 동기화하고 주기적으로 관리하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 정보시스템의 시간을 표준시간으로 동기화하고 있는가?
• 시간 동기화가 정상적으로 이루어지고 있는지 주기적으로 점검하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 정보시스템의 시간을 표준시간으로 동기화하고 있는가?

(예시) 정보시스템 시간 동기화 절차 수립

「접근통제 관리지침」 제 ○○조 (시간 동기화)
① 정보시스템 로그의 정확성을 보장하고 신뢰성 있는 로그 분석을 위하여 정보시스템의 시각을 표준화하고 동기화 하여야 한다.
1. NTP(Network Time Protocol) 등을 활용하여 정보시스템 간 시간 동기화
 

※ 윈도우 서버 NTP 설정 (이해를 돕기 위한 예시)</td></tr>
</table>

	◇ 시간 동기화가 정상적으로 이루어지고 있는지 주기적으로 점검하고 있는가? **시간 동기화 주기적 점검** ① 시간 동기화 오류 발생 여부, OS재설치 또는 설정변경 등에 따른 시간동기화 적용 누락 여부 등 점검

2.9.7 정보자산의 재사용 및 폐기

세부분야	2.9.7 정보자산의 재사용 및 폐기
인증 기준	정보자산의 재사용과 폐기 과정에서 개인정보 및 중요정보가 복구·재생되지 않도록 안전한 재사용 및 폐기 절차를 수립·이행하여야 한다.
주요 확인사항	• 정보자산의 안전한 재사용 및 폐기에 대한 절차를 수립·이행하고 있는가? • 정보자산 및 저장매체를 재사용 및 폐기하는 경우 개인정보 및 중요정보를 복구되지 않는 방법으로 처리하고 있는가? • 자체적으로 정보자산 및 저장매체를 폐기할 경우 관리대장을 통하여 폐기 이력을 남기고 폐기 확인 증적을 함께 보관하고 있는가? • 외부업체를 통하여 정보자산 및 저장매체를 폐기할 경우 폐기 절차를 계약서에 명시하고 완전히 폐기하였는지 여부를 확인하고 있는가? • 정보시스템, PC 등 유지보수, 수리 과정에서 저장매체 교체, 복구 등 발생 시 저장매체 내 정보를 보호하기 위한 대책을 마련하고 있는가?
기준 요약도	
운영 방안	◇ 정보자산의 안전한 재사용 및 폐기에 대한 절차를 수립·이행하고 있는가? 재사용 및 폐기 절차 수립 ① 정보자산 재사용 절차: 데이터 초기화 방법, 재사용 프로세스 등 ② 정보자산 폐기 절차: 폐기 방법, 폐기 프로세스, 폐기 확인, 폐기 관리대장 기록 등

◇ 정보자산 및 저장매체를 재사용 및 폐기하는 경우 개인정보 및 중요정보를 복구되지 않는 방법으로 처리하고 있는가?

(예시) 정보자산 재사용 및 폐기 지침 수립

「**접근통제 관리지침**」 제 ○○조 (정보자산 재사용 및 폐기)

① 정보자산 및 저장매체를 폐기하는 경우 개인정보 및 중요정보가 복구 또는 재생되지 않도록 각 호와 같이 안전하게 파기해야 한다.

1. 물리적 파기

- 하드디스크: 소각 또는 파쇄기를 이용한 파기
- 플로피디스크·CD·DVD: 문서 파쇄기를 이용한 파쇄

2. 논리적 파기

- 전체 삭제: Low-Level 포맷 3회
- 일부 삭제: 임의 데이터 3회 덮어쓰기
- DB 데이터 삭제: Delete 쿼리 이용 삭제

◇ 자체적으로 정보자산 및 저장매체를 폐기할 경우 관리대장을 통하여 폐기 이력을 남기고 폐기확인 증적을 함께 보관하고 있는가?

(예시) 정보자산 폐기 이력 관리

「**접근통제 관리지침**」 제 ○○조 (정보시스템 등록 및 폐기)

① 정보시스템 자산 폐기 시 정보시스템 책임자자는 자산등록/폐기 신청서를 작성하여 정보보호 최고책임자의 승인을 득한 후 파기한다.

② 정보시스템 철수 또는 폐기 시 시스템 내 정보를 완전 삭제하고, 정보자산 관리대장 갱신 및 정보자산 폐기 관리대장에 기록 관리해야 한다.

정보자산 폐기관리대장

정보시스템책임자	정보보호담당자	정보보호책임자

일자	자산명	자산코드	수량	관리번호	관리부서	폐기담당자	확인 담당자
						(인)	(인)
						(인)	(인)
---	---	---	---	---	---	---	---

※ 폐기관리대장 (이해를 돕기 위한 예시)

	◇ 외부업체를 통하여 정보자산 및 저장매체를 폐기할 경우 폐기 절차를 계약서에 명시하고 완전히 폐기하였는지 여부를 확인하고 있는가? **완전한 폐기 여부 확인** ① 폐기 절차 및 보호 대책, 책임소재 등에 대하여 계약서에 반영 ② 계약서에 반영된 폐기 절차에 따라 이행되고 있는지 사진촬영, 실사 등의 이행 증적 확인 **◇ 정보시스템, PC 등 유지보수, 수리 과정에서 저장매체 교체, 복구 등 발생 시 저장매체 내 정보를 보호하기 위한 대책을 마련하고 있는가?** **수리·교체 시 정보보호 대책** ① 유지보수 신청 전 데이터 이관 및 파기 ② 데이터 암호화 ③ 계약 시 비밀유지 서약 ④ 데이터 완전삭제 또는 저장매체 완전파기 조치 등

2.10 시스템 및 서비스 운영관리

2.10.1 보안시스템 운영

세부분야	2.10.1 보안시스템 운영
인증 기준	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영 절차를 수립·이행하고 보안시스템별 정책 적용 현황을 관리하여야 한다
주요 확인사항	• 조직에서 운영하고 있는 보안시스템에 대한 운영 절차를 수립·이행하고 있는가? • 보안시스템 관리자 등 접근이 허용된 인원을 최소화하고 비인가자의 접근을 엄격하게 통제하고 있는가? • 보안시스템별로 정책의 신규 등록, 변경, 삭제 등을 위한 공식적인 절차를 수립·이행하고 있는가? • 보안시스템의 예외 정책 등록에 대하여 절차에 따라 관리하고 있으며, 예외 정책 사용자에 대하여 최소한의 권한으로 관리하고 있는가? • 보안시스템에 설정된 정책의 타당성 여부를 주기적으로 검토하고 있는가? • 개인정보처리시스템에 대한 불법적인 접근 및 개인정보 유출 방지를 위하여 관련 법령에서 정한 기능을 수행하는 보안시스템을 설치하여 운영하고 있는가?
기준 요약도	

운영 방안

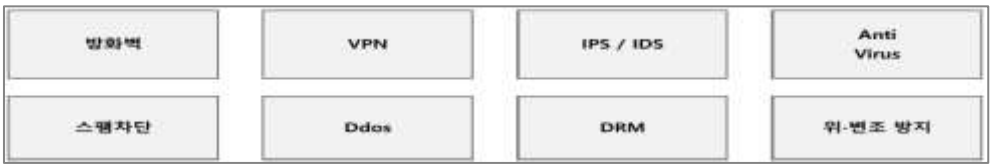
◇ 조직에서 운영하고 있는 보안시스템에 대한 운영 절차를 수립 · 이행하고 있는가?

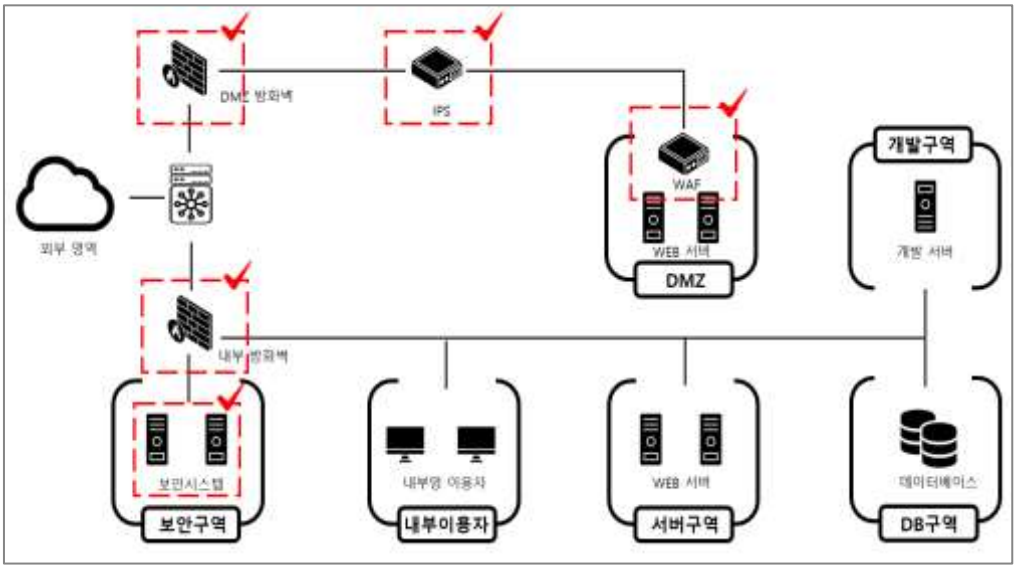
정보보안시스템 운영 절차 수립

보안시스템 운영관리 매뉴얼

순번	내용
1	보안시스템 유형별 책임자 및 관리자 지정
2	보안시스템 정책 적용 절차
3	최신 정책 업데이트 (최신패턴 및 엔진 업데이트)
4	접근통제 (사용자 인증, 단말 인증)
5	보안시스템 현황 점검

구분	직위	성명	일자	서명
승인	정보보호 최고책임자	OOO	2023-01-01	승인
상신	정보보호 담당자	OOO	2022-12-20	-





※ 정보보호 시스템 운영관리 (이해를 돕기 위한 예시)

◇ 보안시스템 관리자 등 접근이 허용된 인원을 최소화하고 비인가자의 접근을 엄격하게 통제하고 있는가?

보안시스템 접근통제

① 강화된 사용자 인증(OTP 등), 관리자 단말 IP 또는 MAC 접근통제 등의 보호 대책을 적용하여 보안시스템 관리자 등 접근이 허용된 인원 이외의 비인가자 접근을 엄격히 통제

② 주기적인 보안시스템 접속로그 분석을 통하여 비인가자에 의한 접근 시도 여부 확인

◇ 보안시스템별로 정책의 신규 등록, 변경, 삭제 등을 위한 공식적인 절차를 수립·이행하고 있는가?

(예시) 보안시스템별 정책 변경 절차 수립

「**접근통제 관리지침**」 제 ○○조 (정보보호 시스템관리)

① 보안시스템운영자는 정책 변경 시 "방화벽 오픈 신청서"를 작성하여 정보보호담당자에게 승인을 득한 후 정책을 적용해야 한다.

② 보안시스템 운영자 사용 목적 달성이나 기간 만료 등의 불필요한 정책은 즉시 삭제 또는 중지하여야 한다.

③ 보안시스템운영자는 침입차단 정책 현황을 '방화벽 정책관리대장'에 기록해야 하며, 분기별 1회 접근통제 정책을 검토 후 부서 정보보호담당자의 승인을 득해야 한다.

방화벽 오픈 신청서

보안시스템 운영자	정보보호 담당자

부서		성명	
직급		신청일자	
신청 구분	□신규 □변경 □삭제	신청사유	
대상 시스템			

번호	출발지 IP	목적지 IP	서비스 (프로토콜, 포트)	이용기간	내 용
1					
2					
3					
4					

본인은 업무 수행을 위해 다음과 같은 보안정책을 신청하오니 허락하여 주시기 바랍니다

서 명 : (인

방화벽 정책관리대장 (예시)

구분	출발지IP	목적지IP	프로토콜	포트	신청기간	만료기간	신청내용	적용일시	작업자	보안시스템 운영자	정보보호 담당자
신규	192.168.1.100	203.0.113.5	TCP	80	2024-05-28 ~	2024-06-28	사무실 웹 서버 접근 허용	2024-05-27	홍길동	(인)	(인)
변경	192.168.2.50	104.244.42.1	UDP	53	2024-05-30 ~	2024-06-30	DNS 서버 변경	2024-05-31	홍길동	(인)	(인)
신규	10.0.0.5	172.16.0.10	TCP	22	2024-06-01 ~	2024-07-01	SSH 접속 허용	2024-06-02	홍길동	(인)	(인)
변경	192.168.3.20	198.51.100.1	TCP	443	2024-06-05 ~	2024-07-05	SSL VPN 서버 변경	2024-06-06	홍길동	(인)	(인)

※ 방화벽 서비스 신청서 (이해를 돕기 위한 예시)

◇ 보안시스템의 예외 정책 등록에 대하여 절차에 따라 관리하고 있으며, 예외 정책 사용자에 대하여 최소한의 권한으로 관리하고 있는가?

보안시스템 예외 정책 절차 수립

① 신청사유의 타당성 검토

② 보안성 검토: 예외 정책에 따른 보안성 검토 및 보완대책 마련

③ 예외 정책 신청·승인: 보안시스템별로 책임자 또는 담당자 승인

④ 예외 정책 만료 여부 및 예외 사용에 대한 모니터링 등

◇ 보안시스템에 설정된 정책의 타당성 여부를 주기적으로 검토하고 있는가?

정보보호 시스템 주기적 검토

「**접근통제 관리지침**」 제 ○○조 (정보보호 시스템관리)

① 정보보호 시스템운영자는 침입차단 정책 현황을 '방화벽 정책관리대장'에 기록해야 하며, 분기별 1회 접근통제 정책을 검토 후 부서 정보보호담당자의 승인을 득 해야 한다.

방화벽 정책 점검 결과보고

구분	직위	성명	일자	서명
승인	정보보호 담당자	OOO	2023-02-01	승인
기안	정보보호시스템 운영자	OOO	2022-01-29	

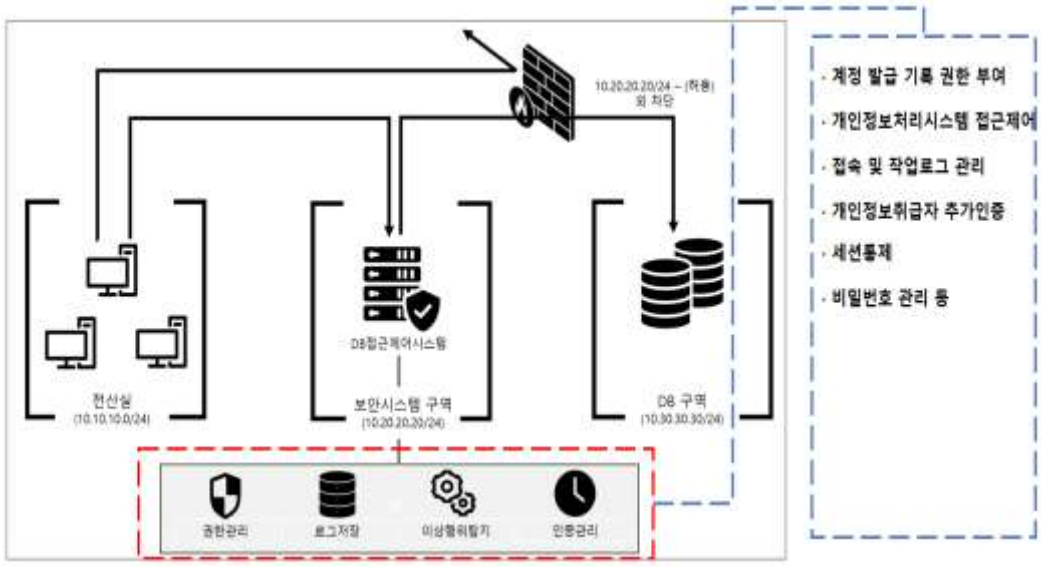
※ 방화벽 정책점검 결과보고(이해를 돕기 위한 예시)

◇ 개인정보처리시스템에 대한 불법적인 접근 및 개인정보 유출 방지를 위하여 관련법령에서 정한 기능을 수행하는 보안시스템을 설치하여 운영하고 있는가?

보안시스템 설치 및 운영

① 개인정보처리시스템에 대한 접속 권한을 IP 주소 등으로 제한하여 인가받지 않은 접근 제한

② 개인정보처리시스템에 접속한 IP 주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응



※ 개인정보처리시스템 보안시스템 설치 운영(이해를 돕기 위한 예시)

2.10.2 클라우드 보안

세부분야	2.10.2 클라우드 보안
인증 기준	클라우드 서비스 이용 시 서비스 유형(SaaS, PaaS, IaaS 등)에 따른 비인가 접근, 설정 오류 등에 따라 중요정보와 개인정보가 유·노출되지 않도록 관리자 접근 및 보안 설정 등에 대한 보호 대책을 수립·이행하여야 한다.
주요 확인사항	• 클라우드 서비스 제공자와 정보보호 및 개인정보보호에 대한 책임과 역할을 명확히 정의하고 이를 계약서(SLA 등)에 반영하고 있는가? • 클라우드 서비스 이용 시 서비스 유형에 따른 보안위험을 평가하여 비인가 접근, 설정 오류 등을 방지할 수 있도록 보안 구성 및 설정 기준, 보안 설정 변경 및 승인 절차, 안전한 접속방법, 권한 체계 등 보안 통제 정책을 수립·이행하고 있는가? • 클라우드 서비스 관리자 권한은 역할에 따라 최소화하여 부여하고 관리자 권한에 대한 비인가 접근, 권한 오·남용 등을 방지할 수 있도록 강화된 인증, 암호화, 접근통제, 감사 기록 등 보호 대책을 적용하고 있는가? • 클라우드 서비스의 보안 설정 변경, 운영 현황 등을 모니터링하고 그 적절성을 정기적으로 검토하고 있는가?
기준 요약도	
운영 방안	**◇ 클라우드 서비스 제공자와 정보보호 및 개인정보보호에 대한 책임과 역할을 명확히 정의하고 이를 계약서(SLA 등)에 반영하고 있는가?** **클라우드 환경에서의 보안관리 책임과 역할 정의 및 SLA 반영** ① 개인정보보호법

1.「**표준 개인정보보호지침**」기준 위탁계약 기재사항

- 위탁업무의 목적 및 범위, 위탁업무 기간, 재위탁 제한, 개인정보의 안전성 확보조치 등 '표준 개인정보처리위탁 계약서' 참고

② 전자금융감독규정

1.「**전자금융감독규정**」별표 2의5 기준 클라우드컴퓨팅서비스 위수탁 계약서 주요 기재사항

2. 기본 포함사항

- 클라우드서비스 이용 대상 업무 및 시스템 개요
- 위탁하는 업무 데이터에 관한 사항
- 위수탁 계약 및 재위탁 관련 중요 변경사항이 있는 경우 통보필요 사항
- 감독당국 또는 내외부 감사인의 조사・ 접근 수용 의무 등

3. 추가 포함사항

- 금융회사 등이 위탁한 정보처리가 실제 수행되는 위치
- 서비스 제공 중단 시 데이터 접근권한 등 비상대책에 관한 사항
- 위탁업무를 다른 수탁자나 금융회사로 이전할 경우 지원의무 및 전환계획 등

③ 클라우드컴퓨팅 발전법

1.「**클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률**」중 이용자 보호 조항

◇ 클라우드 서비스 이용 시 서비스 유형에 따른 보안위험을 평가하여 비인가 접근, 설정 오류 등을 방지할 수 있도록 보안 구성 및 설정 기준, 보안 설정 변경 및 승인 절차, 안전한 접속방법, 권한 체계 등 보안 통제 정책을 수립·이행하고 있는가?

서비스 유형별 보안위험 평가 및 통제정책

① IaaS 환경의 주요 위험

1. 가상머신 설정 오류 및 패치 관리 누락
2. 잘못된 네트워크 보안그룹 구성
3. 스토리지 버킷의 퍼블릭 노출
4. 암호화되지 않은 데이터 저장

② PaaS/SaaS 환경의 주요 위험

1. 과도한 애플리케이션 권한 부여
2. API 보안 취약점
3. 데이터 분리 및 접근통제 미흡
4. 서비스 간 통신 보안 부족

③ 보안 통제 정책 수립

1. 비인가 접근 및 설정오류 방지를 위한 핵심 정책 수립
2. 각 클라우드 서비스별 보안 설정 표준 정의
3. 보안설정 변경 시 승인 및 검토 프로세스 등 변경관리 절차 수립
4. 최소권한 원칙 기반 권한 관리 정책
5. 저장 및 전송 데이터 암호화 기준

※ 참고사항 : 퍼블릭 클라우드 서비스(AWS, AZURE, GCP)의 보안 설정 시 하기자료 참고

※ 출처: SK쉴더스 클라우드 보안 가이드(SK쉴더스)

◇ 클라우드 서비스 관리자 권한은 역할에 따라 최소화하여 부여하고 관리자 권한에 대한 비인가 접근, 권한 오·남용 등을 방지할 수 있도록 강화된 인증, 암호화, 접근통제, 감사기록 등 보호 대책을 적용하고 있는가?

클라우드 접근권한 세분화

① 클라우드 서비스 권한 세분화: 최고관리자, 네트워크 관리자, 보안관리자 등

② 업무 및 역할에 따라 관리자 권한 최소화 부여

③ 클라우드 관리자 권한 접속에 대한 강화된 인증 적용: OTP, 보안키 등

④ 원격 접속 구간에 대한 통신 암호화 또는 VPN 적용

⑤ 클라우드 관리자 접속, 권한 설정에 대한 상세 로그 기록 및 모니터링 등

◇ 클라우드 서비스의 보안 설정 변경, 운영 현황 등을 모니터링하고 그 적절성을 정기적으로 검토하고 있는가?

클라우드 운영현황 정기적 검토

① 클라우드 서비스에 대한 승인받지 않은 환경설정 및 보안 설정 변경을 적발할 수 있도록 알람 설정 및 모니터링

1. CSPM(Cloud Security Posture Management) 도구 활용

- 클라우드 리소스 구성 오류 자동 탐지
- 보안 정책 위반사항 실시간 식별
- 컴플라이언스 준수 상태 지속 모니터링
- 로그 수집 및 분석

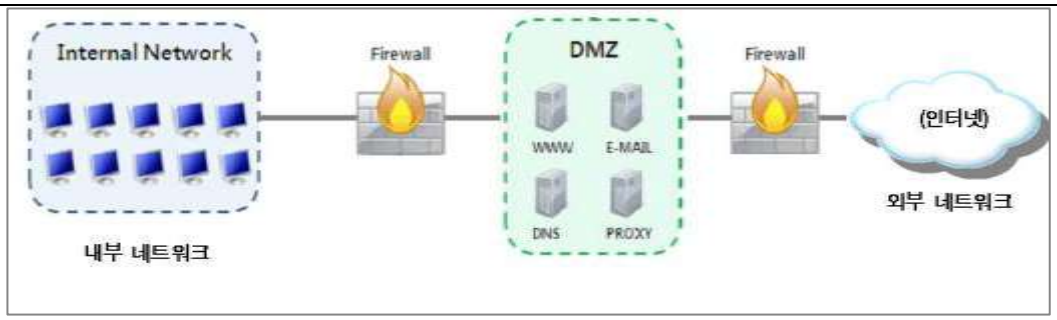
2. CloudTrail, CloudWatch 등 CSP 별 서비스를 통한 API 호출 추적

- 보안 이벤트 로그 중앙집중식 수집
- SIEM 솔루션 연동을 통한 통합 분석

② 클라우드 서비스 보안 설정의 적정성 여부를 정기적으로 검토 및 조치

2.10.3 공개서버 보안

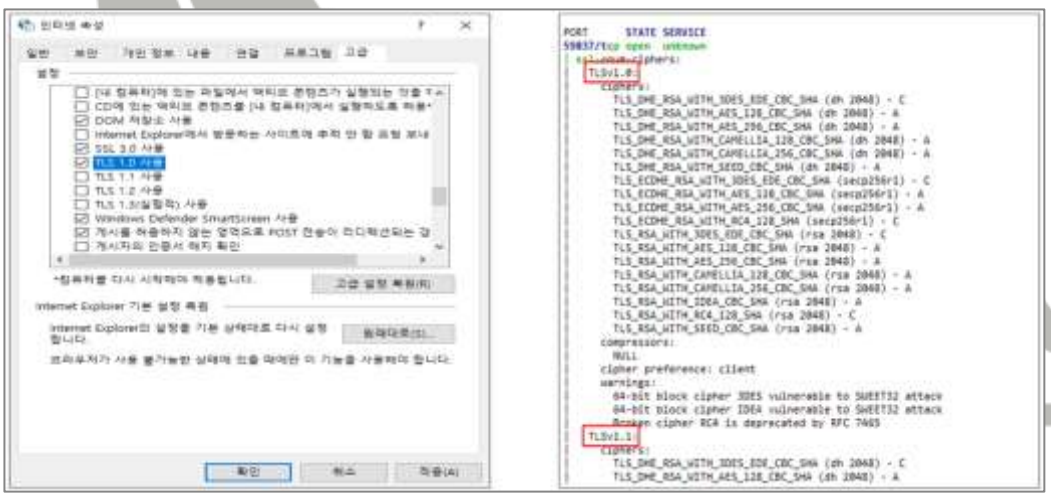
세부분야	2.10.3 공개서버 보안
인증 기준	외부 네트워크에 공개되는 서버의 경우 내부 네트워크와 분리하고 취약점 점검, 접근통제, 인증, 정보 수집·저장·공개 절차 등 강화된 보호 대책을 수립·이행하여야 한다.
주요 확인사항	• 공개서버를 운영하는 경우 이에 대한 보호 대책을 수립·이행하고 있는가? • 공개서버는 내부 네트워크와 분리된 DMZ 영역에 설치하고 침입차단시스템 등 보안 시스템을 통하여 보호하고 있는가? • 공개서버에 개인정보 및 중요정보를 게시하거나 저장하여야 할 경우 책임자 승인 등 허가 및 게시 절차를 수립·이행하고 있는가? • 조직의 중요정보가 웹사이트 및 웹서버를 통하여 노출되고 있는지 여부를 주기적으로 확인하여 중요정보 노출을 인지한 경우 이를 즉시 차단하는 등의 조치를 취하고 있는가?
기준 요약도	
운영 방안	**◇ 공개서버를 운영하는 경우 이에 대한 보호 대책을 수립·이행하고 있는가?** **(예시) 공개서버 보호 대책 수립** 「**접근통제 관리지침**」 제 ○○조 (공개서버 보안관리) ① 외부에 공개할 목적으로 설치되는 웹서버 등 공개서버를 내부망과 분리된 영역(DMZ)에 설치·운용하여야 한다.



※ 출처: 개인정보 안전성 확보조치 (개인정보보호위원회·KISA)

② 공개서버는 다음 각 호의 보안조치를 적용해야 한다.

1. 웹서버를 통한 개인정보 송수신 시 SSL/TLS인증서
2. 백신 설치 및 업데이트 설정
3. 응용프로그램(웹서버, OpenSSL 등), 운영체제 등에 대한 최신 보안패치 설치
4. 불필요한 서비스 제거 및 포트 차단
5. 에러 처리 페이지, 테스트 페이지 등 불필요한 페이지 노출 금지
6. 주기적 취약점 점검 수행



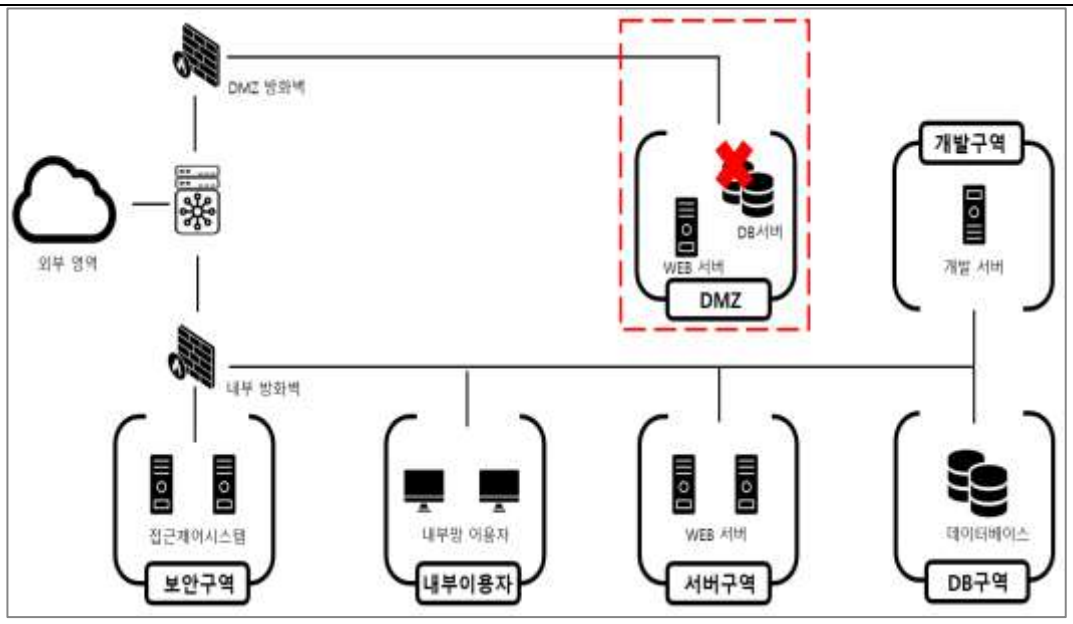
※ 전송구간 암호화 조치 확인(이해를 돕기 위한 예시)

◇ 공개서버는 내부 네트워크와 분리된 DMZ 영역에 설치하고 침입차단시스템 등 보안시스템을 통하여 보호하고 있는가?

공개서버 DMZ 영역 설치

① 공개서버가 침해당하더라도 공개서버를 통한 내부 네트워크 침입이 불가능하도록 침입차단시스템 등을 통한 접근통제 정책을 적용

② DMZ의 공개서버가 내부 네트워크에 위치한 데이터베이스, WAS 등의 정보시스템과 접속이 필요한 경우 엄격하게 접근통제 정책 적용



※ DMZ 구간 (이해를 돕기 위한 예시)

◇ 공개서버에 개인정보 및 중요정보를 게시하거나 저장하여야 할 경우 책임자 승인 등 허가 및 게시 절차를 수립·이행하고 있는가?

(예시) 개인정보 및 중요정보 게시 시 절차 수립

① 공개서버에 개인정보 및 중요정보를 게시하거나 저장하여야 할 경우 책임자 승인 등 허가 및 게시절차를 수립·이행

단계	담당자	주요 확인사항	관련 문서
게시 신청	신청자(업무담당자)	게시목적, 개인정보 범위, 게시기간 명시	개인정보 게시 신청서
사전 검토	업무부서 팀장	업무 필요성, 법적근거, 최소한의 정보 게시여부	업무부서 검토의견서
보안성 검토	정보보호담당자	개인정보 범위 적정성, 접근통제 설정	정보보호 보안성 검토서
최종 승인	정보보호책임자	전체 승인절차 적합성, 최종 게시 승인 여부	최종 승인서
게시 실행	시스템관리자	승인된 내용 범위내 게시, 보안설정 적용	게시 결과
사후 관리	정보보호담당자	게시내용 주기적 점검, 불법 노출 여부 확인	주기적 점검 보고서

※ 공개서버에 개인정보 게시 시 절차(이해를 돕기 위한 예시)

◇ 조직의 중요정보가 웹사이트 및 웹서버를 통하여 노출되고 있는지 여부를 주기적으로 확인하여 중요정보 노출을 인지한 경우 이를 즉시 차단하는 등의 조치를 취하고 있는가?

개인정보 및 중요정보 노출 점검

① 검색엔진 등을 통하여 주기적으로 점검 및 필요한 조치 적용

② 공개 웹 상에 개인정보 또는 내부 중요정보 게시 유무 정기적 점검 실시

③ 개인정보 및 중요정보 노출 여부 점검 결과보고서 작성

※ 출처: 홈페이지 개인정보 노출방지 안내서 (KISA)

2.10.4 전자거래 및 핀테크 보안

세부분야	2.10.4 전자거래 및 핀테크 보안
인증 기준	전자거래 및 핀테크 서비스 제공 시 정보 유출이나 데이터 조작·사기 등의 침해사고 예방을 위하여 인증·암호화 등의 보호 대책을 수립하고, 결제시스템 등 외부 시스템과 연계할 경우 안전성을 점검하여야 한다.
주요 확인사항	• 전자거래 및 핀테크 서비스를 제공하는 경우 거래의 안전성과 신뢰성 확보를 위한 보호 대책을 수립·이행하고 있는가? • 전자거래 및 핀테크 서비스 제공을 위하여 결제시스템 등 외부 시스템과 연계하는 경우 송수신되는 관련 정보의 보호를 위한 대책을 수립·이행하고 안전성을 점검하고 있는가?
기준 요약도	
운영 방안	**◇ 전자거래 및 핀테크 서비스를 제공하는 경우 거래의 안전성과 신뢰성 확보를 위한 보호 대책을 수립·이행하고 있는가?** **(예시) 전자거래 및 핀테크 서비스 보호대책 수립** ① 인증 및 접근통제 1. 다중인증(MFA): OTP, 인증서, 생체인증 등 2차 이상 인증 2. 계정 관리: 관리자 권한에 대한 엄격한 접근통제 ② 데이터 암호화 1. 전송 구간: SSL/TLS 1.3 이상 권고, HTTPS 강제 적용 2. 저장 구간: AES-256 암호화, 키 관리 체계(HSM) 구축 3. 종단간 암호화: E2E 암호화를 통한 완전한 데이터 보호 ③ 거래 무결성 보장 1. 전자서명: 공인인증서 또는 공동인증서 활용

2. 해시함수: SHA-256 이상의 안전한 해시 알고리즘

3. 블록체인: 거래내역의 위변조 방지 기술

④ 부정거래 탐지

1. AI/ML 기반 탐지: 이상 거래 패턴 실시간 분석

2. 규칙 기반 필터링: 임계값 설정을 통한 자동 차단

3. 행동 분석: 사용자 행동 패턴 분석을 통한 이상 탐지

⑤ 핀테크 서비스 보안대책

1. 가상자산 거래소 관련 요구사항

- 멀티시그 적용: 다중서명을 통한 출금 보안 강화
- 콜드월렛 관리: 오프라인 저장을 통한 개인키 보호
- 거래기록 보존: 15년간 가상자산 거래기록 보관

2. 간편결제 서비스 보안대책

- 토큰화 기술: 카드정보를 토큰으로 대체하여 저장
- 원터치 결제 보안: 생체인증과 결합한 간편 결제
- PCI-DSS 준수: 결제카드 산업 데이터 보안 표준 준수

◇ 전자거래 및 핀테크 서비스 제공을 위하여 결제시스템 등 외부 시스템과 연계하는 경우 송수신되는 관련 정보의 보호를 위한 대책을 수립·이행하고 안전성을 점검하고 있는가?

(예시) 시스템 연계 보호 대책 수립 및 점검

① 연계 인증 구간

1. API 키/인증서의 주기적 갱신 및 유효성 검증

2. 상호인증(Mutual Authentication) 구현 확인

3. 인증서 만료일 모니터링 체계 구축

② 통신 구간

1. SSL/TLS 버전 및 암호화 강도 점검

2. 취약한 암호화 알고리즘 사용 여부 확인

3. 인증서 검증 및 중간자 공격 방지

③ 데이터 전송 구간

1. 결제정보 암호화 적용 상태 확인

2. 키 관리 체계(KMS) 운영 현황 점검

3. 데이터 무결성 검증 메커니즘 확인

2.10.5 정보전송 보안

세부분야	2.10.5 정보전송 보안
인증 기준	다른 조직에 개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립하고 조직 간 합의를 통하여 관리 책임, 전송방법, 개인정보 및 중요정보 보호를 위한 기술적 보호조치 등을 협약하고 이행하여야 한다
주요 확인사항	• 외부 조직에 개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립하고 있는가? • 업무상 조직 간 개인정보 및 중요정보를 상호 교환하는 경우 안전한 전송을 위한 협약 체결 등 보호 대책을 수립·이행하고 있는가?
기준 요약도	
운영 방안	**◇ 외부 조직에 개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립하고 있는가?** **(예시) 개인정보 및 중요정보 전송 정책 수립** 「**접근통제 관리지침**」 제 ○○조 (정보전송 보안) ① 외부기관에 개인정보 등 중요정보를 전송할 경우 안전한 전송을 위한 협약을 체결하고 이행하여야 한다. 1. 업무정의: 개인정보 제3자 제공, 신용카드결제 정보 전달 등 2. 범위정의: 필요 최소한의 정보 송 수신 3. 기술표준: 암호화 방식, 키 교환 및 관리, 연계 및 통신 방식 등 4. 검토절차: 보고 및 승인, 관련 조직간 역할 및 책임, 보안성 검토 등 5. 협약기준: 보안약정서, 계약서, 부속합의서, SLA 등

6. 법적 요구사항을 반영한 보호조치: 전송·저장·파기 시 기술적 보호 대책

7. 상기업무를 수행할 담당자 및 책임자 지정

분 류	개인신용정보 전송요구		마이데이터사업자 전송	
	본인에게 전송	기관 간 전송		
인증방식	통합인증		통합인증	개별인증
본인인증/전송요구서작성화면 제공	전송요구앱		마이데이터사업자	정보제공자
전송요구 관계 (정보수신자:정보제공자)	1 : 1*		1 : N	1 : 1
API 요청 방식	전송요구앱 또는 정보수신자가 호출한 API는 거점기관을 경유하여 정보제공자에게 요청		마이데이터사업자가 직접 정보제공자(또는 중계기관)에게 API 요청	

※ 출처: 금융분야 개인신용정보 전송요구 표준 API 규격 (금융위원회·금융보안원)

◇ 업무상 조직 간 개인정보 및 중요정보를 상호 교환하는 경우 안전한 전송을 위한 협약체결 등 보호 대책을 수립·이행하고 있는가?

조직 간 상호교환 시 협약체결 등 보호대책 수립

① 교환 목적·범위 정의

1. 교환 대상 정보의 종류·범위·목적 명시
2. 상호교환 시점·주기·방법 고지

② 책임·역할 분담

1. 송신자 책임: 정보 송신 전 암호화·무결성 검증
2. 수신자 책임: 수신 후 무결성 확인, 저장 시 암호화 적용
3. 공동 책임: 사고 발생 시 공동 대응 절차·통보 의무

③ 보안대책

1. 안전 전송 정책 적용
2. 송·수신 서버의 취약점 점검, 최신 패치 적용
3. 접근통제: 상호교환 전용 계정 사용, MFA 적용

④ 위험관리·모니터링

1. 위험 분석: 연 1회 상호교환 보안위험 평가
2. 로그·감사: 교환 내역 로그 상호 공유, 정기적 감사
3. 침해 대응: 발견 즉시 동시 통보·차단 및 원인분석·재발방지

⑤ 계약 조건

1. 계약 기간·해지: 교환 기간 명시, 계약 위반 시 해지 조건
2. 재위탁 금지: 제3자 재위탁 금지 또는 사전 동의 절차 명시

	3. 손해배상: 위반 시 손해배상 범위·절차 규정 4. 정기적 교육 : 연 1회 이상 교환 담당자 대상 보안·절차 교육

2.10.6 업무용 단말기기 보안

세부분야	2.10.6 업무용 단말기기 보안
인증 기준	PC, 모바일 기기 등 단말기기를 업무 목적으로 네트워크에 연결할 경우 기기 인증 및 승인, 접근 범위, 기기 보안 설정 등의 접근통제 대책을 수립하고 주기적으로 점검하여야 한다.
주요 확인사항	• PC, 노트북, 가상PC, 태블릿 등 업무에 사용되는 단말기에 대하여 기기인증, 승인, 접근범위 설정, 기기 보안 설정 등의 보안 통제 정책을 수립·이행하고 있는가? • 업무용 단말기를 통하여 개인정보 및 중요정보가 유출되는 것을 방지하기 위하여 자료 공유프로그램 사용 금지, 공유설정 제한, 무선망 이용 통제 등의 정책을 수립·이행하고 있는가? • 업무용 모바일 기기의 분실, 도난 등으로 인한 개인정보 및 중요정보의 유·노출을 방지하기 위하여 보안대책을 적용하고 있는가? • 업무용 단말기기에 대한 접근통제 대책의 적절성에 대하여 주기적으로 점검하고 있는가?
기준 요약도	
운영 방안	**◇ PC, 노트북, 가상PC, 태블릿 등 업무에 사용되는 단말기에 대하여 기기인증, 승인, 접근범위 설정, 기기 보안 설정 등의 보안 통제 정책을 수립·이행하고 있는가?** **업무용 단말기기 보안통제** ① 기기 등록 및 인증 1. 사내 승인 모델만 사용하며 IP, MAC 주소 등 자산현황·관리 2. 별도 인증서 설치 및 상호인증 적용 3. 사용자 인증은 ID/PW + OTP(2차 인증) 병용

② 사용 승인 절차

1. 신청서 작성(사용 목적·기간·접근범위 기재) → 부서장·정보보호팀 보안 검토 → 정보보호책임자 최종 승인

2. 승인된 단말기에 한해 접근범위 설정

③ 접근범위 설정

1. 사용자 유형별 권한 분리

- 일반직원: 그룹웨어·업무시스템

- 개발자: 개발·테스트 환경

- 관리자: 운영·관리 인터페이스

2. 네트워크 분리(업무망·개발망·관리망·인터넷망) 및 VPN/전용선 사용

④ 운영체제 별 보안설정 기준 수립

1. Windows: 관리자 계정 비활성화, 화면보호기 잠금(10분), USB·공유폴더 차단 등

2. macOS: SIP 활성화, 자동 잠금(10분) 등

⑤ 보안 SW 설치

1. 백신, 개인방화벽, DLP, 패치관리 에이전트 의무화

2. 모바일/태블릿 : 잠금화면 패턴/생체인증, 인가된 앱만 설치, 루팅 탐지 등

⑥ 주기적 점검 및 모니터링

1. 일일: 백신·패치 현황, 보안 로그 확인

2. 월간: 단말기 등록·소프트웨어 설치 상태 점검

3. 분기별: 보안정책 준수율 평가, 기기 위험도 재평가

◇ 업무용 단말기를 통하여 개인정보 및 중요정보가 유출되는 것을 방지하기 위하여 자료 공유 프로그램 사용 금지, 공유설정 제한, 무선망 이용 통제 등의 정책을 수립·이행하고 있는가?

업무용 단말기 자료공유 및 무선망 통제정책

① 적용범위

1. 업무용 PC, 노트북, 가상PC, 태블릿, 업무용 스마트폰

2. 사내·원격 근무 환경 모두 적용

② 금지 항목 및 통제 조치

1. 자료공유프로그램(파일공유 P2P) 사용 금지

2. BitTorrent, eMule, Kazaa, Dropbox 등 파일공유 프로그램 금지

3. 설치 시 자동 제거 스크립트 및 중앙관리 서버에서 차단

4. 네트워크 차단: 방화벽·IPS 룰로 P2P 포트·프로토콜 차단

③ 공유 설정 제한

1. AD 등을 통한 로컬·네트워크 공유 폴더 기능 비활성화
2. Windows 파일 및 프린터 공유 서비스 중지
3. macOS의 파일 공유, AirDrop 비활성화
4. MDM 정책으로 공유 설정 잠금

◇ 업무용 모바일 기기의 분실, 도난 등으로 인한 개인정보 및 중요정보의 유·노출을 방지하기 위하여 보안대책을 적용하고 있는가?

업무용 단말 정보보호 시스템 설치 운영

① 파일 전송이 주된 목적일 때에는 읽기 권한만을 부여하고 상대방이 쓰기를 할 때만 개별적으로 쓰기 권한 설정

② P2P 프로그램, 상용 웹메일, 웹하드, 메신저, SNS 서비스 등을 통하여 고의·부주의로 인한 개인정보 및 중요정보의 유·노출 방지

③ WPA2(Wi-Fi Protected Access 2) 등 보안 프로토콜이 적용된 무선망 이용 등

※ 출처: 네트워크접근통제 NAC를 통한 보안프로그램 설치 (SK쉴더스)

◇ 업무용 단말기기에 대한 접근통제 대책의 적절성에 대하여 주기적으로 점검하고 있는가?

업무용 단말 주기적 검토

① 업무용 단말기 신청·승인, 등록·해제, 기기인증 이력

② 업무용 단말기 보안 설정 현황 등

2.10.7 보조저장매체 관리

세부분야	2.10.7 보조저장매체 관리
인증 기준	보조저장매체를 통하여 개인정보 또는 중요정보의 유출이 발생하거나 악성코드가 감염되지 않도록 관리 절차를 수립·이행하고, 개인정보 또는 중요정보가 포함된 보조저장매체는 안전한 장소에 보관하여야 한다.
주요 확인사항	• 외장하드, USB메모리, CD 등 보조저장매체 취급(사용), 보관, 폐기, 재사용에 대한 정책 및 절차를 수립·이행하고 있는가? • 보조저장매체 보유현황, 사용 및 관리실태를 주기적으로 점검하고 있는가? • 주요 정보시스템이 위치한 통제구역, 중요 제한구역 등에서 보조저장매체 사용을 제한하고 있는가? • 보조저장매체를 통한 악성코드 감염 및 중요정보 유출 방지를 위한 대책을 마련하고 있는가? • 개인정보 또는 중요정보가 포함된 보조저장매체를 잠금장치가 있는 안전한 장소에 보관하고 있는가?
기준 요약도	
운영 방안	**◇ 외장하드, USB메모리, CD 등 보조저장매체 취급(사용), 보관, 폐기, 재사용에 대한 정책 및 절차를 수립·이행하고 있는가?** **(예시) 보조저장매체 관리 절차 수립** 「**휴대용 저장매체 관리 매뉴얼**」 제 ○○조 (보조저장매체 관리) ① 보조저장매체 보유 현황 관리 방안 1. 정보보호담당자는 보조저장매체의 등록 및 불용처리 등에 관한 기록을 보조저장매체 관리대장에 기록·관리하여야 한다.

2. 부서 정보보호 책임자는 월1회 이상 보조기억매체 수량 및 보관상태를 점검하고 정보보호담당자에게 승인을 득해야 한다.

② 보조저장매체 사용허가 및 등록 절차

③ 보조저장매체 반출·입 관리 절차

1. 관리책임자는 휴대용 저장매체의 반·출입을 통제하여야 하며 보조기억매체 반출입관리대장에 기록관리 해야 한다.

④ 보조저장매체 폐기 및 재사용 절차

⑤ 보조저장매체 사용 범위: 통제구역, 제한구역 등 보호구역별 사용 정책 및 절차

⑥ 보조저장매체 보호 대책 등

보조저장매체 관리 대장

순번	관리번호(S/N)	매체형태	등록일자	취급자 (성명)	불용처리 일자	불용처리방법 (재사용용도)	비고 (사유)

※ 보조저장매체 관리대장 (이해를 돕기 위한 예시)

◇ 보조저장매체 보유현황, 사용 및 관리실태를 주기적으로 점검하고 있는가?

보조저장매체 현황 주기적 검토

① 보조저장매체 사용 승인 증적, 보유 현황, 관리 대장, 사용이력 확인 등 관리 실태 점검

보조 저장매체 점검대장

점검일시	현 보유수량					이상 유무	정보보호담당자 (서명)
	2 등급	3 등급	대외비	일반	인증		

※ 보조저장매체 점검대장 (이해를 돕기 위한 예시)

◇ 주요 정보시스템이 위치한 통제구역, 중요 제한구역 등에서 보조저장매체 사용을 제한하고 있는가?

통제구역 보조저장매체 제한

① 불가피하게 사용할 경우 책임자의 허가절차를 거친 후 적법한 절차에 따른 사용

② 통제구역, 중요 제한구역 내 보조저장매체 사용 현황에 대한 정기적인 검토 수행

◇ 보조저장매체를 통한 악성코드 감염 및 중요정보 유출 방지를 위한 대책을 마련하고 있는가?

	보조저장매체를 통한 악성코드 감염 및 중요정보 유출 방지를 위한 대책 수립 ① 보조저장매체 자동실행 방지 및 백신프로그램 검사 후 사용 등 보호 대책 수립·이행 **◇ 개인정보 또는 중요정보가 포함된 보조저장매체를 잠금장치가 있는 안전한 장소에 보관하고 있는가?** **물리적 안전한 장소 보관** ① 개인정보 또는 중요정보가 포함된 보조저장매체(이동형 하드디스크, USB메모리, SSD 등)는 금고, 잠금장치가 있는 안전한 장소에 보관

2.10.8 패치관리

세부분야	2.10.8 패치관리
인증 기준	소프트웨어, 운영체제, 보안시스템 등의 취약점으로 인한 침해사고를 예방하기 위하여 최신 패치를 적용하여야 한다. 다만 서비스 영향을 검토하여 최신 패치 적용이 어려울 경우 별도의 보완대책을 마련하여 이행하여야 한다.
주요 확인사항	• 서버, 네트워크시스템, 보안시스템, PC 등 자산별 특성 및 중요도에 따라 운영체제(OS)와 소프트웨어의 패치관리 정책 및 절차를 수립·이행하고 있는가? • 주요 서버, 네트워크시스템, 보안시스템 등의 경우 설치된 OS, 소프트웨어 패치 적용 현황을 주기적으로 관리하고 있는가? • 서비스 영향도 등에 따라 취약점을 조치하기 위한 최신의 패치 적용이 어려운 경우 보완대책을 마련하고 있는가? • 주요 서버, 네트워크시스템, 보안시스템 등의 경우 공개 인터넷 접속을 통한 패치를 제한하고 있는가? • 패치관리시스템을 활용하는 경우 접근통제 등 충분한 보호 대책을 마련하고 있는가?
기준 요약도	
운영 방안	**◇ 서버, 네트워크시스템, 보안시스템, PC 등 자산별 특성 및 중요도에 따라 운영체제(OS)와 소프트웨어의 패치관리 정책 및 절차를 수립·이행하고 있는가?** **(예시) 자산별 패치관리 절차 수립** 「**정보자산 관리지침**」 제 ○○조 (패치관리) ① 패치를 통해 정보자산의 취약점을 신속하게 제거하여 정보자산의 가용성·무결성·기밀성을 보호한다 ② 대상이 되는 적용범위는 다음과 같이 규정한다.

1. 전사 서버(물리·가상), 네트워크 장비 등 정보자산
2. 업무용 PC, 노트북, 가상PC, 태블릿·모바일 등 모든 단말기
3. 주요 업무 애플리케이션, DBMS, 미들웨어 등

③ 패치관리를 위한 업무는 다음 각 호와 같다.

1. 보안운영팀: 패치관리 정책 수립·검토, 취약점 모니터링
2. 시스템운영팀: 테스트 환경 구축, 패치 검증·배포
3. 서비스담당부서: 적용 대상 시스템 식별·업무 영향도 평가

④ 새로운 취약성에 대한 보안패치가 발표되는 즉시 시스템에 적용한다. 다만, 서비스 영향도 등에 따라 최신 패치 적용이 어려운 경우 각 호에 따라 보안대책을 마련한다.

1. 운영 시스템의 경우 시스템 영향도 검토 후 패치 적용
2. 운영 환경에 따라 패치 적용이 어려운 경우 그 사유와 추가 보안대책을 마련하여 정보보호책임자에게 보고하고 그 현황을 관리

◇ 주요 서버, 네트워크시스템, 보안시스템 등의 경우 설치된 OS, 소프트웨어 패치 적용현황을 주기적으로 관리하고 있는가?

(예시) 패치 적용현황 주기적 관리

「**정보자산 관리지침**」 제 ◌◌조 (패치관리)

① 정보자산의 패치 적용현황을 '패치관리대장'에 기록하고, 관리자는 최신 보안패치 여부를 반기 1회 확인하여야 한다.

서버 패치관리대장

서버 담당자	정보보호담당자

서버명		IP	

순번	패치명	패치 ID	용도	패치일	담당자	비고
1						
2						
3						
4						
…	…	…	…	…	…	…

※ 서버패치관리대장 (이해를 돕기 위한 예시)

◇ 서비스 영향도 등에 따라 취약점을 조치하기 위한 최신의 패치 적용이 어려운 경우 보완대책을 마련하고 있는가?

서비스 중요도에 따른 보안대책 적용

① 운영 시스템에 패치를 적용하는 경우 시스템 가용성에 영향을 미칠 수 있으므로 운영 시스템의 중요도와 특성을 고려하여 영향도 분석 등 정해진 절차에 따라 분하게 영향을 분석한 후 적용

② 운영 환경에 따라 즉시 패치 적용이 어려운 경우 그 사유와 추가 보완대책을 마련하여 책임자에게 보고하고 그 현황을 관리

◇ 주요 서버, 네트워크시스템, 보안시스템 등의 경우 공개 인터넷 접속을 통한 패치를 제한하고 있는가?

주요 시스템 패치

① 주요 서버, 네트워크시스템, 보안시스템 등의 경우 공개 인터넷 접속을 통한 패치를 제한

1. 불가피한 경우 사전 위험분석을 통하여 보호 대책을 마련하여 책임자 승인 적용

◇ 패치관리시스템을 활용하는 경우 접근통제 등 충분한 보호 대책을 마련하고 있는가?

(예시) 패치관리시스템 보호 대책 수립

「**정보자산 관리지침**」 제 ○○조 (패치관리)

① 패치관리시스템(PMS) 활용 시 다음 각 호의 보호 대책을 마련해야 한다.

1. 패치관리시스템에 대한 안전성 확보 조치(접근제어, 보안취약점 제거 등
2. 업데이트 파일 배포 시 파일 무결성 검사 등

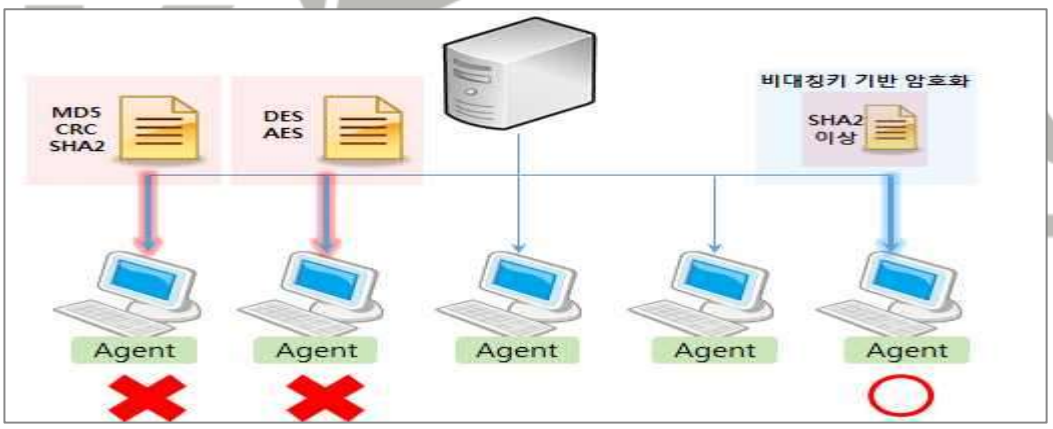
중앙관리소프트웨어 보안

- **(파일 무결성 검증)** 실행바이너리, 설치, 업데이트, 정책 파일 등 파일에 대한 무결성 검증을 수행해야 한다.
- **(안전한 방법의 무결성 검증기술 사용)** 무결성 검증은 클라이언트에 하드코딩 된 값 또는 CRC 비교가 아닌 공개키 방식 등 안전한 방법으로 검증해야 한다.
- **(안전한 암호화 알고리즘 및 키 관리)** 파일 전송 통신 구간 등은 안전한 암호화 알고리즘 사용 및 키 관리를 수행해야 한다.
- **(클라이언트 프로그램 상시 오픈포트 제거)** 클라이언트 프로그램에서 명령어 또는 파일을 수신하기 위해 사용하는 상시 오픈 포트를 제거해야 한다.
- **(원격 시스템 명령어 처리 기능 제거)** 관리 서버에서 원격으로 클라이언트에 시스템 명령 실행 기능을 제거해야 한다.
- **(고객 요청 기능 시)** 고객의 요청에 의해 기본 제품의 기능 외 추가적인 기능을 제공해야 할 때, 보안을 고려하여 기능을 제공하여야 한다.
- **(정책 설정 보안 관리)** 서버와 에이전트간의 정책 설정은 지정된 관리자만 수행할 수 있도록 구현해야 한다.
- **(중앙 관리 서버 IP, URL 변조 불가)** 중앙 관리 서버 IP, URL의 변조가 불가능하도록 구성되어 있어야 한다.
- **(서버↔클라이언트 간 안전한 상호 인증)** 서버↔클라이언트 간 안전한 상호 인증 절차가 존재해야 한다.
- **(관리 S/W ID, PW 암호화)** 관리자 ID, PW에 대해 통신 구간 암호화가 적용되어 있어야 한다.

관리프로그램 보안

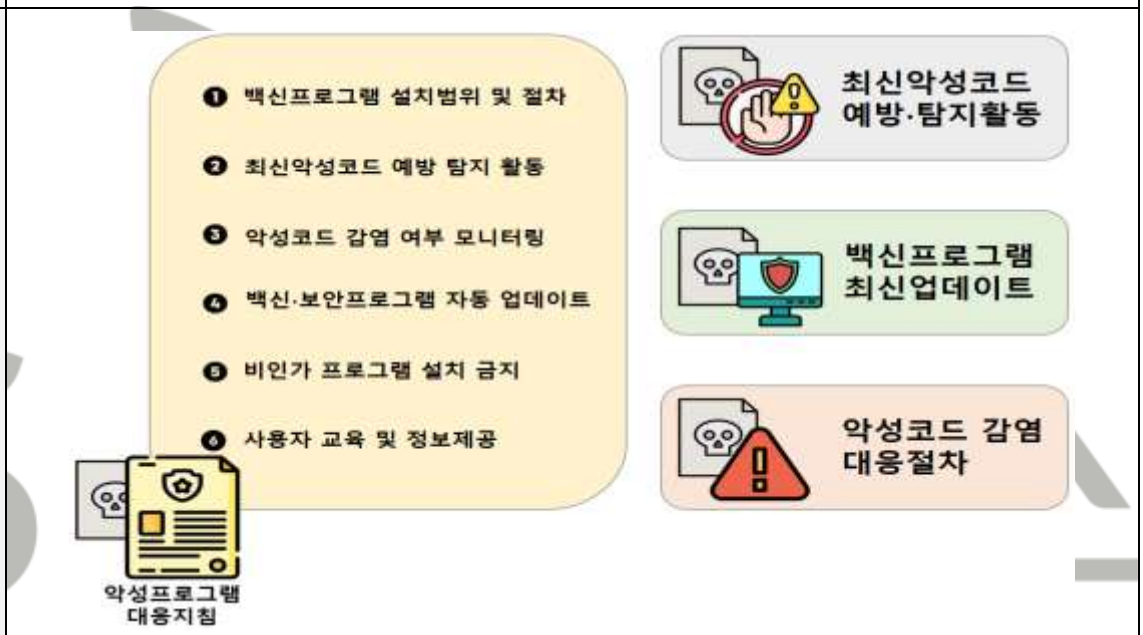
- **(계정 관리)** 개발사에서 관리 목적으로 만든 불필요한 계정이 없어야 한다.
- **(패스워드 관리)** 관리자 계정 생성 시 비밀번호 복잡도(2조합 10글자 또는 3조합 8글자)를 만족하도록 설정해야 하며, 최초 설치 시 사용자에게 패스워드를 설정하도록 유도해야 한다.
- **(접근통제)** 접근 가능한 관리자 IP 지정 등을 통한 중앙 관리 프로그램에 대한 접근 통제 기능을 제공해야 한다.
- **(세션 타임 아웃 설정)** 관리 프로그램을 일정 시간 동안 사용하지 않을 경우, 로그아웃 되도록 세션 타임아웃 기능을 제공해야 한다.
- **(자동 접속 제한)** 관리 프로그램에 대한 자동 로그인 기능을 제공해서는 안 된다.
- **(ID/PW 평문 전송 서비스 미사용)** 평문으로 패킷이 전송되는 서비스 기능을 제공해서는 안 된다.
- **(로그 관리)** 접속 로그, 설정 변경 로그를 기록하는 기능 등 시스템 로그는 최소 3개월 이상 로그를 기록하도록 제공 한다.

※ 출처: 중앙 관리 소프트웨어 보안가이드 (KISA)



※ 출처: 중앙 관리형 소프웨어 보안가이드 (KISA)

2.10.9 악성코드 통제

세부분야	2.10.9 악성코드 통제
인증 기준	바이러스·웜·트로이목마·랜섬웨어 등의 악성코드로부터 개인정보 및 중요정보, 정보시스템 및 업무용 단말기 등을 보호하기 위하여 악성코드 예방·탐지·대응 등의 보호 대책을 수립·이행하여야 한다.
주요 확인사항	• 바이러스, 웜, 트로이목마, 랜섬웨어 등의 악성코드로부터 정보시스템 및 업무용 단말기 등을 보호하기 위하여 보호 대책을 수립·이행하고 있는가? • 백신 소프트웨어 등 보안프로그램을 통하여 최신 악성코드 예방·탐지 활동을 지속적으로 수행하고 있는가? • 백신 소프트웨어 등 보안프로그램은 최신의 상태로 유지하고 필요시 긴급 보안 업데이트를 수행하고 있는가? • 악성코드 감염 발견 시 악성코드 확산 및 피해 최소화 등의 대응 절차를 수립·이행하고 있는가?
기준 요약도	
운영 방안	**◇ 바이러스, 웜, 트로이목마, 랜섬웨어 등의 악성코드로부터 정보시스템 및 업무용 단말기 등을 보호하기 위하여 보호 대책을 수립·이행하고 있는가?** **(예시) 악성코드 보호 대책 수립** 「**정보자산 관리지침**」 제 ○○조 (악성코드 관리) ① 모든 PC·노트북은 사내 백신프로그램을 설치하여야 한다. ② 백신프로그램은 항상 최신 버전으로 업데이트해야 하며, 실시간 감시 기능을 사용하여 바이러스 감염 전 자동적으로 점검되도록 한다. ③ 메신저·P2P·웹하드 등 업무에 무관하거나 불필요한 Active-X 등 보안에 취약한 프로그램과 비인가 프로그램·장치의 설치를 금지한다.

◇ 백신 소프트웨어 등 보안프로그램을 통하여 최신 악성코드 예방·탐지 활동을 지속적으로 수행하고 있는가?

최신 악성코드 예방·탐지 활동

① 이메일 등 첨부파일에 대한 악성코드 감염 여부 검사

② 실시간 악성코드 감시 및 치료

③ 주기적인 악성코드 점검: 자동 바이러스 점검 일정 설정

◇ 백신 소프트웨어 등 보안프로그램은 최신의 상태로 유지하고 필요시 긴급 보안 업데이트를 수행하고 있는가?

백신 업데이트 주기 및 Hotfix 관련 대책 수립

① 백신 업데이트 주기 준수: 자동 업데이트 또는 일1회 이상 업데이트 악성 프로그램 관련 경보가 발령되거나 긴급 업데이트 공지가 있는 경우 이에 따른 업데이트 수행

② 백신 중앙관리시스템을 이용하여 백신프로그램을 관리하는 경우 관리서버에 대한 접근통제, 배포 파일에 대한 무결성 검증 등 보호 대책 마련

◇ 악성코드 감염 발견 시 악성코드 확산 및 피해 최소화 등의 대응 절차를 수립·이행하고 있는가?

(예시) 악성코드 감염 대응 절차 수립

① 악성코드 탐지

1. 실시간 모니터링: EDR·IPS·안티바이러스 솔루션 등으로 의심행위 탐지
2. 알림 체계: 탐지 즉시 정보보호팀 알람 및 SIEM 기록

② 악성코드 및 관련 시스템 격리

1. 네트워크 차단: 감염 단말을 네트워크에서 즉시 분리(스위치 포트 차단, NAC 동작)
2. 프로세스 중단: 악성 프로세스·서비스 강제 종료

③ 악성코드 분석

1. 샘플 수집: 악성 파일·메모리 덤프 확보
2. 기초분석: 해시, 속성, C2 주소 등 정보 수집
3. 심층분석: 샌드박스 실행·행위 분석

④ 악성코드 제거

1. EDR·안티바이러스 전용 엔진으로 완전 치료 또는 격리
2. 수동으로 레지스트리·파일시스템 정리(전문인력 수행)

	⑤ 시스템 복구 1. 백업복원: 최신 백업자료를 통해 시스템·데이터 복원 2. 재발 방지: 취약점 패치·보안설정 강화 3. 재검증: 복구 후 재감염 여부 점검 ⑥ 보고 및 문서화 1. 사고보고: 경영진 및 관련 부서에 대응결과 보고 2. 사고기록: 대응조치, 타임라인, 교육사항 문서화 ⑦ 사후조치 1. 원인분석: 침입경로·취약점·피해규모 파악 2. 정책개선: 대응절차·보안통제·교육 체계 보완 3. 재발방지 교육: 전사 보안 인식 제고 교육 실시

2.11 사고 예방 및 대응

2.11.1 사고 예방 및 대응체계 구축

세부분야	2.11.1 사고 예방 및 대응체계 구축
인증 기준	침해사고 및 개인정보 유출 등을 예방하고 사고 발생 시 신속하고 효과적으로 대응할 수 있도록 내·외부 침해시도의 탐지·대응·분석 및 공유를 위한 체계와 절차를 수립하고, 관련 외부기관 및 전문가들과 협조체계를 구축하여야 한다.
주요 확인사항	• 침해사고 및 개인정보 유출사고를 예방하고 사고 발생 시 신속하고 효과적으로 대응하기 위한 체계와 절차를 마련하고 있는가? • 보안관제서비스 등 외부 기관을 통하여 침해사고 대응체계를 구축·운영하는 경우 침해사고 대응 절차의 세부사항을 계약서에 반영하고 있는가? • 침해사고의 모니터링, 대응 및 처리를 위하여 외부전문가, 전문업체, 전문기관 등과의 협조체계를 수립하고 있는가?
기준 요약도	
운영 방안	**◇ 침해사고 및 개인정보 유출사고를 예방하고 사고 발생 시 신속하고 효과적으로 대응하기 위한 체계와 절차를 마련하고 있는가?** **(예시) 사고 대응 체계 및 절차 수립** **「침해사고 대응 매뉴얼」** ① 침해사고의 정의 및 범위 1. 정보자산의 손실·절도·파괴 등이 발생하여 정상적인 업무에 지장을 초래하는 사고 ② 침해사고 유형 및 중요도 1. 침해사고 유형 - 정보시스템: 정보통신망에 대한 해킹, 악성코드 유포 등 - 정보자료: 비밀자료 유출·파괴·변조 및 노출 등 - 암호장비: 암호장비 키 운용체계 노출 등 2. 침해사고 중요도 분류 - 심각: 핵심 서비스 중단, 대규모 내부 정보 유출 등 기업이나 기관에 막대한 금전적

손실을 초래하는 사고.

- 주의: 일부 서비스 중단, 경미한 정보 유출 등 영업에 미치는 영향이 비교적 적은 사고.

- 관심: 서비스에는 직접적인 영향을 주지 않으나, 향후 확산될 가능성이 있거나 잠재적인 위협이 될 수 있는 사고.

③ 침해사고 선포절차 및 방법

④ 비상 연락망 등의 연락체계

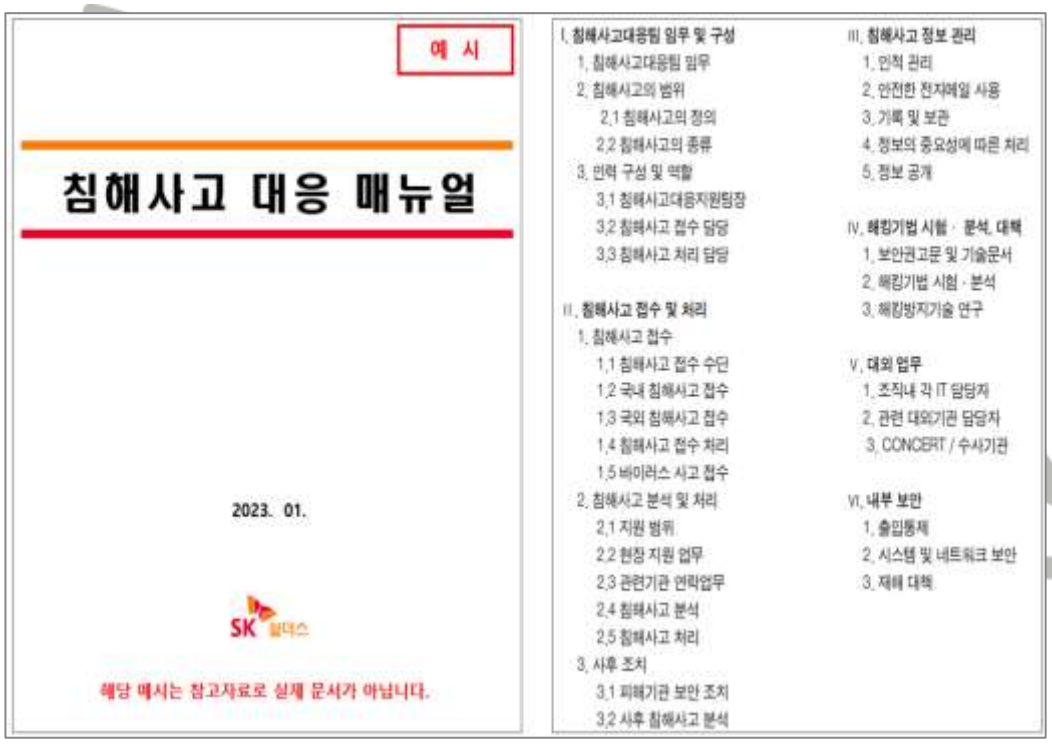
1. 침해사고 비상 연락망

- 침해사고대응팀 연락망: 침해사고팀장, 침해사고 분석담당자 등

- 관련 부서 연락망: 서비스보안팀, 부서별 보안담당자 등

- 관련 업체 연락망: 정보보호전문업체, 정보보호시스템 업체 등

⑤ 침해사고 탐지 체계


예 시

침해사고 대응 매뉴얼

2023. 01.

SK 쉴더스

해당 예시는 참고자료로 실제 문서가 아닙니다.

I. 침해사고대응팀 임무 및 구성
1. 침해사고대응팀 임무
2. 침해사고의 범위
2.1 침해사고의 정의
2.2 침해사고의 종류
3. 인력 구성 및 역할
3.1 침해사고대응지원팀장
3.2 침해사고 접수 담당
3.3 침해사고 처리 담당

II. 침해사고 접수 및 처리
1. 침해사고 접수
1.1 침해사고 접수 수단
1.2 국내 침해사고 접수
1.3 국외 침해사고 접수
1.4 침해사고 접수 처리
1.5 바이러스 사고 접수
2. 침해사고 분석 및 처리
2.1 지원 범위
2.2 현장 지원 업무
2.3 관련기관 연락업무
2.4 침해사고 분석
2.5 침해사고 처리
3. 사후 조치
3.1 피해기관 보안 조치
3.2 사후 침해사고 분석

III. 침해사고 정보 관리
1. 인적 관리
2. 안전한 전자메일 사용
3. 기록 및 보관
4. 정보의 중요성에 따른 처리
5. 정보 공개

IV. 해킹기법 시험 · 분석, 대책
1. 보안권고문 및 기술문서
2. 해킹기법 시험 · 분석
3. 해킹방지기술 연구

V. 대외 업무
1. 조직내 각 IT 담당자
2. 관련 대외기관 담당자
3. CONCERT / 수사기관

VI. 내부 보안
1. 출입통제
2. 시스템 및 네트워크 보안
3. 재해 대책

※ 침해사고 대응 매뉴얼 (이해를 돕기 위한 예시)

◇ 보안관제서비스 등 외부 기관을 통하여 침해사고 대응체계를 구축·운영하는 경우 침해사고 대응 절차의 세부사항을 계약서에 반영하고 있는가?

침해사고 대응절차 세부사항 계약서 반영

① 보안관제서비스의 범위

② 침해 징후 발견 시 보고 및 대응 절차

③ 침해사고 발생 시 보고 및 대응 절차

④ 침해사고 발생에 따른 책임 및 역할에 관한 사항 등

◇ 침해사고의 모니터링, 대응 및 처리를 위하여 외부전문가, 전문업체, 전문기관 등과의 협조체계를 수립하고 있는가?

침해사고 대비 협조체계 현행화

① 침해사고 대비 비상 연락망 현행화

침해사고 대비 비상 연락망

침해사고 대응팀 연락망			
부서	담당업무	담당자명	연락처
...	...	...	...

관련업체 연락망			
부서	담당업무	담당자명	연락처
...	...	...	...

관련기관 연락망			
부서	담당업무	담당자명	연락처
...	...	...	...

※ 협조체계 수립을 위한 비상 연락망 (이해를 돕기 위한 예시)

2.11.2 취약점 점검 및 조치

세부분야	2.11.2 취약점 점검 및 조치
인증 기준	정보시스템의 취약점이 노출되어 있는지를 확인하기 위하여 정기적으로 취약점 점검을 수행하고, 발견된 취약점에 대해서는 신속하게 조치하여야 한다. 또한 최신 보안취약점의 발생 여부를 지속적으로 파악하고, 정보시스템에 미치는 영향을 분석하여 조치하여야 한다.
주요 확인사항	• 정보시스템 취약점 점검 절차를 수립하고, 정기적으로 점검을 수행하고 있는가? • 발견된 취약점에 대한 조치를 수행하고, 그 결과를 책임자에게 보고하고 있는가? • 최신 보안취약점 발생 여부를 지속적으로 파악하고, 정보시스템에 미치는 영향을 분석하여 조치하고 있는가? • 취약점 점검 이력을 기록 관리하여 전년도에 도출된 취약점이 재발생하는 등의 문제점에 대하여 보호 대책을 마련하고 있는가?
기준 요약도	
운영 방안	◇ 정보시스템 취약점 점검 절차를 수립하고, 정기적으로 점검을 수행하고

있는가?

(예시) 취약점 점검 절차 수립

「**정보자산 관리지침**」 제 ○○조 (취약점 점검계획)

① 정보보호 책임자는 정보서비스 전체를 대상으로 주기적(연 1회 이상)으로 취약점 점검을 수행하여야 한다.

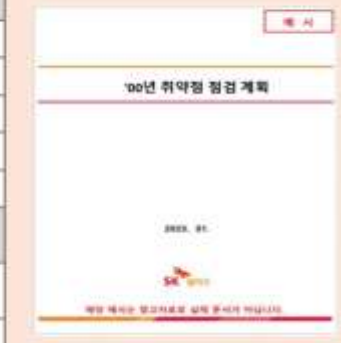
② 정보보호담당자는 취약점 점검 계획을 수립하고 정보보호 책임자의 승인을 받은 후에 수행하여야 한다. 취약점 점검 계획에는 다음의 사항이 포함되어야 한다.

1. 취약점 점검대상
2. 취약점 점검일정
3. 취약점 점검 담당자 및 책임자
4. 취약점 점검 절차 및 방법

③ 취약점 점검결과 발견된 취약점별로 대응방안 및 조치 결과를 문서화하여야 하며 조치 결과서를 작성하여 정보보호 최고책임자에게 보고하여야 한다

'00년 취약점 점검 계획

순번	내용			
1	점검 목적			
2	점검 대상			
3	점검 일정			
4	취약점 점검 담당자 및 책임자			
5	취약점 점검 절차 및 방법			
구분	직위	성명	일자	서명
승인	정보보호 최고책임자	OOO	2023-01-01	승인
상신	정보보호 담당자	OOO	2022-12-20	-



※ 취약점 점검 계획(이해를 돕기 위한 예시)

※ 출처: SK쉴더스 취약점진단 서비스 (https://www.skshieldus.com)

◇ 발견된 취약점에 대한 조치를 수행하고, 그 결과를 책임자에게 보고하고 있는가?

취약점 점검 및 조치 결과 보고

① 취약점 점검 시 이력 관리가 될 수 있도록 점검일시, 점검대상, 점검방법, 점검내용 및 결과, 발견사항,

② 조치사항 등이 포함된 보고서 작성

③ 취약점별로 대응조치 완료 후 이행점검 등을 통하여 완료 여부 확인

④ 불가피하게 조치할 수 없는 취약점에 대해서는 그 사유를 명확하게 확인하고, 이에 따른 위험성, 보완대책 등을 책임자에게 보고

00년 취약점 조치 보고

구분	직위	성명	일자	서명
승인	정보보호 최고책임자	OOO	2023-02-01	승 인
기안	정보보호 담당자	OOO	2022-01-29	

※ 취약점 점검 결과보고서 (이해를 돕기 위한 예시)

◇ 최신 보안취약점 발생 여부를 지속적으로 파악하고, 정보시스템에 미치는 영향을 분석하여 조치하고 있는가

최신 보안취약점 지속 파악

① 최신 보안취약점 파악 및 정보시스템 영향도 분석

	※ 출처: SK쉴더스 최신동향 전파 (SK쉴더스) **◇ 취약점 점검 이력을 기록·관리하여 전년도에 도출된 취약점이 재발생하는 등의 문제점에 대하여 보호 대책을 마련하고 있는가?** **전년도 도출 취약점 원인 분석 및 대응** ① 취약점 점검 이력에 대한 기록관리 ② 취약점 점검 시 지난 취약점 점검결과와 비교 분석하여 취약점 재발 여부 확인 ③ 유사한 취약점이 재발되고 있는 경우 근본원인 분석 및 재발방지 대책 마련

2.11.3 이상행위 분석 및 모니터링

세부분야	2.11.3 이상행위 분석 및 모니터링
인증 기준	내·외부에 의한 침해시도, 개인정보 유출 시도, 부정행위 등을 신속하게 탐지·대응할 수 있도록 네트워크 및 데이터 흐름 등을 수집하여 분석하며, 모니터링 및 점검 결과에 따른 사후 조치는 적시에 이루어져야 한다.
주요 확인사항	• 내·외부에 의한 침해시도, 개인정보 유출 시도, 부정행위 등 이상행위를 탐지할 수 있도록 주요 정보시스템, 응용프로그램, 네트워크, 보안시스템 등에서 발생한 네트워크 트래픽, 데이터 흐름, 이벤트 로그 등을 수집하여 분석 및 모니터링하고 있는가? • 침해시도, 개인정보 유출시도, 부정행위 등의 여부를 판단하기 위한 기준 및 임계치를 정의하고 이에 따라 이상행위의 판단 및 조사 등 후속 조치가 적시에 이루어지고 있는가?
기준 요약도	
운영 방안	**◇ 내·외부에 의한 침해시도, 개인정보 유출 시도, 부정행위 등 이상행위를 탐지할**

수 있도록 주요 정보시스템, 응용프로그램, 네트워크, 보안시스템 등에서 발생한 네트워크 트래픽, 데이터 흐름, 이벤트 로그 등을 수집하여 분석 및 모니터링하고 있는가?

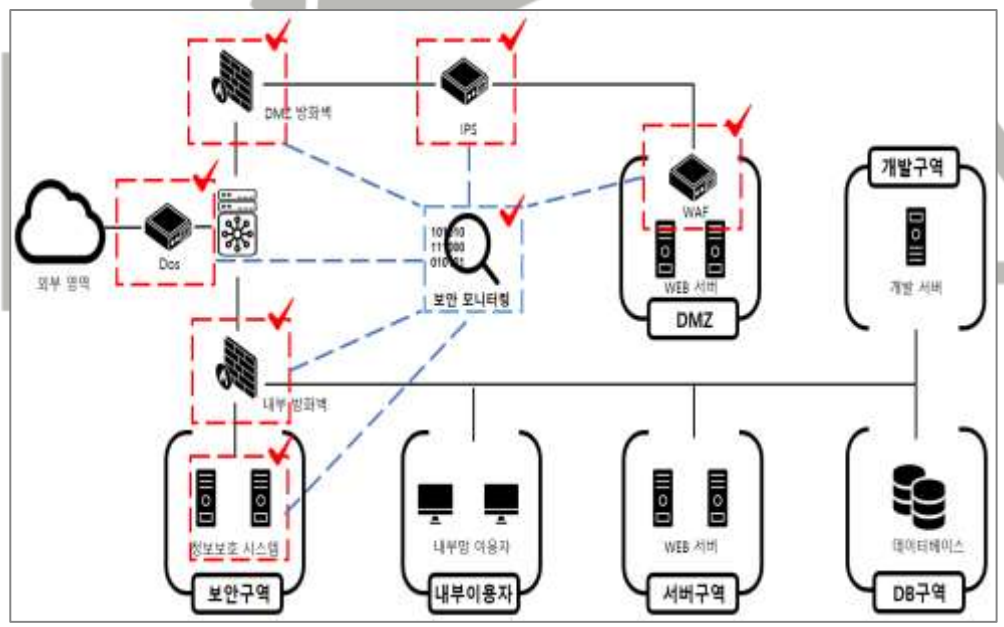
(예시) 침해시도 모니터링 절차 및 체계 구축

「**접근통제 관리지침**」 제 ○○조 (침해사고 모니터링)

① 정보보호관리자는 보안사고를 예방하기 위해 사전 모니터링 및 탐지·대응 체계를 다음 각 호에 맞춰 운영·관리 한다.

1. 대상 및 범위
2. 수집 및 분석, 모니터링 방법

- 자동으로 생성되는 정보를 각 호의 수집 이용하여 보안 모니터링을 실시한다.
  - · 사이버공격 공격 의심 패킷
  - · 공격지 및 피해 의심지 IP 주소, MAC주소, 전자우편, 계정정보 등 식별가능정보
  - · 그 밖에 사이버공격 의심 및 피해 확인에 필요한 정보
- 담당자 및 책임자 지정 등
- 분석 및 모니터링 결과보고
- 이상행위 발생 시 대응 절차



※ 정보보호 시스템운영관리 (이해를 돕기 위한 예시)

◇ 침해시도, 개인정보 유출시도, 부정행위 등의 여부를 판단하기 위한 기준 및 임계치를 정의하고 이에 따라 이상행위의 판단 및 조사 등 후속 조치가 적시에 이루어지고 있는가?

	판단기준 정의 및 후속 조치 ① 사전 정의된 규칙 1. 퇴사자/휴직자 계정 사용, 해외접근 IP 탐지 등 확실한 비정상 동작에 대한 규칙 기반 탐지 2. 미리 정의된 Rule에 매칭되는 침입 판단 3. 이미 정립된 공격 패턴과의 비교를 통한 탐지 ② 행동 기반 탐지 1. 사용자 행위 패턴 분석 2. 특정 사용자의 평소 패턴(근무시간, 사내 네트워크 접근)과 다른 행위 탐지 3. 기계학습 기반 정상 범주 설정 후 이상 행위 탐지 4. 사용자 계정 또는 접속 디바이스별 로그인 시간, 접근 위치, 데이터 조회 빈도 분석 ⑥ 모니터링 체계 구축 1. 조직 규모 및 정보시스템 중요도가 높은 경우 24시간 실시간 모니터링 체계 구축 2. 24×365 모니터링 체계 수립(가상자산 취급업소 등 연중무휴 운영 조직) 3. 실시간 알람을 통한 사고 방지 체계 구축

2.11.4 사고 대응 훈련 및 개선

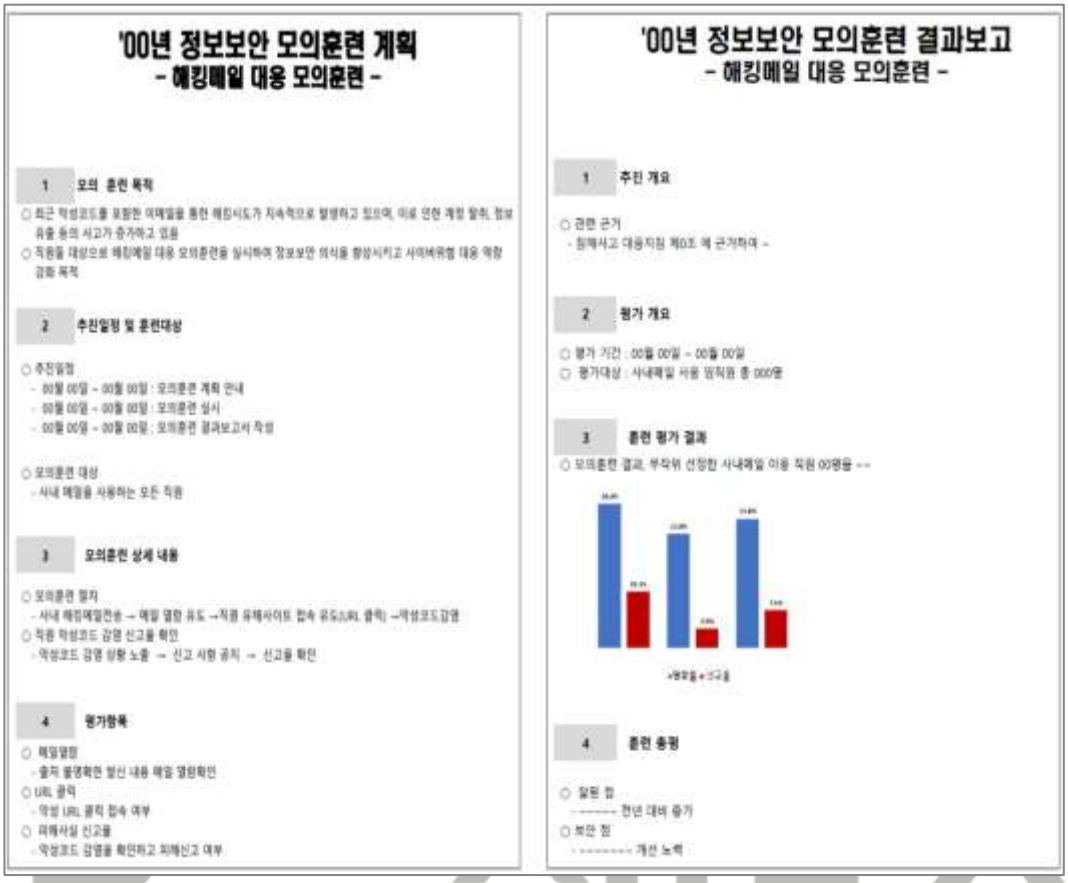
세부분야	2.11.4 사고 대응 훈련 및 개선
인증 기준	침해사고 및 개인정보 유출사고 대응 절차를 임직원과 이해관계자가 숙지하도록 시나리오에 따른 모의훈련을 연 1회 이상 실시하고 훈련결과를 반영하여 대응체계를 개선하여야 한다
주요 확인사항	• 침해사고 및 개인정보 유출사고 대응 절차에 관한 모의훈련 계획을 수립하고 이에 따라 연 1회 이상 주기적으로 훈련을 실시하고 있는가? • 침해사고 및 개인정보 유출사고 훈련 결과를 반영하여 침해사고 및 개인정보 유출사고 대응체계를 개선하고 있는가?
기준 요약도	
운영 방안	**◇ 침해사고 및 개인정보 유출사고 대응 절차에 관한 모의훈련 계획을 수립하고 이에 따라 연 1회 이상 주기적으로 훈련을 실시하고 있는가?** **(예시) 침해사고 대응 모의훈련 계획 수립** 「**침해사고 관리지침**」 제 ○○조 (침해사고 대응 훈련) ① 침해사고 대응 절차에 관한 연 1회 이상 모의훈련 계획을 수립하고 이에 따라 주기적으로 훈련 실시 및 적정성과 효과성을 평가해야 한다.

① 침해사고 대응 훈련 계획 배경 및 근거

② 훈련 대상 및 내용

③ 평가 항목 및 세부 평가 내용

④ 추진 일정 등



00년 정보보안 모의훈련 계획

구분	직위	성명	일자	서명
승인	정보보호 최고책임자	OOO	2023-01-01	승인
상신	정보보호 담당자	OOO	2022-12-20	-

00년 정보보안 모의훈련 결과보고

구분	직위	성명	일자	서명
승인	정보보호 최고책임자	OOO	2023-01-01	승인
상신	정보보호 담당자	OOO	2022-12-20	-

※ 정보보안 모의훈련 보고 (이해를 돕기 위한 예시)

◇ 침해사고 및 개인정보 유출사고 훈련 결과를 반영하여 침해사고 및 개인정보 유출사고 대응체계를 개선하고 있는가?

	침해사고 훈련결과 반영 침해사고 대응체계 개선 ① 모의훈련 시행 후 결과보고서 작성 및 내부 보고 ② 모의훈련 결과를 바탕으로 개선사항을 도출하여 필요시 대응 절차에 반영

2.11.5 사고 대응 및 복구

세부분야	2.11.5 사고 대응 및 복구
인증 기준	침해사고 및 개인정보 유출 징후나 발생을 인지한 때에는 법적 통지 및 신고 의무를 준수하여야 하며, 절차에 따라 신속하게 대응 및 복구하고 사고분석 후 재발방지 대책을 수립하여 대응체계에 반영하여야 한다.
주요 확인사항	• 침해사고 및 개인정보 유출의 징후 또는 발생을 인지한 경우 정의된 침해사고 대응 절차에 따라 신속하게 대응 및 보고가 이루어지고 있는가? • 개인정보 침해사고 발생 시 관련 법령에 따라 정보주체(이용자) 통지 및 관계기관 신고 절차를 이행하고 있는가? • 침해사고가 종결된 후 사고의 원인을 분석하여 그 결과를 보고하고 관련 조직 및 인력과 공유하고 있는가? • 침해사고 분석을 통하여 얻은 정보를 활용하여 유사 사고가 재발하지 않도록 대책을 수립하고 필요한 경우 침해사고 대응 절차 등을 변경하고 있는가?
기준 요약도	
운영 방안	**◇ 침해사고 및 개인정보 유출의 징후 또는 발생을 인지한 경우 정의된 침해사고 대응 절차에 따라 신속하게 대응 및 보고가 이루어지고 있는가?** **(예시) 침해사고 대응 절차 수립**

「침해사고 대응매뉴얼」

① 정보시스템별 담당자는 침해사고 유형별 절차에 따라 대응한다.

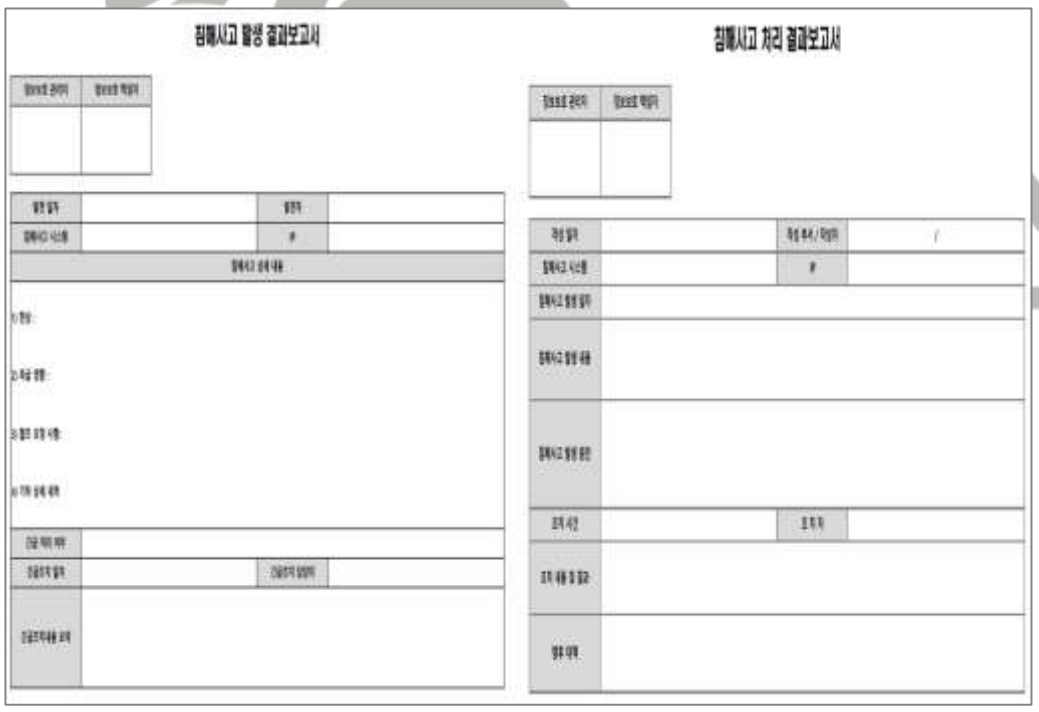
1. 서버의 네트워크 분리, 공격 포트 차단 등 응급조치
2. 사내 업무 전체 영향을 미치는 경우 업무 시간 종료 후 서비스 중단
3. 사내 일부 시스템에 영향을 미치는 경우 업무부서 협의 후 즉시 중단
4. 응급조치 후 정보보호 침해사고 원인 분석 및 증거자료 확보
5. 재발방지 대책 수립 및 이행

(예시) 침해사고 대응 결과 보고서 작성

「침해사고 대응매뉴얼」

① 정보시스템별 담당자는 접수된 신고에 대해 조치가 완료될 때 까지의 모든 기록을 유지 및 관리해야 하며, 침해사고 발생 및 처리 결과보고서를 작성하여 정보보호 최고책임자에게 보고한다. 보고 시 다음 각 호의 사항을 포함해야 한다.

1. 침해사고 발생 유형 및 날짜
2. 피해 범위 및 정도
3. 침해사고 발생원인
4. 대응조치 및 수립된 보안대책



※ 침해사고 발생 결과보고서 (이해를 돕기 위한 예시)

◇ 개인정보 침해사고 발생 시 관련 법령에 따라 정보주체(이용자) 통지 및 관계기관 신고 절차를 이행하고 있는가?

개인정보 침해사고 발생 시 정보주체(이용자) 통지 절차

① 통지 대상 및 기준

1. 통지 대상: 개인정보가 분실·도난·유출된 모든 정보주체에게 개별적으로 통지

2. 통지 시기: 개인정보 유출 등 사실을 알게 된 때로부터 72시간 이내에 정보주체에게 통지. 정당한 사유가 없다면 지체 없이 즉시 통지하는 것이 원칙.

3. 통지 내용 (필수 5가지 항목. 개인정보보호법 제34조 제1항 기준)

- 유출등이 된 개인정보의 항목 (예: 이름, 이메일 주소, 휴대폰 번호 등 구체적으로 명시)
- 유출등이 된 시점과 그 경위 (언제, 어떤 원인으로 유출되었는지)
- 유출등으로 인하여 발생할 수 있는 피해를 최소화하기 위한 정보주체의 조치 방법 (예: 비밀번호 변경, 명의도용 방지 서비스 신청 등)
- 개인정보처리자의 대응조치 및 피해 구제절차
- 피해 발생시 신고 등을 접수할 수 있는 담당부서 및 연락처

② 통지 방법 및 예외사항

1. 통지 방법: 개인별 직접 통지가 원칙이며, 전화, 문자, 이메일, 서면 등을 활용한 개별 통지 필요.

2. 통지 갈음 조치: 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치(홈페이지 게시 등)를 취할 수 있음

구분	개인정보처리자	정보통신서비스 제공자
신고 대상 건수	1천 명 이상 정보주체에 관한 개인정보 유출 시	유출 건수와 무관
신고 시점	지체 없이(72시간 이내)	정당한 사유가 없는 한 그 사실을 안 때부터 24시간 이내
신고 기관	개인정보보호위원회 또는 KISA	

※ 개인정보 유출 신고 기준

개인정보 침해사고 발생 시 관계기관 신고 절차

① 신고 기준

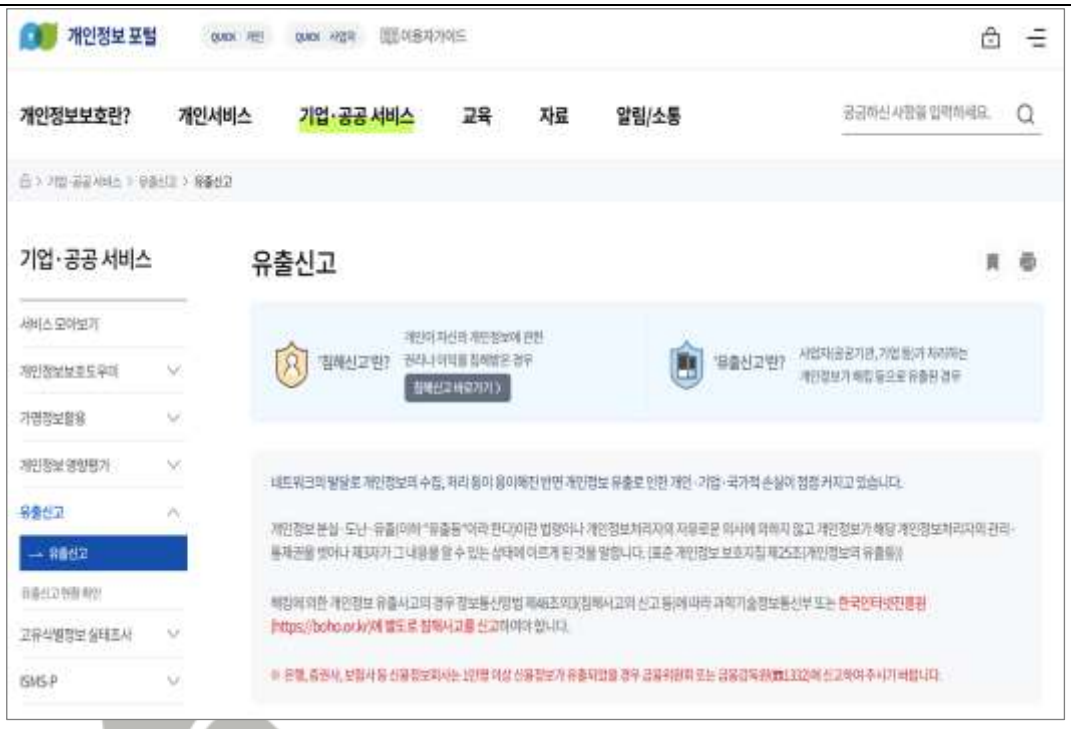
1. 1,000명 이상의 정보주체에 관한 개인정보가 유출등이 된 경우

2. 민감정보 또는 고유식별정보가 유출등이 된 경우 (단 1명이라도 해당)

3. 외부로부터의 불법적인 접근에 의해 개인정보가 유출등이 된 경우

② 신고 시기 및 방법

	1. 신고 시기: 신고 기준에 해당하는 유출등 사실을 알게 된 때부터 72시간 이내 2. 신고 방법: 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법으로 신고 ③ 신고 기관 1. 주요 신고 기관: - 개인정보보호위원회 또는 한국인터넷진흥원(KISA) · 개인정보보호 포털: www.privacy.go.kr · 한국인터넷진흥원: privacy.kisa.or.kr - 은행, 증권사, 보험사 등 신용정보회사는 1만명 이상 신용정보가 유출되었을 경우 금융위원회 또는 금융감독원 ④ 신고 내용 1. 정보주체에의 통지 여부 2. 유출등이 된 개인정보의 항목 및 규모 3. 유출등이 된 시점과 그 경위 4. 유출등에 따른 피해 최소화 대책·조치 및 결과 5. 정보주체가 할 수 있는 피해 최소화 방법 및 구제절차 6. 담당부서·담당자 및 연락처 ⑤ 신고 예외사항 및 우선신고 1. 천재지변이나 그 밖의 부득이한 사유로 72시간 내 신고가 곤란한 경우 (사유 해소 후 지체 없이 신고) 2. 개인정보 유출등의 경로가 확인되어 해당 개인정보를 회수·삭제하는 등의 조치를 통해 정보주체의 권익 침해 가능성이 현저히 낮아진 경우 3. 구체적인 내용을 확인하지 못한 경우에는 우선신고 후 추가신고 가능



※ 출처: 개인정보 포털 유출신고 (개인정보보호위원회)

◇ 침해사고가 종결된 후 사고의 원인을 분석하여 그 결과를 보고하고 관련 조직 및 인력과 공유하고 있는가?

침해사고 원인 분석 및 공유

① 침해사고가 종결된 후 사고 원인을 분석하여 그 결과를 보고하고 관련 조직 및 인력과 공유

② 침해사고가 처리되고 종결된 후 이에 대한 사고 원인에 대한 분석을 수행하고 결과보고서를 작성하여 책임자에게 보고

③ 침해사고 정보와 발견된 취약점 및 원인, 조치 방안 등을 관련 조직 및 인력에게 공유

침해사고 대응 결과보고서

사고번호			발생일시		
			조치완료일		
탐지 내용					
작업내용					
탐지 방법		탐지포트		탐지건수	
탐지 로그				감염 IP	
출발지 IP		출발지포트		목적지 IP	목적지 포트

※ 침해사고 대응 결과보고서 (이해를 돕기 위한 예시)

◇ 침해사고 분석을 통하여 얻은 정보를 활용하여 유사 사고가 재발하지 않도록 대책을 수립하고 필요한 경우 침해사고 대응 절차 등을 변경하고 있는가?

침해사고 재발방지 대책 수립

① 침해사고 분석을 통하여 얻은 정보를 활용하여 유사 사고가 반복되지 않도록 하는 재발방지 대책 수립

② 분석된 결과에 따라 필요한 경우 침해사고 대응 절차, 정보보호 정책 및 절차 등 침해사고 대응체계에 대한 변경 수행

2.12 재해 복구

2.12.1 재해·재난 대비 안전조치

세부분야	2.12.1 재해·재난 대비 안전조치
인증 기준	자연재해, 통신·전력 장애, 해킹 등 조직의 핵심 서비스 및 시스템의 운영 연속성을 위협할 수 있는 재해 유형을 식별하고, 유형별 예상 피해규모 및 영향을 분석하여야 한다. 또한 복구 목표시간, 복구 목표시점을 정의하고 복구 전략 및 대책, 비상시 복구 조직, 비상연락체계, 복구 절차 등 재해 복구체계를 구축하여야 한다.
주요 확인사항	• 조직의 핵심 서비스(업무) 연속성을 위협할 수 있는 IT 재해 유형을 식별하고, 유형별 피해규모 및 업무에 미치는 영향을 분석하여 핵심 IT 서비스(업무) 및 시스템을 식별하고 있는가? • 핵심 IT 서비스 및 시스템의 중요도 및 특성에 따른 복구 목표시간, 복구 목표 시점을 정의하고 있는가? • 재해·재난 발생 시에도 핵심 서비스 및 시스템의 연속성을 보장할 수 있도록 복구 전략 및 대책, 비상시 복구 조직, 비상연락체계, 복구 절차 등 재해 복구 계획을 수립·이행하고 있는가?
기준 요약도	
운영 방안	**◇ 조직의 핵심 서비스(업무) 연속성을 위협할 수 있는 IT 재해 유형을 식별하고, 유형별 피해규모 및 업무에 미치는 영향을 분석하여 핵심 IT 서비스(업무) 및 시스템을 식별하고 있는가?** **IT 재해 유형 식별** ① 자연재해: 화재, 홍수, 지진, 태풍 등

② 외부 요인: 해킹, 통신장애, 정전 등

③ 내부 요인: 시스템 결함, 기계적 오류, 사용자 실수, 의도적·악의적 운영, 핵심 운영자 근무 이탈, 환경설정 오류 등

피해규모 및 업무영향도 분석

① 핵심 서비스 도출

1. 전사 서비스 목록화 → 제공 고객·거래 수, 매출 비중, 법적·규제 요구사항 기반 우선순위 지정

② 피해 규모 산정

1. 서비스 중단 시 일별 매출 손실, SLA 위반 비용, 고객 이탈률, 평판 하락 비용 계량

③ 업무 영향 분석

1. 정성적(고객 민원, 규제 제재, 브랜드 신뢰도 하락 등) 분석
2. 정량적(금전 손실, 법적 벌금 등) 분석

◇ 핵심 IT 서비스 및 시스템의 중요도 및 특성에 따른 복구 목표시간, 복구 목표시점을 정의하고 있는가?

핵심 IT 서비스 및 시스템 식별

① 주요 업무별 프로세스 식별

1. 조직의 핵심적 고객서비스
2. 조직 전략 측면에서의 중요 업무

② 업무 프로세스간 상호연관성 분석

1. 선후관계: 후행 프로세스의 수행을 위해서는 선행 프로세스가 반드시 수행
2. 참조관계: 수행 결과를 참조해야만 하는 두 프로세스

※ 시스템 중요도 산정 (이해를 돕기 위한 예시)

정보시스템 복구목표 시간결정

① 정보시스템 업무 중요도에 따라 복구시간 지정

1. RTO: 복구목표 시간

2. RPO: 복구목표 시점

※ RTO·RPO 산정 (이해를 돕기 위한 예시)

◇ 재해·재난 발생 시에도 핵심 서비스 및 시스템의 연속성을 보장할 수 있도록 복구 전략 및 대책, 비상시 복구 조직, 비상연락체계, 복구 절차 등 재해 복구 계획을 수립·이행하고 있는가?

(예시) 재해복구계획 수립

① 복구 전략 및 대책

1. 이중화 구축: 주요 서버는 Active–Standby(passive) 이중화, 스토리지는 실시간 복제

2. DR 센터 활용: 물리적/지리적 분리된 2차 데이터센터에 정기 동기화

3. 클라우드 백업: 중요 데이터는 매시간 증분 백업 및 주간 전체 백업

② 비상 복구 조직

1. DR 총괄 책임자: 정보보호최고책임자(CISO)

2. 기술복구: 서버·네트워크·DB 관리자

3. 지원/운영: 애플리케이션, 보안, 커뮤니케이션 담당자

③ 비상 연락체계

1. 자동 알림: 장애 감지 시 SMS·메일·메신저로 전원 통보

2. 연락망: 이름·직위·휴대폰·이메일을 포함한 연락 리스트 유지

④ 단계별 복구 절차

1. 발견 및 보고: 모니터링 경보 → 관련 담당자 보

2. 초기 평가: 영향 범위·우선순위 결정 → RTO/RPO 검토

3. 격리 및 전환: 장애 시스템 격리 → DR 센터 전환

	4. 데이터 복원: 백업환경에서 복원 후 무결성 검사 5. 서비스 검증: 기능·성능 테스트 → 운영 환경 복귀 6. 사후 평가: 복구 결과 보고 및 개선점 도출 7. 결과 보고서: RTO/RPO 달성률, 절차 준수 여부, 개선 이행 계획 작성 ⑤ 정기 연습 및 검토 1. 주기적 재해복구 대상 검토 2. 주기적 실제 복구 테스트

2.12.2 재해 복구 시험 및 개선

세부분야	2.12.2 재해 복구 시험 및 개선
인증 기준	재해 복구 전략 및 대책의 적정성을 정기적으로 시험하여 시험결과, 정보시스템 환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완하여야 한다
주요 확인사항	• 수립된 IT 재해 복구체계의 실효성을 판단하기 위하여 재해 복구 시험 계획을 수립·이행하고 있는가? • 시험결과, 정보시스템 환경변화, 법률 등에 따른 변화를 반영할 수 있도록 복구전략 및 대책을 정기적으로 검토·보완하고 있는가?
기준 요약도	
운영 방안	**◇ 수립된 IT 재해 복구체계의 실효성을 판단하기 위하여 재해 복구 시험 계획을 수립·이행하고 있는가?** **재해복구 시험 계획 수립·이행** **「서비스 연속성관리지침」** 제 ○○조 (재해복구 모의훈련) ① IT 재해복구 시험 계획에 따라 모의훈련을 해야 하며, 모의훈련은 문서에 의거하여 실시한 테스트, 특정 업무를 표본으로 모의 테스트를 실시한다. ② 모의훈련 실시 후 훈련에 참여한 구성원은 모의훈련 실시결과를 평가하고 정보보호 책임자는 훈련결과를 정보보호최고책임자(CISO)에게 보고해야 한다.

00년 IT재해 복구 시험 계획

구분	직위	성명	일자	서명
승인	정보보호 최고책임자	OOO	2023-01-01	승인
상신	정보보호 담당자	OOO	2022-12-20	-

00년 IT 재해 복구 시험결과

구분	직위	성명	일자	서명
승인	정보보호 최고책임자	OOO	2023-01-01	승인
상신	정보보호 담당자	OOO	2022-12-20	-

※ IT재해복구 시험 계획 (이해를 돕기 위한 예시)

◇ 시험결과, 정보시스템 환경변화, 법률 등에 따른 변화를 반영할 수 있도록 복구전략 및 대책을 정기적으로 검토·보완하고 있는가?

재해복구 테스트 정기적 검토

① 현황 수집

1. 최근 복구 훈련 결과 보고서, 장애 로그·모니터링 데이터, 법령 개정 목록 수집
2. 신규 인프라·서비스 도입 현황 파악

② 갭 분석

1. 목표 RTO/RPO 대비 실제 복구 성능 차이
2. 환경 변화로 인한 시나리오 누락·절차 불일치 여부

3. 법·규제 요구사항 미반영 항목

③ 개선 계획 수립

1. 우선순위: 비즈니스 영향도, 법적 컴플라이언스, 기술 리스크 기준

2. 조치 항목별 담당자·이행 일정·완료 기준 정의

④ 승인 및 공지

1. 정보보호최고책임자 및 경영진 승인

2. 공유: 절차 변경 사항, 담당자 역할, 교육 일정 안내

⑤ 이행 모니터링

1. 개선 항목 완료 여부 추적 관리

2. 다음 검토 시까지 조치 내역 이행 검증

※ IT재해복구 시험 계획 및 결과 (이해를 돕기 위한 예시)

3. 개인정보 처리 단계별 요구사항

3.1 개인정보 수집 시 보호조치

3.1.1 개인정보 수집·이용

세부분야	3.1.1 개인정보 수집·이용
인증 기준	개인정보는 적법하고 정당하게 수집·이용하여야 하며, 정보주체의 동의를 근거로 수집하는 경우에는 적법한 방법으로 정보주체의 동의를 받아야 한다. 또한 만 14세 미만 아동의 개인정보를 수집하는 경우에는 그 법정대리인의 동의를 받아야 하며 법정대리인이 동의하였는지를 확인하여야 한다.
주요 확인사항	• 개인정보를 수집하는 경우 정보주체 동의, 법령상 의무준수, 계약 체결·이행 등 적법 요건에 따라 수집하고 있는가? • 정보주체에게 개인정보 수집 동의를 받는 경우 동의방법 및 시점은 적절하게 되어 있는가? • 정보주체에게 동의를 서면(전자문서 포함)으로 받는 경우 법령에서 정한 중요한 내용에 대하여 명확히 표시하여 알아보기 쉽게 표시하고 있는가? • 만 14세 미만 아동의 개인정보에 대하여 수집·이용·제공 등의 동의를 받는 경우 법정대리인에게 필요한 사항에 대하여 고지하고 동의를 받고 있는가? • 법정대리인의 동의를 받기 위하여 필요한 최소한의 개인정보만을 수집하고 있으며, 법정대리인이 자격 요건을 갖추고 있는지 확인하는 절차와 방법을 마련하고 있는가? • 만 14세 미만의 아동에게 개인정보 처리와 관련한 사항 등의 고지 시 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어로 표현하고 있는가? • 정보주체 및 법정대리인에게 동의를 받은 기록을 보관하고 있는가? • 정보주체의 동의 없이 처리할 수 있는 개인정보에 대해서는 그 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 개인정보처리방침에 공개하거나 정보주체에게 알리고 있는가? • 정보주체의 동의 없이 개인정보의 추가적인 이용 시 당초 수집 목적과의 관련성, 예측 가능성, 이익 침해 여부, 안전성 확보조치 등의 고려사항에 대한 판단기준을 수립·이행하고, 추가적인 이용이 지속적으로 발생하는 경우 고려사항에 대한 판단기준을 개인정보처리방침에 공개하고 이를 점검하고 있는가?

기준 요약도	
운영 방안	**◇ 개인정보를 수집하는 경우 정보주체 동의, 법령상 의무준수, 계약 체결·이행 등 적법 요건에 따라 수집하고 있는가?** **개인정보의 수집·이용 시 적법 요건** ① 정보주체 동의 확보 1. 수집 목적·항목·보관 기간·이용·제3자 제공 범위 명시 2. 별도 동의서 또는 체크박스 방식으로 명확·자유의사 동의 취득 3. 동의 철회 절차 안내 및 기록 보관 ② 법령상 의무 준수 1. 개인정보보호법, 위치정보법, 신용정보법 등 관련 법규별 수집 근거 검토 2. 법률에 근거한 수집 항목·수단·절차 준수 3. 고유식별정보·민감정보 수집 시 별도 의무 이행 ③ 계약 체결·이행 목적 시 이용 1. 서비스 제공·계약 이행에 필수적 최소 정보만 수집 2. 계약서·개인정보처리방침 등에 관련 근거 및 범위 명시 - 고객 문의·정산·배송 등 계약 이행 목적 외 사용 제한 ④ 최소 수집·목적 외 사용 금지 1. 필요한 최소한의 항목만 수집 2. 당초 명시된 목적 외 개인정보 처리 금지

3. 신규 목적 발생 시 사전 고지·동의 절차 이행

개인정보의 수집·이용 동의 시 고지 사항

① 개인정보의 수집·이용 목적

② 수집하려는 개인정보의 항목

③ 개인정보의 보유 및 이용기간

④ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

※ 출처: SK쉴더스 홈페이지 가입상담화면 (SK쉴더스)

※ 출처: SK쉴더스 홈페이지 가입상담화면(필수동의 상세) (SK쉴더스)

◇ 정보주체에게 개인정보 수집 동의를 받는 경우 동의 방법 및 시점은 적절하게 되어 있는가?

개인정보 수집 동의 방법 및 시점

① 동의 방식

1. 명시적·능동적 동의: 수집 목적·항목·보유기간 등 핵심정보를 체크박스 또는 서명으로 별도 표시하고, 미체크 시 수집되지 않도록 구현

2. 필수/선택 동의 구분: 필수동의(서비스 제공) 항목과 선택동의(마케팅 등) 항목을 분리하여 개별 동의 확보

3. 온/오프라인 동의: 오프라인은 서면 동의서, 온라인은 팝업 또는 전용 화면에 동의 절차 구현

② 동의 시점

1. 개인정보 최초 수집: 서비스 회원가입, 앱 설치, 설문 시작 등 데이터 입력 전에 동의내용을 명확히 제시

2. 목적 및 처리내용 변경 시: 기존 동의 범위를 벗어난 처리 목적 발생 시 재동의

3. 최초 동의 후 사후 제공되는 서비스: 해당 서비스 제공시점에 동의

- 다만, 반복적인 서비스의 경우로서 최초 서비스 이용 시점에 선택 동의 항목으로 분류하여 동의를 받는 경우에는 수집·이용 가능

◇ 정보주체에게 동의를 서면(전자문서 포함)으로 받는 경우 법령에서 정한 중요한 내용에 대하여 명확히 표시하여 알아보기 쉽게 표시하고 있는가?

동의서 작성 시 중요내용을 명확히 표시

① 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실

② 개인정보 항목 중 민감정보, 고유식별정보

③ 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간)

④ 제공받는 자와 제공받는 자의 개인정보 이용 목적

1. 글씨의 크기, 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 할 것

작성 예시

■ 개인정보 수집·이용 내역

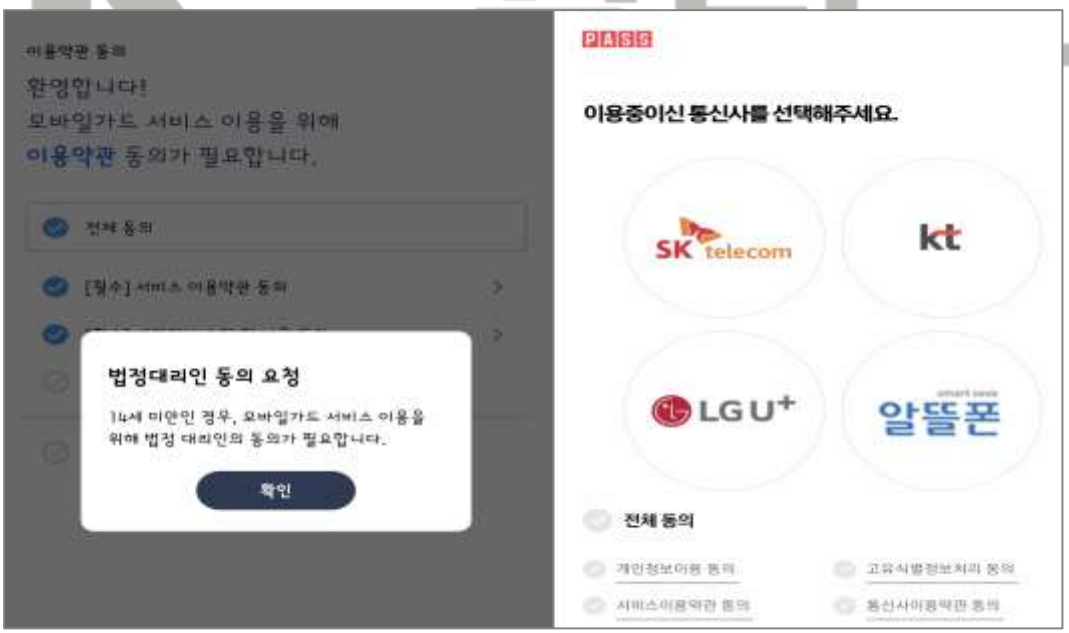
항 목	수집·이용 목적	보유·이용기간
성명, 전화번호	홍보문자 발송	1년

※ 출처: 알기쉬운 개인정보 처리 동의 안내서 (개인정보보호위원회)

◇ 만 14세 미만 아동의 개인정보에 대하여 수집·이용·제공 등의 동의를 받는 경우 법정대리인에게 필요한 사항에 대하여 고지하고 동의를 받고 있는가?

개인정보 수집 시 만 14세 확인절차 필요

① 인터넷 등 비대면 회원가입 시, 만 14세 미만 여부는 정보주체가 "법정 생년월일"을 직접 입력하거나 "만 14세 이상" 항목에 스스로 체크하는 방법으로 확인하는 것이 바람직함.



※ 출처: SK쉴더스 모바일가드 스마트폰 앱(SK쉴더스)

※ 출처: 알기쉬운 개인정보 처리 동의 안내서 (개인정보보호위원회)

◇ 법정대리인의 동의를 받기 위하여 필요한 최소한의 개인정보만을 수집하고 있으며, 법정대리인이 자격 요건을 갖추고 있는지 확인하는 절차와 방법을 마련하고 있는가?

법정대리인 진위확인 및 수집·이용·제공 동의 절차

① 동의 목적 달성에 필요한 최소 정보만 수집

1. 최소 정보: 이름, 생년월일, 법정대리인 성명
2. 확인용 정보: 법정대리인 연락처(휴대전화), 관계(부모·후견인 등)
3. 아동으로부터 수집한 법정대리인의 개인정보는 동의를 얻기 위한 용도로만 활용

② 법정대리인의 성명·연락처 수집 시 절차

1. 해당 아동에게 자신의 신분과 연락처, 법정대리인의 이름과 연락처를 수집하고자 하는 이유를 고지

③ 법정대리인의 진위여부 확인

1. 법정대리인의 미성년자 여부 확인
2. 아동과의 나이 차이 확인 등

④ 법정대리인 동의 거부 혹은 동의 의사 미확인 시

1. 수집일로부터 5일 이내 파기

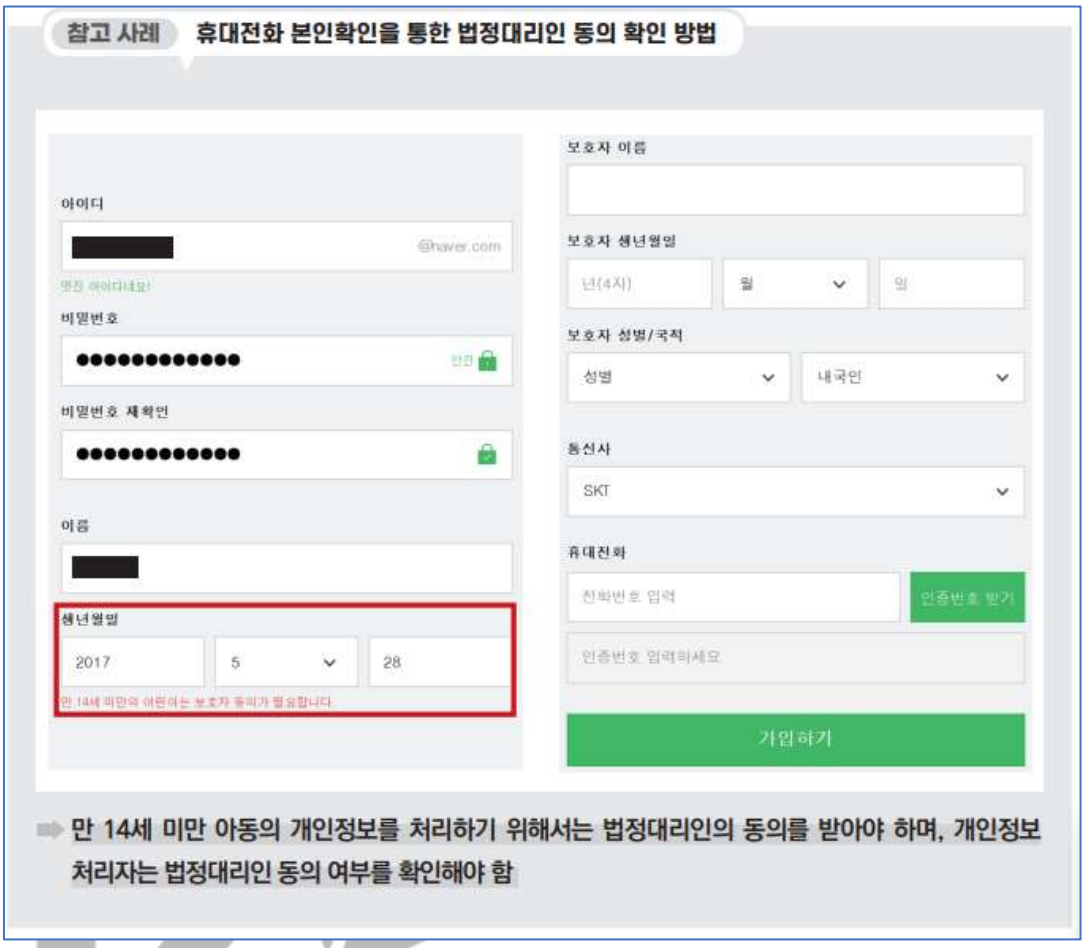
법정대리인 동의 절차

① 전자서명

② 휴대폰 인증, 아이핀 등을 통하여 본인확인 후 명시적으로 동의

③ 우편, 팩스, 전자우편 등으로 법정대리인이 서명 날인한 서류를 제출

④ 법정대리인과 직접 통화하여 확인하는 방법 등



※ 출처: 아동청소년 개인정보 보호 가이드라인 (개인정보보호위원회)

◇ 만 14세 미만의 아동에게 개인정보 처리와 관련한 사항 등의 고지 시 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어로 표현하고 있는가?

만 14세 미만 아동이 이해하기 쉬운 언어로 표현

「**개인정보보호법**」 제22조의 2(아동의 개인정보 보호)

③ 개인정보처리자는 만 14세 미만의 아동에게 개인정보 처리와 관련한 사항의 고지 등을 할 때에는 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어를 사용하여야 한다.

◇ 정보주체 및 법정대리인에게 동의를 받은 기록을 보관하고 있는가?

(예시) 동의기록 보관 기준

① 보관 대상

1. 정보주체 동의 내역: 개인정보 수집·이용·제3자 제공 동의
2. 법정대리인 동의 내역: 아동·청소년 개인정보 처리 동의

3. 동의 철회 내역: 철회 시점 및 방법

② 보관 항목

1. 동의 일시
2. 동의 방법: 웹, 앱, 서면, 전화 등)
3. 동의자 정보: 법정대리인이 동의한 경우 법정대리인 정보 포함
4. 동의 항목

③ 보관 방식

1. 전자적 기록: DB 테이블 및 로그 시스템
2. 문서 기록: 오프라인 서면 동의서는 스캔 후 전자문서화, 원본 별도 보관 등
3. 필요 시 백업 관리: 주간 증분 백업·월간 전체 백업 수행

④ 보관 기간

1. 동의 철회 또는 계약 종료 후 즉시 파기
2. 법정 보관 기간이 법령에 별도 규정된 경우 해당 기간 준수

회원테이블 (예시 속성)

Column Name	Data Type	Constraints	Description
id	INT	PRIMARY KEY, AUTO INCREMENT	고유 식별자
username	VARCHAR(255)	NOT NULL	사용자 이름
email	VARCHAR(255)	NOT NULL, UNIQUE	이메일 주소
password	VARCHAR(255)	NOT NULL	비밀번호
age	INT	NOT NULL	나이
agreement	TINYINT	NOT NULL	선택 동의 여부 (0: 거부, 1: 동의)
method_of_agreement	VARCHAR(255)	NOT NULL	동의 수단
authorized_representative_agreement	TINYINT	NOT NULL	대리인 동의 여부 (0: 거부, 1: 동의)
child_presence	TINYINT	NOT NULL	아동 유무 (0: 없음, 1: 있음)
created_at	DATETIME	NOT NULL	생성일시
updated_at	DATETIME	NOT NULL	업데이트일시

※ 동의기록 보관(이해를 돕기 위한 예시)

◇ 정보주체의 동의 없이 처리할 수 있는 개인정보에 대해서는 그 항목과 처리의 법적 근거를 정보주체의 동의를 받아 처리하는 개인정보와 구분하여 개인정보처리방침에 공개하거나 정보주체에게 알리고 있는가?

법적 근거를 통해 동의없이 처리하는 개인정보 구분

「**개인정보보호법**」 제15조의 제2항 ~ 제7항 (개인정보의 수집·이용)

② 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우

③ 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우

④ 정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우

⑤ 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우

⑥ 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

⑦ 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

개인정보의 처리 및 보유기간

① 개인정보위는 법령에 따른 개인정보 보유·이용기간 또는 정보주체로부터 개인정보 수집 시에 동의받은 개인정보 보유·이용기간 내에서 개인정보를 처리하고 보유합니다.

② 각각의 개인정보 처리 및 보유 기간은 다음과 같습니다.

서비스 명칭	운영근거	수집항목	보유기간
교육서비스 제공 사용자 정보	정보주체 동의	(필수) 성명, 기관명, 직위, 전화번호, 전자우편, 생년월일	2년
개인정보 열람등요구 처리 사용자 정보	개인정보 보호법 제35조~제38조	(필수) 성명, 생년월일, 전화번호, 주소 (선택) 휴대전화번호, 팩스번호, 전자우편	3년
유출사고 신고 처리 사용자 정보	개인정보 보호법 제34조 및 정보통신서비스 제공자의 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제39조	(필수) 성명, 기관명, 전화번호, 전자우편 (선택) 부서, 직위	준영구
개인정보보호 전문감사 명단	정보주체 동의	(필수) 성명, 연락처, 전자우편	위촉 종료 후 2년
가명정보 전문가 명단	정보주체 동의	(필수) 성명, 전자우편, 휴대전화번호 (선택) 소속, 직급(직위)	위촉기간 종료시까지

※ 출처: 개인정보처리방침 법적근거고지 (개인정보 포털)

◇ 정보주체의 동의 없이 개인정보의 추가적인 이용 시 당초 수집 목적과의 관련성, 예측 가능성, 이익 침해 여부, 안전성 확보조치 등의 고려사항에 대한 판단기준을 수립·이행하고, 추가적인 이용이 지속적으로 발생하는 경우 고려사항에 대한 판단기준을 개인정보처리방침에 공개하고 이를 점검하고 있는가?

정보주체의 동의 없이 개인정보를 추가적으로 이용·제공하는 경우 판단기준 수립

① 당초 수집목적과의 관련성

1. 동일한 법적 근거 또는 사업 영역 내에서의 이용
2. 수집 목적과 논리적·기능적 연관성이 인정되는 범위
3. 전혀 다른 목적(예: 회원가입→마케팅)은 관련성 없음

② 예측 가능성

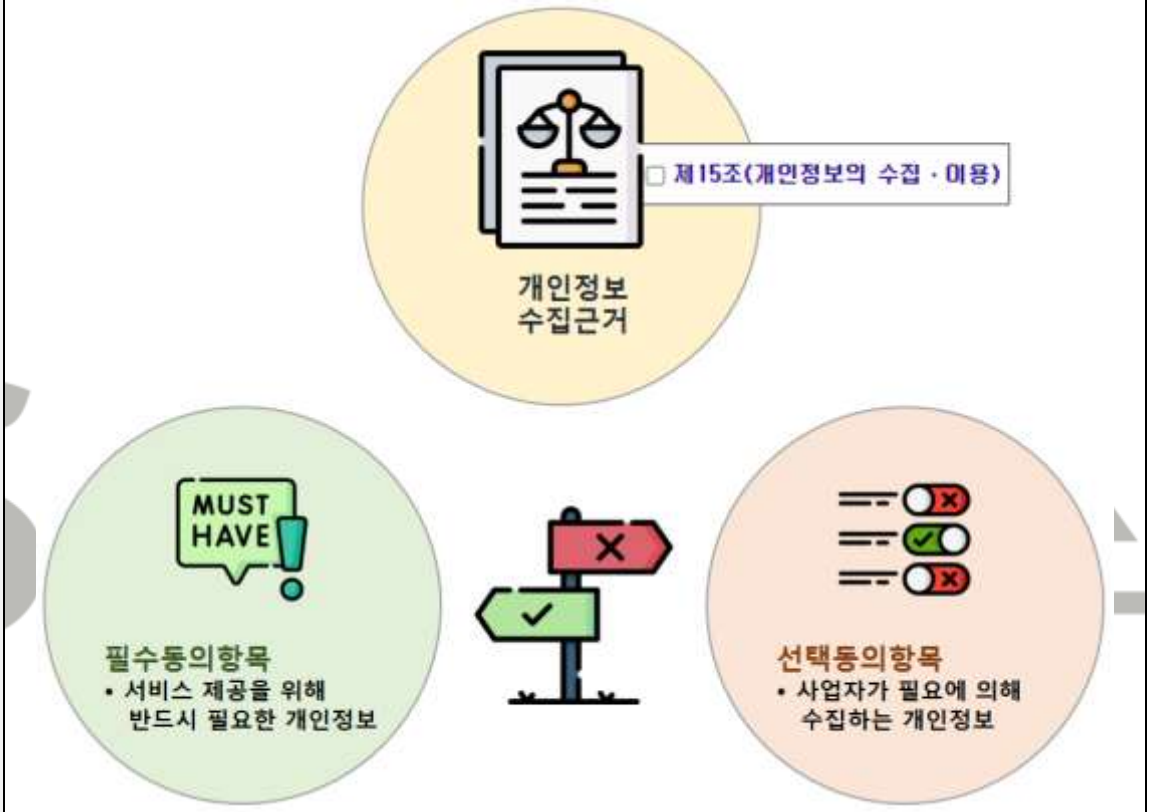
1. 개인정보 수집 시 정보주체가 합리적으로 예상할 수 있는 처리 범위
2. 서비스 이용약관·개인정보처리방침에 명시된 처리내용
3. 동종 업계의 일반적 처리 관행 및 사회통념상 예측 가능한 범위

③ 정보주체 이익 침해 여부

1. 개인정보 민감도·규모 대비 처리 필요성 비교

	2. 정보주체에게 불이익(경제적 손실, 차별, 명예훼손 등) 발생 가능성 3. 처리 목적의 공익성·사회적 가치 고려 ④ 안전성 확보조치 1. 가명처리·암호화·접근권한 제한 등 기술적 보호조치 적용 2. 내부 관리계획·교육·감사 등 관리적 보호조치 이행 3. 개인정보의 안전성 확보조치 기준 등 관련 법 준수 ⑤ 지속적 발생 시 처리방침 공개 1. 추가적 이용·제공이 지속적으로 발생하는 경우 개인정보 처리방침에 판단기준을 공개

3.1.2 개인정보의 수집 제한

세부분야	3.1.2 개인정보 수집 제한
인증 기준	개인정보를 수집하는 경우 처리 목적에 필요한 최소한의 개인정보만을 수집하여야 하며, 정보주체가 선택적으로 동의할 수 있는 사항 등에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하지 않아야 한다.
주요 확인사항	• 개인정보를 수집하는 경우 그 목적에 필요한 범위에서 최소한의 정보만을 수집하고 있는가? • 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 않을 수 있다는 사실을 구체적으로 알리고 있는가? • 정보주체가 수집 목적에 필요한 최소한의 정보 이외의 개인정보 수집에 동의하지 않는다는 이유로 서비스 또는 재화의 제공을 거부하지 않도록 하고 있는가?
기준 요약도	
운영 방안	**◇ 개인정보를 수집하는 경우 그 목적에 필요한 범위에서 최소한의 정보만을 수집하고 있는가?** **최소 수집 원칙에 입각한 개인정보 수집** ① 수집 목적 범위 내 최소한의 정보만 요청 1. 서비스 이용계약 이행에 반드시 필요한 개인정보(예: 회원 식별 정보, 결제 처리 정보)만 수집

2. 추가 기능(마케팅, 설문 등)을 위한 정보는 별도 '선택' 항목으로 분리

② 계약 관련 개인정보는 동의 없이 처리

1. 서비스 가입·계약 이행에 필수적인 개인정보는 정보주체의 동의 없이도 처리

2. 동의 없이 수집·이용하는 개인정보 항목과 근거는 내부 정책 문서 및 개인정보처리방침에 명확히 기록

③ 선택 항목 동의 시 고려사항

1. 계약 이행과 무관한 개인정보 수집 시에는 정보주체가 자유로운 의사로 동의 여부를 결정할 수 있도록 안내

2. 동의 전에 "필수 항목"과 "선택 항목"을 분리하여 설명하고, 선택 항목에 동의하지 않아도 서비스 이용에 불이익이 없음을 명확히 고지

④ 개인정보처리방침 공개

1. 수집·이용하는 개인정보를 "동의 없이 처리" 항목과 "정보주체 동의 필요" 항목으로 구분하여 방침에 명시

2. 각 항목에 대해 처리 근거(계약 이행, 법령 근거 등)를 함께 기재

개인정보 필수동의 관행 개선 주요 내용

① 계약 이행 관련 개인정보

1. 서비스 이용계약 이행에 반드시 필요한 개인정보는 정보주체 동의 없이 수집·이용 가능하며, 이를 처리할 법적 책임은 개인정보처리자가 부담

② 동의 필요 항목 분리 및 자유의사 보장

1. 계약과 무관한 개인정보 수집 시에는 '필수'와 '선택' 항목을 명확히 구분

2. 정보주체가 자유롭게 동의 여부를 결정할 수 있도록 안내

③ 동의 방법에 관한 원칙

1. 동의 내용은 이해하기 쉬운 문구로 제공

2. 동의 화면 또는 서면에 "자유로운 의사에 따른 선택권 보장"을 명시

④ 혼합 수집 시 분리 조치

1. 필수적 개인정보와 선택적 개인정보가 함께 동의받은 경우, 필수적 항목만 남기고 선택적 항목은 별도 동의 절차를 거쳐야 함

⑤ 처리방침 공개

1. 개인정보처리방침에 "동의 없이 처리하는 개인정보"와 "정보주체 동의를 받아 수집하는 개인정보"를 구분하여 기재

2. 각 항목의 처리 근거를 명시

⑥ 민감정보·고유식별정보

1. 서비스 제공 특성상 불가피하게 필요한 경우 별도 필수 동의를 받아 처리

2. 법령 근거가 있을 때는 동의 없이 처리할 수 있음

◇ 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 않을 수 있다는 사실을 구체적으로 알리고 있는가?

필수 동의·선택 동의 상세내용

① 필수 동의: 사업자가 해당 서비스 제공을 위해 반드시 필요한 개인정보에 대해서는 이용자로부터 수집 동의

② 선택 동의: 사업자가 해당 서비스의 추가적 기능 또는 사업자의 필요에 의해 이용자에게 개인정보 수집 동의

※ 출처: SK쉴더스 홈페이지 가입상담화면 (SK쉴더스)

◇ 정보주체가 수집 목적에 필요한 최소한의 정보 이외의 개인정보 수집에 동의하지 않는다는 이유로 서비스 또는 재화의 제공을 거부하지 않도록 하고 있는가?

선택 동의거부로 인한 서비스 제공 거부 금지

① 정보주체가 선택 항목에 대한 동의만 거부하더라도, 필수 기능과 재화 제공

1. 선택 항목 동의 여부와 서비스 이용 권한을 완전 분리
2. 동의 화면에서 "선택"과 "필수"를 구분한 체크박스 배치
3. 동의 거부 시에도 정상적으로 서비스 이용(로그인·구매·문의 기능 등)이 작동하도록 시스템 설계
4. 내부 품질검증 프로세스에 '선택 항목 미동의→정상 서비스 가능 여부' 테스트

3.1.3 주민등록번호 처리 제한

세부분야	3.1.3 주민등록번호 처리 제한
인증 기준	주민등록번호는 법적 근거가 있는 경우를 제외하고는 수집·이용 등 처리할 수 없으며, 주민등록번호의 처리가 허용된 경우라 하더라도 인터넷 홈페이지 등에서 대체수단을 제공하여야 한다.
주요 확인사항	• 주민등록번호는 명확한 법적 근거가 있는 경우에만 처리하고 있는가? • 주민등록번호의 수집 근거가 되는 법 조항을 구체적으로 식별하고 있는가? • 법적 근거에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하고 있는가?
기준 요약도	
운영 방안	**◇ 주민등록번호는 명확한 법적 근거가 있는 경우에만 처리하고 있는가?** **주민등록번호 처리의 제한** 「**개인정보보호법**」 제24조의2 중 1항(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다. 1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우 2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우 3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우

「**정보통신망법**」제23조의2 중 1항(주민등록번호의 사용 제한)

① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다.

1. 제23조의3에 따라 본인확인기관으로 지정받은 경우

3.「전기통신사업법」제38조제1항에 따라 기간통신사업자로부터 이동통신서비스 등을 제공받아 재판매하는 전기통신사업자가 제23조의3에 따라 본인확인기관으로 지정받은 이동통신사업자의 본인확인업무 수행과 관련하여 이용자의 주민등록번호를 수집·이용하는 경우

◇ 주민등록번호의 수집 근거가 되는 법 조항을 구체적으로 식별하고 있는가?

주민등록번호 수집 근거 식별

② 하기 법령 등 주민등록 수집 근거 법 조항을 구체적으로 식별

관련 법령	조항
국세기본법 시행령	제68조(민감정보 및 고유식별정보의 처리)
부가가치세법	제32조(세금계산서 등)
금융실명법 시행령	제4조의2(실명거래의 확인 등)
소득세법	제127조(원천징수의무), 제164조(지급명세서의 제출)
신용정보보호법	제34조(개인식별정보의 수집·이용 및 제공)
전기통신사업법	제32조의4(이동통신단말장치 부정이용 방지 등), 제32조의5(부정가입방지시스템 구축), 제32조의6(명의도용방지서비스의 제공 등), 제83조(통신비밀의 보호)
상기 내용은 관련 법령 중 일부에 해당함	

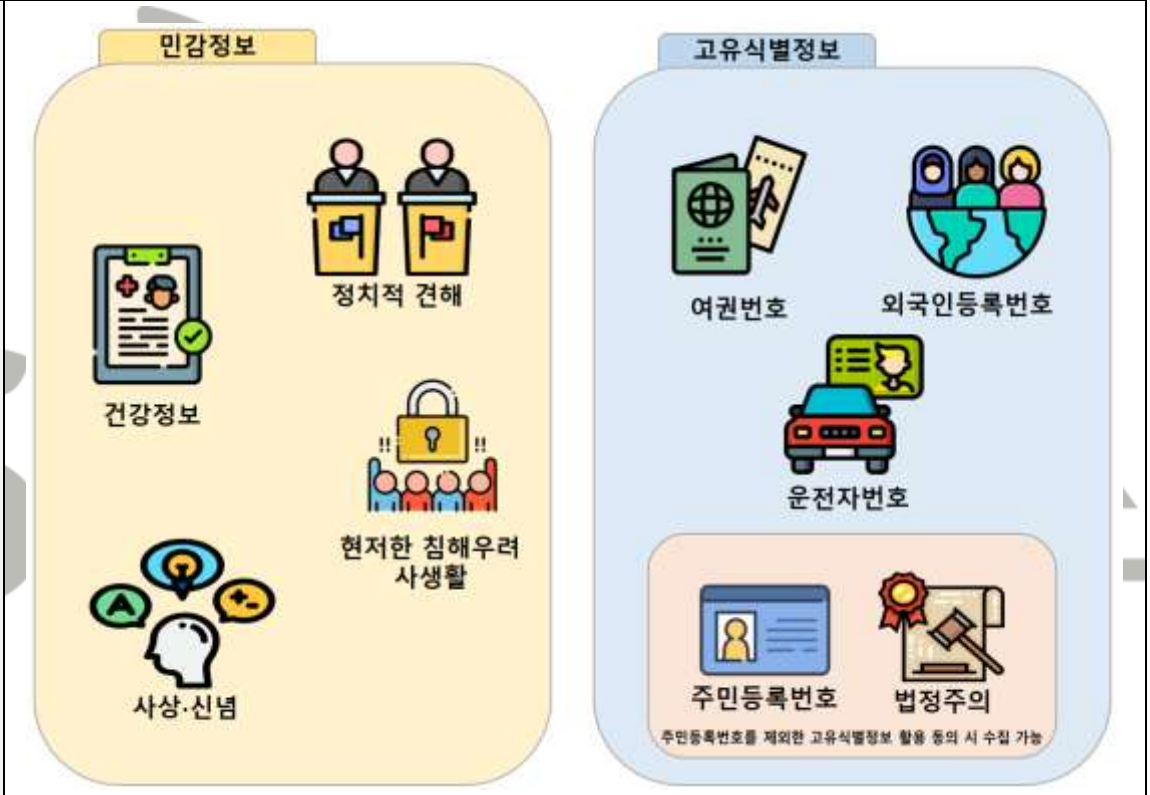
◇ 법적 근거에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하고 있는가?

주민등록번호 대체 수단 제공

① 법적 근거에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법(주민등록번호 대체가입수단)을 제공

	1. 주민등록번호 대체가입수단 예시 : 아이핀, 휴대전화, 신용카드, 인증서 등  ※ 출처: 한국인터넷진흥원 (https://www.kisa.or.kr)

3.1.4 민감정보 및 고유식별정보의 처리 제한

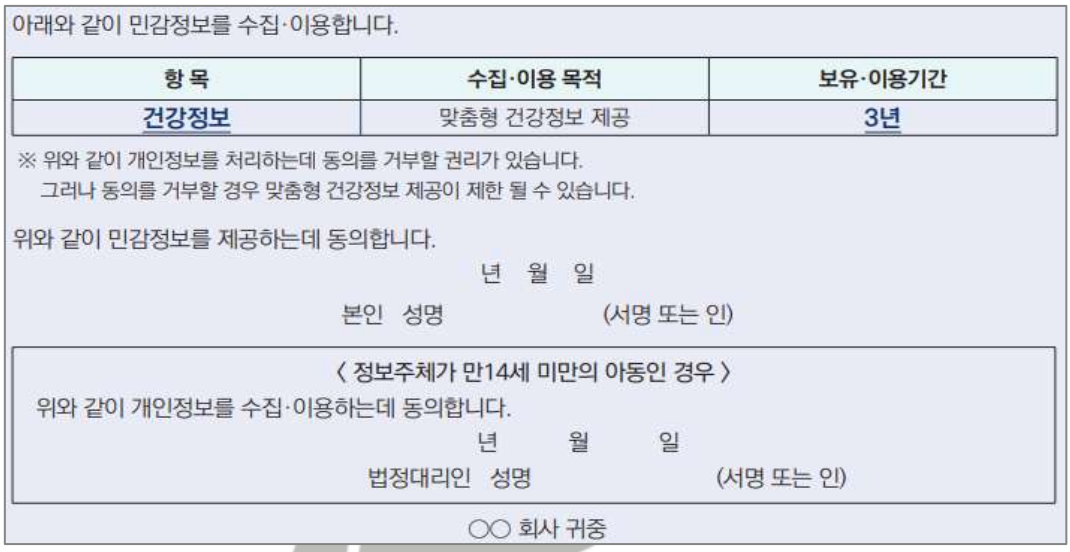
세부분야	3.1.4 민감정보 및 고유식별정보의 처리 제한
인증 기준	민감정보와 고유식별정보(주민등록번호 제외)를 처리하기 위해서는 법령에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고는 정보주체의 별도의 동의를 받아야 한다.
주요 확인사항	• 민감정보는 정보주체로부터 별도의 동의를 받거나 관련 법령에 근거가 있는 경우에만 처리하고 있는가? • 고유식별정보(주민등록번호 제외)는 정보주체로부터 별도의 동의를 받거나 관련 법령에 구체적인 근거가 있는 경우에만 처리하고 있는가? • 재화 또는 서비스를 제공하는 과정에서 공개되는 정보에 정보주체의 민감정보가 포함됨으로써 사생활 침해의 위험성이 있다고 판단하는 때에는 재화 또는 서비스의 제공 전에 민감정보의 공개 가능성 및 비공개를 선택하는 방법을 정보주체가 알아보기 쉽게 알리고 있는가?
기준 요약도	
운영 방안	**◇ 민감정보는 정보주체로부터 별도의 동의를 받거나 관련 법령에 근거가 있는 경우에만 처리하고 있는가?** **민감정보 처리 요건** ① 별도 동의 또는 법령 근거 1. 민감정보(인종·사상·신념, 정치적 견해, 노조 가입, 유전정보, 건강·성생활 정보 등)에 대한 정보주체로부터 명시적 별도 동의

2.「개인정보보호법」 및 개별 법령(예:「의료법」,「고용보험법」 등)에 구체적 근거가 있을 때만 처리

② 동의서 구성

1. 민감정보 항목, 처리 목적, 보유 기간, 제3자 제공 여부 등 관련사항을 구체적으로 명시

2. 동의 거부권 관련 내용 고지



아래와 같이 민감정보를 수집·이용합니다.

항 목	수집·이용 목적	보유·이용기간
건강정보	맞춤형 건강정보 제공	3년

※ 위와 같이 개인정보를 처리하는데 동의를 거부할 권리가 있습니다.
그러나 동의를 거부할 경우 맞춤형 건강정보 제공이 제한 될 수 있습니다.

위와 같이 민감정보를 제공하는데 동의합니다.

년 월 일

본인 성명 (서명 또는 인)

〈 정보주체가 만14세 미만의 아동인 경우 〉

위와 같이 개인정보를 수집·이용하는데 동의합니다.

년 월 일

법정대리인 성명 (서명 또는 인)

○○ 회사 귀중

※ 출처: 알기쉬운 개인정보 처리 동의 안내서 (개인정보보호위원회)

◇ 고유식별정보(주민등록번호 제외)는 정보주체로부터 별도의 동의를 받거나 관련 법령에 구체적인 근거가 있는 경우에만 처리하고 있는가?

고유식별정보(주민등록번호 제외) 처리 요건

① 별도 동의 또는 법령 근거

1. 여권번호, 운전면허번호, 외국인등록번호, 법인등록번호 등 고유식별정보 수집에 대한 정보주체 별도 동의

2.「여신전문금융업법」·「여행업법」·「전자정부법」 등 법령에 구체적 수집·처리 근거가 있는 경우

② 동의 및 문서화

1. 고유식별정보 처리 전 별도 체크박스 동의 확보

2. 법령명·조문·근거 목적을 내부 문서와 개인정보처리방침에 명시

◇ 재화 또는 서비스를 제공하는 과정에서 공개되는 정보에 정보주체의

민감정보가 포함됨으로써 사생활 침해의 위험성이 있다고 판단하는 때에는 재화 또는 서비스의 제공 전에 민감정보의 공개 가능성 및 비공개를 선택하는 방법을 정보주체가 알아보기 쉽게 알리고 있는가?

개인정보처리방침 또는 서비스를 제공하는 과정에서 해당 내용 공개

① 민감정보의 공개 가능성 및 비공개를 선택하는 방법

1. '민감정보가 공개될 수 있다는 사실'과 '비공개를 선택하는 방법'을 정보주체가 쉽게 이해할 수 있도록 기재

- 단, 공개 게시판, 소셜네트워크서비스(SNS) 등 서비스 자체가 공개를 기본으로 하여 상호 의사소통을 목적으로 하고 있어 정보주체가 공개 게시판 등에 스스로 입력하는 정보가 공개된다는 사실을 이미 알고 있다고 볼 수 있는 경우에는 제외할 수 있음

2. 공개될 수 있는 민감정보 항목을 모두 명확히 기재하고, 이용자가 원하는 경우 비공개를 선택할 수 있는 구체적인 절차와 방법을 기재

작성 예시

□ 민감정보의 공개 가능성 및 비공개를 선택하는 방법

*〈개인정보처리자명〉*이(가) 다음과 같은 재화 또는 서비스를 제공하는 과정에서 공개되는 정보에 정보주체의 민감정보가 포함될 수 있으며 이에 대해 정보주체는 비공개를 선택할 수 있습니다.

재화 또는 서비스 명	민감정보	공개 가능성	비공개 선택 방법
지도앱 서비스	성생활, 건강정보	이용자가 스스로 정보를 입력하여 저장한 폴더에 민감정보가 저장된 경우 해당 폴더가 공개로 설정되어 있다면 공개 가능함	☑ 민감정보가 공개될 가능성이 있는 경우 경고창을 띄워 해당 경고창에서 민감정보 공개 가능성을 안내하고, 비공개 여부를 선택할 수 있도록 링크 제공함 ☑ 나의 정보 → 폴더설정 → 민감정보 공개 여부 설정
운동앱 서비스	체지방지수, 심박수, 근육량 지수, 칼로리 소모량	이용자가 스스로 정보를 입력하여 저장한 폴더에 민감정보가 저장된 경우 해당 폴더가 공개로 설정되어 있다면 공개 가능함	☑ 민감정보가 공개될 가능성이 있는 경우 경고창을 띄워 해당 경고창에서 민감정보 공개 가능성을 안내하고, 비공개 여부를 선택할 수 있도록 링크 제공함 ☑ 나의 정보 → 헬스설정 → 민감정보 공개 여부 설정

※ 출처: 개인정보 처리방침 작성지침 (개인정보보호위원회)

3.1.5 개인정보 간접수집

세부분야	3.1.5 개인정보 간접수집
인증 기준	정보주체 이외로부터 개인정보를 수집하거나 제3자로부터 제공받는 경우에는 업무에 필요한 최소한의 개인정보를 수집하거나 제공받아야 하며, 법령에 근거하거나 정보주체의 요구가 있으면 개인정보의 수집 출처, 처리목적, 처리정지의 요구권리를 알려야 한다
주요 확인사항	• 정보주체 이외의 제3자로부터 개인정보를 제공받는 경우 개인정보 수집에 대한 동의획득 책임이 개인정보를 제공하는 자에게 있음을 계약을 통해 명시하고 있는가? • 공개된 매체 및 장소에서 개인정보를 수집하는 경우 정보주체의 공개 목적·범위 및 사회 통념상 동의 의사가 있다고 인정되는 범위 내에서만 수집·이용하고 있는가? • 서비스 계약 이행을 위해 필요한 경우로서, 서비스 제공 과정에서 자동수집장치 등에 의해 수집·생성하는 개인정보의 경우에도 최소수집 원칙을 적용하고 있는가? • 정보주체 이외로부터 수집하는 개인정보에 대해 정보주체의 요구가 있는 경우 즉시 필요한 사항을 정보주체에게 알리고 있는가? • 정보주체 이외로부터 수집한 개인정보를 처리하는 경우 개인정보의 종류·규모 등이 법적 요건에 해당하는 경우 필요한 사항을 정보주체에게 알리고 있는가? • 정보주체에게 수집 출처에 대해 알린 기록을 해당 개인정보의 파기 시까지 보관·관리하고 있는가?
기준 요약도	
운영 방안	**◇ 정보주체 이외의 제3자로부터 개인정보를 제공받는 경우 개인정보 수집에 대한 동의획득 책임이 개인정보를 제공하는 자에게 있음을 계약을 통해 명시하고 있는가?** **개인정보를 제공받은 경우**

① 개인정보를 제공하는 자에게 수집동의에 대한 입증책임이 있음을 계약에 명시

1. 제3자 동의서 사본 또는 동의 증빙 제출 요구
2. 수집 전 개인정보 수집동의 내용과 수집항목의 일치 여부 확인

◇ 공개된 매체 및 장소에서 개인정보를 수집하는 경우 정보주체의 공개 목적·범위 및 사회 통념상 동의 의사가 있다고 인정되는 범위 내에서만 수집·이용하는가?

(예시) 공개된 개인정보 수집

① 상품거래 목적의 중고거래사이트 전화번호 기재

② 정보주체로부터 직접 명함 또는 유사한 매체 제공

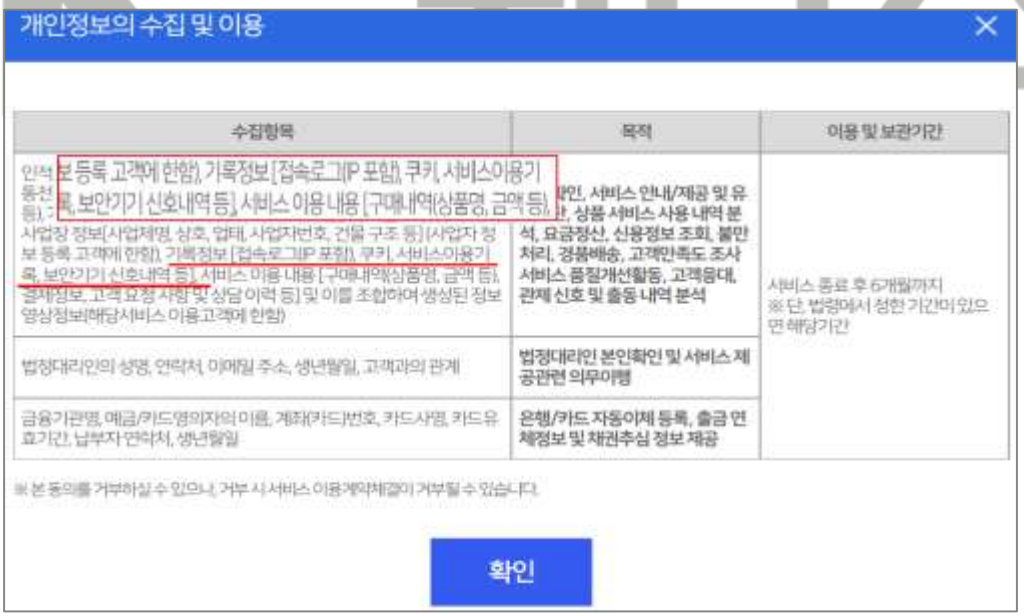
③ 업무처리를 위해 회사나 기관 홈페이지 등에 게재된 담당직원 회사번호나 이메일 등

※ 공개정보를 목적 외 용도(홍보나 마케팅 등) 이용·수집·가공·제공할 수 없음

◇ 서비스 계약 이행을 위하여 필요한 경우로서 사업자가 서비스 제공 과정에서 자동 수집장치 등에 의하여 수집·생성하는 개인정보의 경우에도 최소 수집 원칙을 적용하고 있는가?

자동수집 정보 동의 사항

① 자동수집장치 등에 의하여 수집·생성되는 개인정보(통화기록, 접속로그, 결제기록, 이용내역 등)에 대해서도 해당 서비스의 계약이행 및 제공을 위하여 필요한 최소한의 개인정보만을 수집



※ 출처: SK쉴더스 홈페이지 캡스홈 도어 가이드 온라인가입 화면 (SK쉴더스)

◇ 정보주체 이외로부터 수집하는 개인정보에 대하여 정보주체의 요구가 있는 경우 즉시 필요한 사항을 정보주체에게 알리고 있는가?

간접수집한 개인정보의 정보주체 요구 시 알려야 할 사항

① 정보주체의 요구가 있는 경우 알려야 할 사항

1. 개인정보의 수집 출처
2. 개인정보의 처리 목적
3. 개인정보 처리의 정지를 요구하거나 동의를 철회할 권리가 있다는 사실

② 정당한 사유가 없는 한 정보주체의 요구가 있은 날로부터 3일 이내에 알려야 함

◇ 정보주체 이외로부터 수집하는 개인정보에 대하여 정보주체의 필요한 사항을 정보주체에게 알리고 있는가?

간접수집한 개인정보의 처리 시 통지

① 통지 의무

1. 법적 요건에 해당하는 경우

- 5만 명 이상 정보주체에 관한 민감정보 또는 고유식별정보를 처리하는 자
- 100만 명 이상의 정보주체에 관한 개인정보를 처리하는 자

2. 정보주체의 요구가 있는 경우

② 정보주체에게 알려야 할 사항

1. 개인정보의 수집 출처
2. 개인정보의 처리 목적
3, 개인정보 처리의 정지를 요구할 권리가 있다는 사실

③ 통지 시기

1. 개인정보를 제공받는 날로부터 3개월 이내
2. 연 2회 이상 주기적으로 개인정보를 제공받아 처리하는 경우에는 개인정보를 제공받은 날부터 3개월 이내에 정보주체에게 알리거나 그 동의를 받은 날부터 기산하여 연 1회 이상

④ 통지 방법

1. 서면·전자우편·전화·문자전송 등 정보주체가 통지 내용을 쉽게 확인할 수 있는 방법
2. 재화 및 서비스를 제공하는 과정에서 정보주체가 쉽게 알 수 있도록 알림창을 통해 알리는 방법

⑤ 통지 예외

1. 통지를 요구하는 대상이 되는 개인정보가 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우

	통지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우 ※ 다만, 이 법에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한함 **◇ 정보주체에게 수집 출처에 대하여 알린 기록을 해당 개인정보의 파기 시까지 보관·관리하고 있는가?** **수집 출처에 대해 알린 기록 보관·관리** ① 정보주체에게 알린 사실 ② 알린 시기 ③ 알린 방법

3.1.6 영상정보처리기기 설치·운영

세부분야	3.1.6 영상정보처리기기 설치·운영
인증기준	고정형 영상정보처리기기를 공개된 장소에 설치·운영하거나 이동형 영상정보처리기기를 공개된 장소에서 업무를 목적으로 운영하는 경우 설치 목적 및 위치에 따라 법적 요구사항을 준수하고, 적절한 보호 대책을 수립·이행하여야 한다.
주요 확인사항	• 공개된 장소에 고정형 영상정보처리기기를 설치·운영할 경우 법적 허용 요건에 해당하는지를 검토하고 있는가? • 공공기관이 공개된 장소에 고정형 영상정보처리기기를 설치·운영하려는 경우 공청회·설명회 개최 등의 법령에 따른 절차를 거쳐 관계 전문가 및 이해관계자의 의견을 수렴하고 있는가? • 고정형 영상정보처리기기 설치·운영 시 정보주체가 쉽게 인식할 수 있도록 안내판 설치 등 필요한 조치를 하고 있는가? • 업무를 목적으로 공개된 장소에서 이동형 영상정보처리기기를 운영하는 경우 법적 허용 요건에 해당하는지를 검토하고 있는가? • 업무를 목적으로 공개된 장소에서 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하는 경우 불빛, 소리, 안내판 등의 방법으로 촬영 사실을 표시하고 알리고 있는가? • 영상정보처리기기 및 영상정보의 안전한 관리를 위한 영상정보처리기기 운영·관리 방침을 마련하여 시행하고 있는가? • 영상정보의 보관 기간을 정하고 있으며, 보관 기간 만료 시 지체 없이 파기하고 있는가? • 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우 관련 절차 및 요건에 따라 계약서에 반영하고 있는가?
기준 요약도	

운영 방안	**◇ 공개된 장소에 고정형 영상정보처리기기를 설치·운영할 경우 법적 허용 요건에 해당하는지를 검토하고 있는가?** **공개된 장소에 영상정보처리기기를 설치·운영할 수 있는 경우** ① 법령에서 구체적으로 허용하고 있는 경우 ② 범죄의 예방 및 수사를 위하여 필요한 경우 ③ 시설안전 및 화재 예방을 위하여 필요한 경우 ④ 교통단속을 위하여 필요한 경우 ⑤ 교통정보의 수집·분석 및 제공을 위하여 필요한 경우 **◇ 공공기관이 공개된 장소에 고정형 영상정보처리기기를 설치·운영하려는 경우 공청회·설명회 개최 등의 법령에 따른 절차를 거쳐 관계 전문가 및 이해관계자의 의견을 수렴하고 있는가?** **관계 전문가 및 이해관계자의 의견 수렴** ① 절차 및 방법 1. 공공기관은 고정형 영상정보처리기기 설치·운영 시 다음 중 어느 하나에 해당하는 절차를 거쳐 관계인의 의견을 수렴하여야 함. - 행정절차법에 따른 행정예고의 실시 또는 의견 청취(공청회 등) - 해당 고정형 영상정보처리기기의 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회·설문조사 또는 여론조사 ② 특별시설 의견수렴 대상 1. 교도소, 정신보건시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설에 고정형 영상정보처리기기를 설치하는 경우 다음 각 호에 해당하는 사람으로부터 의견 수렴. - 관계 전문가 - 해당 시설에 종사하는 사람, 해당 시설에 구금되어 있거나 보호받고 있는 사람 또는 그 사람의 보호자 등 이해관계인 ③ 목적 변경 시 절차 1. 고정형 영상정보처리기기의 설치 목적 변경 및 추가 설치 등의 경우에도 관계 전문가 및 이해관계인의 의견 수렴. 2. 단, 설치 목적이나 촬영범위 등의 주요 내용 변경이 없는 단순 추가 설치의 경우에는 의견 수렴을 하지 않을 수 있음

◇ 고정형 영상정보처리기기 설치·운영 시 정보주체가 쉽게 인식할 수 있도록 안내판 설치 등 필요한 조치를 하고 있는가?

안내판 설치

① 안내판 설치 원칙

1. 안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 설치

2. 안내판의 크기나 위치는 자율적으로 정하되, 정보주체가 손쉽게 인식할 수 있도록 다음 사항을 유의하여 설치

- 정보주체가 쉽게 알아볼 수 있는 출입구, 정문 등 눈에 잘 띄는 장소에 설치

- 건물 내, 공원 등 설치 장소에 따라 정보주체가 쉽게 판독할 수 있도록 안내판의 글자 크기와 높이를 조절

② 안내판 기재사항

1. 설치 목적 및 장소

2. 촬영 범위 및 시간

3. 관리책임자의 연락처

4. 공공기관이 고정형 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 수탁자의 명칭 및 연락처

③ 설치 예외사항

1. 다음에 해당하는 시설에 설치하는 고정형 영상정보처리기기에 대해서는 안내판을 설치하지 않을 수 있음.

- 군사기지 및 군사시설 보호법에 따른 군사시설

- 통합방위법에 따른 국가중요시설

- 보안업무규정에 따른 국가보안시설

안내판 및 홈페이지 게재 내용 예시

고정형 영상정보처리기기(CCTV) 설치 안내

- 설치목적: 범죄 예방 및 시설 안전·관리
- 설치장소: 출입구의 벽면/천장, 엘리베이터/각 층의 천장
- 촬영범위: 출입구, 엘리베이터 및 각 층 복도(360°회전)
- 촬영시간: 24시간 연속 촬영
- 관리책임자: 02-○○○-○○○○
  (설치·운영을 위탁한 경우)
- 수탁관리자: ○○○○ 업체, 02-○○○-○○○○

※ 안내판에 CCTV 그림을 표시하여 정보주체가 쉽게 인식할 수 있도록 하는 것이 바람직

※ 출처: 고정형 영상정보처리기기 설치·운영 안내서 (개인정보보호위원회)

◇ 업무를 목적으로 공개된 장소에서 이동형 영상정보처리기기를 운영하는 경우 법적 허용 요건에 해당하는지를 검토하고 있는가?

이동형 영상정보처리기기 허용 요건

① 개인정보보호법 제15조제1항 각 호의 어느 하나에 해당하는 경우

1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약 이행을 위하여 필요한 경우
5. 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우
7. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

② 촬영 사실을 명확히 표시하여 정보주체가 촬영 사실을 알 수 있도록 하였음에도 불구하고 촬영 거부 의사를 밝히지 아니한 경우

1. 정보주체의 권리를 부당하게 침해할 우려가 없고 합리적인 범위를 초과하지 아니하는 경우로 한정

③ 그 밖에 제1호 및 제2호에 준하는 경우로서 대통령령으로 정하는 경우

사 례 **이동형 영상정보처리기기 관련 법 제15조제1항 각 호의 적용 사례**

구분	법률 조항	사례
제1호	정보주체의 동의를 받은 경우	정보주체에게 서면 등을 통해 촬영목적 등*을 사전에 알리고 동의를 받은 경우를 말함 * 구체적 고지사항은 법 제15조제2항 각 호에 규정
제2호	법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우	법률에서 영상 촬영을 구체적으로 요구·허용하는 규정이 있거나, 법령*에서 부과한 의무를 이행하기 위하여 영상 촬영이 불가피한 경우를 말함 * 법령은 법률 외에도 대통령령, 총리령, 부령 등 포함(「행정기본법」 제2조제1항가목 참조)
제3호	공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우	공공기관이 법령 등*에 따른 소관업무 수행을 위하여 영상 촬영이 불가피한 경우를 말함 * '법령 등'에는 기관별 직제, 조례 등 포함 ※ 예 : 지자체 등에서 불법주차 차량 촬영 등
제4호	정보주체와 체결한 계약을 이행하거나 계약을 체결하는 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우	개인정보처리자가 정보주체와 영상 촬영이 수반되는 계약을 체결하여 이를 이행하거나 계약 과정에서 정보주체의 요청에 따른 조치를 이행하기 위하여 필요한 경우를 말함 ※ 예 : 광고촬영, 웨딩촬영, 배송완료 촬영 등
제5호	명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우	본인 또는 다른 사람의 급박한 생명, 신체, 재산상 이익(또는 위험)과 관련하여 영상 촬영이 필요하다고 인정되는 경우를 말함 ※ 예 : 사건사고 상황을 촬영하여 피해구제 활용 등
제6호	개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.	개인정보처리자가 자신의 정당한 이익 달성을 위해 영상을 촬영하는 경우로서 그 이익이 정보주체의 권리보다 명백하게 우선하는 경우를 말하며, 이러한 경우에도 개인정보처리자의 이익과 상당한 관련성이 있고 합리적 범위를 초과하지 않아야 함 ※ 예 : 위험지역에 대한 원격 영상 모니터링 등
제7호	공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우	공공의 안전과 안녕을 위한 사항과 관련하여 영상 촬영이 긴급히 필요한 경우를 말함 ※ 예 : 감염병 상황을 촬영하여 긴급히 전파 등

※ 출처: 이동형 영상정보처리기기를 위한 개인영상정보 보호·활용 안내서 (개인정보보호위원회)

◇ 업무를 목적으로 공개된 장소에서 이동형 영상정보처리기기로 사람 또는 그 사람과 관련된 사물의 영상을 촬영하는 경우 불빛, 소리, 안내판 등의 방법으로 촬영 사실을 표시하고 알리고 있는가?

이동형 영상정보처리기기 촬영 사실 표시 및 알림

① 정보주체가 촬영 사실을 쉽게 알 수 있도록 표시하고 알려야 함

1. 불빛
2. 소리
3. 안내판
4. 안내서면
5. 안내방송
6. 그 밖에 이에 준하는 수단이나 방법

② 예외적 공지 방법

1. 드론을 이용한 항공촬영 등 촬영 방법의 특성으로 인해 정보주체에게 촬영 사실을 알리기 어려운 경우에는 개인정보보호위원회가 구축하는 인터넷 사이트에 공지하는 방법으로 알릴 수 있음

※ 출처: 개인정보 포털 (개인정보보호위원회)

◇ 영상정보처리기기 및 영상정보의 안전한 관리를 위한 영상정보처리기기 운영·관리 방침을 마련하여 시행하고 있는가?

영상정보처리기기 운영·관리 방침 포함 사항

① 영상정보처리기기의 설치 근거 및 설치 목적

② 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위

③ 관리책임자, 담당 부서 및 영상정보에 대한 접근권한이 있는 사람

④ 영상정보의 촬영시간, 보관 기간, 보관 장소 및 처리 방법

⑤ 영상정보 확인 방법 및 장소

⑥ 정보주체의 영상정보 열람 등 요구에 대한 조치

⑦ 영상정보 보호를 위한 기술적·관리적·물리적 조치

⑧ 그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항

인터넷 홈페이지에 게재하여 정보주체에게 공개

※ 출처: SK쉴더스 홈페이지 (SK쉴더스)

◇ 영상정보의 보관 기간을 정하고 있으며, 보관 기간 만료 시 지체 없이 파기하고 있는가?

영상정보의 보관 기간을 정하여 보관 기간 만료 시 지체 없이 삭제

① 영상정보의 보유 목적 달성을 위한 최소한의 기간으로 보관 기간 결정

② 영상정보처리기기운영자가 그 사정에 따라 보유 목적 달성을 위한 최소한의 기간을 산정하기 곤란한 때에는 보관 기간을 개인영상정보 수집 후 30일 이내로 함

※ 보관 목적 달성을 위해 필요한 최소한의 기간이 30일을 초과하는 경우에는 이를 CCTV 운영·관리 방침에 반영하고 그 기간 동안 보관할 수 있음


4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법

촬영시간	보관기간	보관장소
24시간	촬영일로부터 30일	담당부서

- 처리방법: 개인영상정보의 목적 외 이용, 제3자 제공, 파기, 열람 등 요구에 관한 사항을 기록 관리하고, 보관기간 만료 시 복원이 불가능한 방법으로 영구 삭제(출력물의 경우 파쇄 또는 소각)합니다.

※ 출처: SK쉴더스 홈페이지 (SK쉴더스)

	◇ 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우 관련 절차 및 요건에 따라 계약서에 반영하고 있는가? **영상정보처리기기 설치·운영사무 위탁 계약서에 포함되어야 할 내용** ① 위탁하는 사무의 목적 및 범위 ② 재위탁 제한에 관한 사항 ③ 영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항 ④ 영상정보의 관리 현황 점검에 관한 사항 ⑤ 위탁받는 자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

3.1.7 마케팅 목적의 개인정보 수집·이용

세부분야	3.1.7 마케팅 목적의 개인정보 수집·이용
인증 기준	재화나 서비스의 홍보, 판매 권유, 광고성 정보전송 등 마케팅 목적으로 개인정보를 수집·이용하는 경우 그 목적을 정보주체가 명확하게 인지할 수 있도록 고지하고 동의를 받아야 한다
주요 확인사항	• 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보 처리에 대한 동의를 받는 경우 정보주체가 이를 명확하게 인지할 수 있도록 알리고 별도의 동의를 받고 있는가? • 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 경우 수신자의 명시적인 사전 동의를 받고 있으며, 2년마다 정기적으로 수신자의 수신동의 여부를 확인하고 있는가? • 전자적 전송매체를 이용한 영리목적의 광고성 정보 전송에 대하여 수신자가 수신거부의사를 표시하거나 사전 동의를 철회한 경우 영리목적의 광고성 정보 전송을 중단하도록 하고 있는가? • 영리목적의 광고성 정보를 전송하는 경우 전송자의 명칭, 수신거부 방법 등을 구체적으로 밝히고 있으며, 야간시간에는 전송하지 않도록 하고 있는가?
기준 요약도	
운영 방안	◇ 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보 처리에 대한 동의를 받는 경우 정보주체가 이를 명확하게 인지할 수 있도록 알리고 별도의 동의를 받고 있는가?

영리목적 광고성 정보 전송 시 별도 동의

① 개인정보 처리 동의와 광고성 정보 수신동의 구분

1. 수신자의 개인정보를 수집·이용하는 것과 개인정보 이용 목적에 대한 동의는 광고성 정보 수신동의와 구분

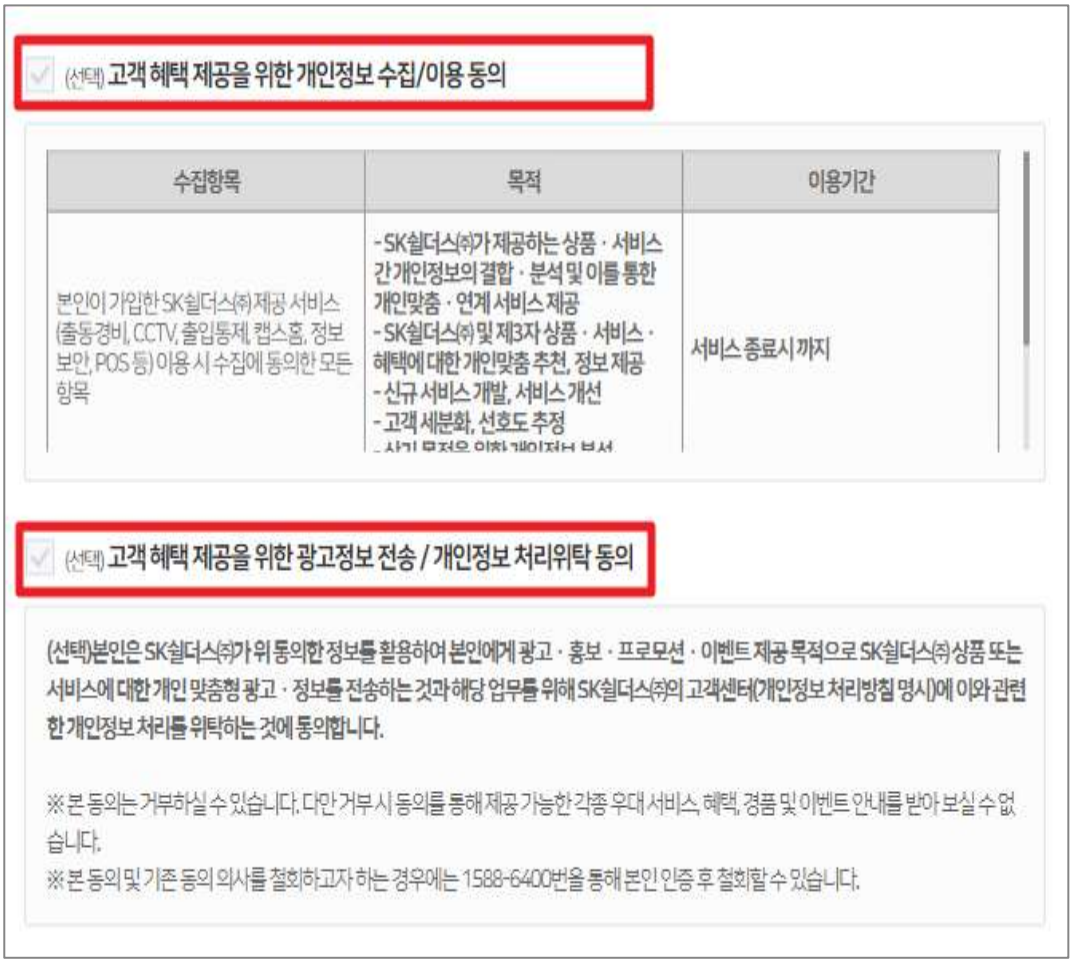
- 개인정보보호법 : 제15조(개인정보의 수집・이용)
- 정보통신망법 : 제50조(영리목적의 광고성 정보 전송 제한)

2. 광고성 정보 수신동의는 전송자가 보내는 광고성 정보를 수신하겠다는 것에 대한 동의를 의미하며 각 동의는 별개로 받아야 함

② 명확한 인지를 위한 요건

1. 정보주체가 마케팅·홍보 목적의 개인정보 처리에 대해 명확하게 인지할 수 있도록 다음 사항을 준수해야 함.

- 수집·이용 목적 명시: "마케팅 정보 발송", "홍보 및 마케팅" 등 구체적 목적 기재
- 수집 항목 구체화: 마케팅에 사용될 개인정보 항목을 명확히 명시
- 별도 동의 절차: 개인정보 수집·이용 동의와 구분
- 동의 거부권 고지: 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익 내용 안내



※ 출처: SK쉴더스 홈페이지 (SK쉴더스)

◇ 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 경우 수신자의 명시적인 사전 동의를 받고 있으며, 2년마다 정기적으로 수신자의 수신동의 여부를 확인하고 있는가?

명시적인 사전 동의 및 정기적인 수신동의 여부 확인

① 전송 가능한 경우

1. 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송 시 수신자의 명시적인 사전 동의를 받아야 함.

2. 단, 다음의 경우는 예외

- 거래관계 예외: 재화 등의 거래관계를 통하여 수신자로부터 직접 연락처를 수집한 자가 거래 종료일로부터 6개월 이내에 동종 재화 등에 대한 광고성 정보를 전송하는 경우

- 전화권유판매 예외: 방문판매법에 따른 전화권유판매자가 육성으로 개인정보 수집 출처를 고지하고 전화권유하는 경우

② 앱 푸시 알림 특별 규정

1. 스마트폰 앱 푸시알림을 통해 광고성 정보를 전송하는 경우

- 앱 설치만으로는 광고성 정보 전송 불가

- 최초 실행 단계나 로그인 이후 단계에서 명시적 수신동의 필요

- "광고성 정보 수신동의"와 "푸시 알림 승인"을 구분하여 받아야 함

③ 정기적인 수신동의 여부 확인

1. 수신동의를 받은 날부터 2년마다 수신동의 여부를 확인하여야 함.

2. 확인 방법 및 내용

- 전송자의 명칭

- 수신동의 날짜 및 수신에 동의한 사실

- 수신동의에 대한 유지 또는 철회 의사를 표시하는 방법

※ 출처: 불법스팸방지 안내서 (개인정보보호위원회•KISA)

◇ 전자적 전송매체를 이용한 영리목적의 광고성 정보 전송에 대하여 수신자가 수신거부의사를 표시하거나 사전 동의를 철회한 경우 영리목적의 광고성 정보 전송을 중단하도록 하고 있는가?

수신거부의사•동의를 철회한 경우 및 효력

① 수신거부의사 표시 대상자

- 수신거부의사 표시
- 회원탈퇴
- 휴면회원

② 그 의사를 표시한 때부터 즉시 효력이 발생하므로 수신거부의 의사를 표시하거나 사전 동의를 철회하였음에도 불구하고 광고성 정보를 전송한 때에는 관련 규정을 위반

③ 통합회원으로 사전 동의를 받은 경우 수신거부시 통합회원에 대한 모든 동의 철회

◇ 영리목적의 광고성 정보를 전송하는 경우 전송자의 명칭, 수신거부 방법 등을 구체적으로 밝히고 있으며, 야간시간에는 전송하지 않도록 하고 있는가?

광고성 정보 전송 시 명시사항

① 전송자의 명칭 및 연락처

② 수신의 거부 또는 수신동의의 철회 의사표시를 쉽게 할 수 있는 조치 및 방법에 관한 사항

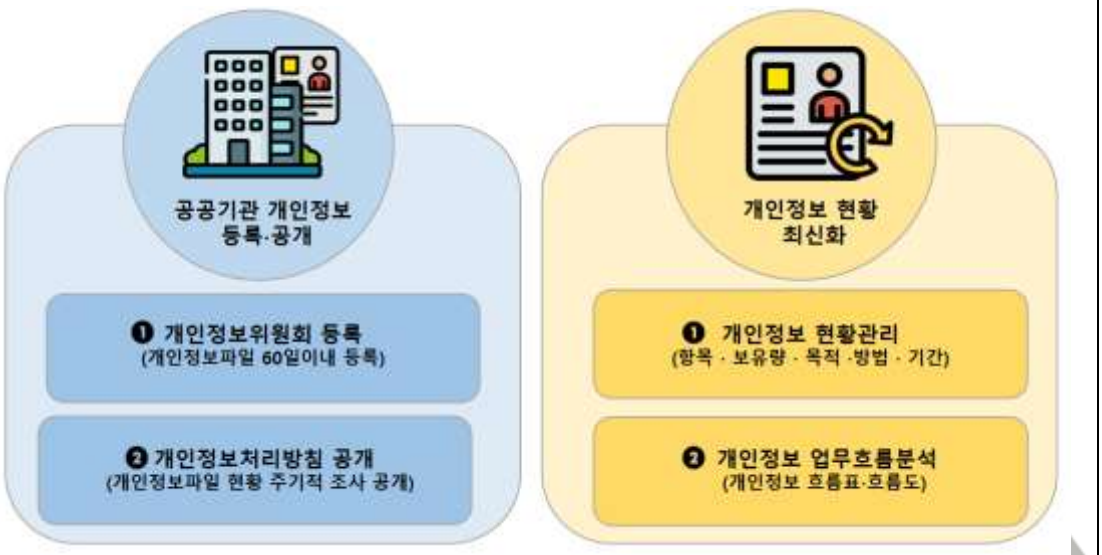
야간광고 전송 제한 및 예외

① 야간광고 제한: 오후 9시부터 그 다음 날 오전 8시까지

② 예외사항: 전자우편 야간광고 가능

3.2 개인정보 보유 및 이용 시 보호조치

3.2.1 개인정보 현황관리

세부분야	3.2.1 개인정보 현황관리
인증 기준	수집·보유하는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하여야 하며, 공공기관의 경우 이를 법률에서 정한 관계기관의 장에게 등록하여야 한다.
주요 확인사항	• 수집·보유하고 있는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하고 있는가? • 공공기관이 개인정보파일을 운용하거나 변경하는 경우 관련된 사항을 법률에서 정한 관계기관의 장에게 등록하고 있는가? • 공공기관은 개인정보파일의 보유 현황을 개인정보처리방침에 공개하고 있는가?
기준 요약도	
운영 방안	**◇ 수집·보유하고 있는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하고 있는가?** **개인정보 현황을 정기적으로 관리** ① 개인정보 현황 기재 항목 1. 개인정보의 항목: 수집·보유하고 있는 구체적인 개인정보 항목 2. 보유량: 처리하고 있는 개인정보의 규모 및 양 3. 처리 근거: 동의, 법령 등에 따른 처리 근거 4. 처리 목적 및 방법: 개인정보를 처리하는 목적과 방법 5. 보유기간: 개인정보를 보유하는 기간 ② 개인정보 현황 관리 문서 1. 개인정보 현황표

- 개인정보파일별 처리현황을 일목요연하게 정리한 표
- 개인정보 항목, 수집방법, 처리목적, 보유기간, 제3자 제공 현황 등 포함

2. 개인정보 흐름표/흐름도
- 개인정보의 수집부터 파기까지 전체 생명주기를 도식화
- 수집→이용→보관→제공→파기 단계별 처리 현황 명시

③ 정기적 관리
- 정기적 점검: 개인정보 현황을 주기적으로 점검
- 문서 최신화: 변경사항 발생 시 관련 문서를 지체없이 업데이트
- 관리대장 작성: 개인정보파일 관리대장을 통한 체계적 관리

개인정보 처리 업무표 예시

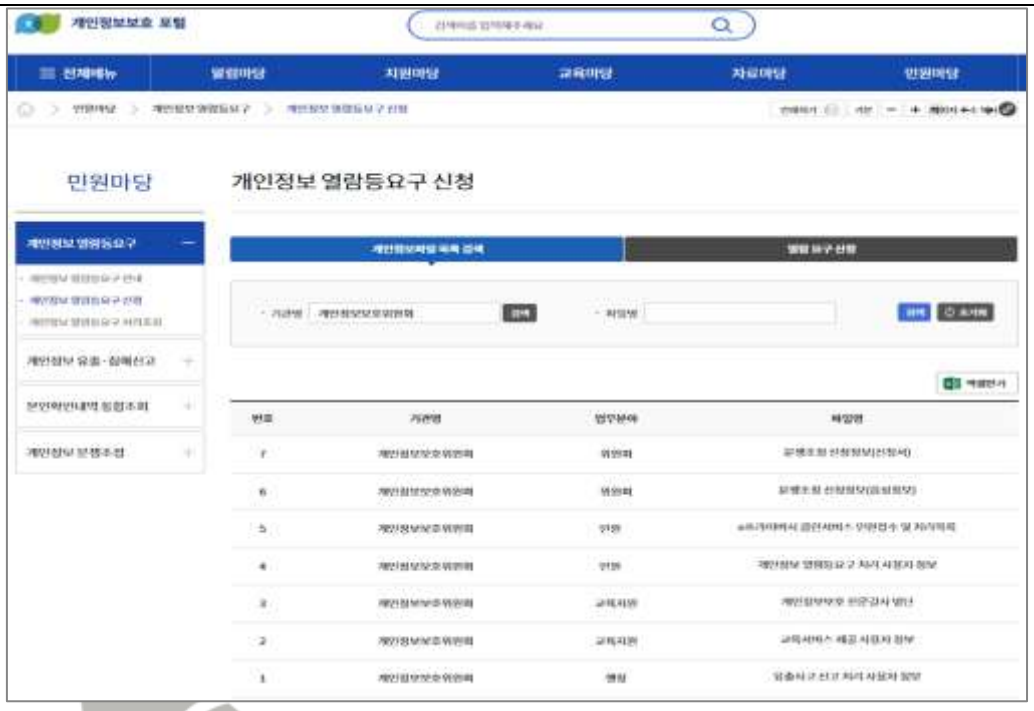
평가 업무명	처리 목적	처리 개인정보	주관 부서	개인정보 건수 (고유식별정보수)	개인정보 영향도
회원관리	홈페이지 회원가입, 본인확인, 정보제공 등 회원 서비스 제공	**필수** : 성명, 생년월일, 전화번호, 이메일주소, ID, 비밀번호 **선택** : 집주소, 집전화번호	민원팀	10만건 (0건)	5
상담업무	고객 문의 및 민원 응대	**필수** : 성명, 전화번호, 상담내용	민원팀	5천건 (0건)	3
실업급여 관리	실업급여 지급확인 및 관련 절차 알림, 확인	**필수** : 성명, 주민등록번호, 계좌번호, 전화번호 **선택** : 이메일주소	민원팀	3만건 (3만건)	5
...	...	...	...	...	...

※ 출처: 개인정보 영향평가 수행 안내서 (개인정보보호위원회•KISA)

◇ 공공기관이 개인정보파일을 운용하거나 변경하는 경우 관련된 사항을 법률에서 정한 관계기관의 장에게 등록하고 있는가?

공공기관 개인정보파일 운용 현황 등록

① 개인정보파일 등록 또는 변경 신청을 받은 개인정보보호책임자는 등록·변경 사항을 검토하고 그 적정성을 판단한 후 개인정보보호위원회에 60일 이내에 등록



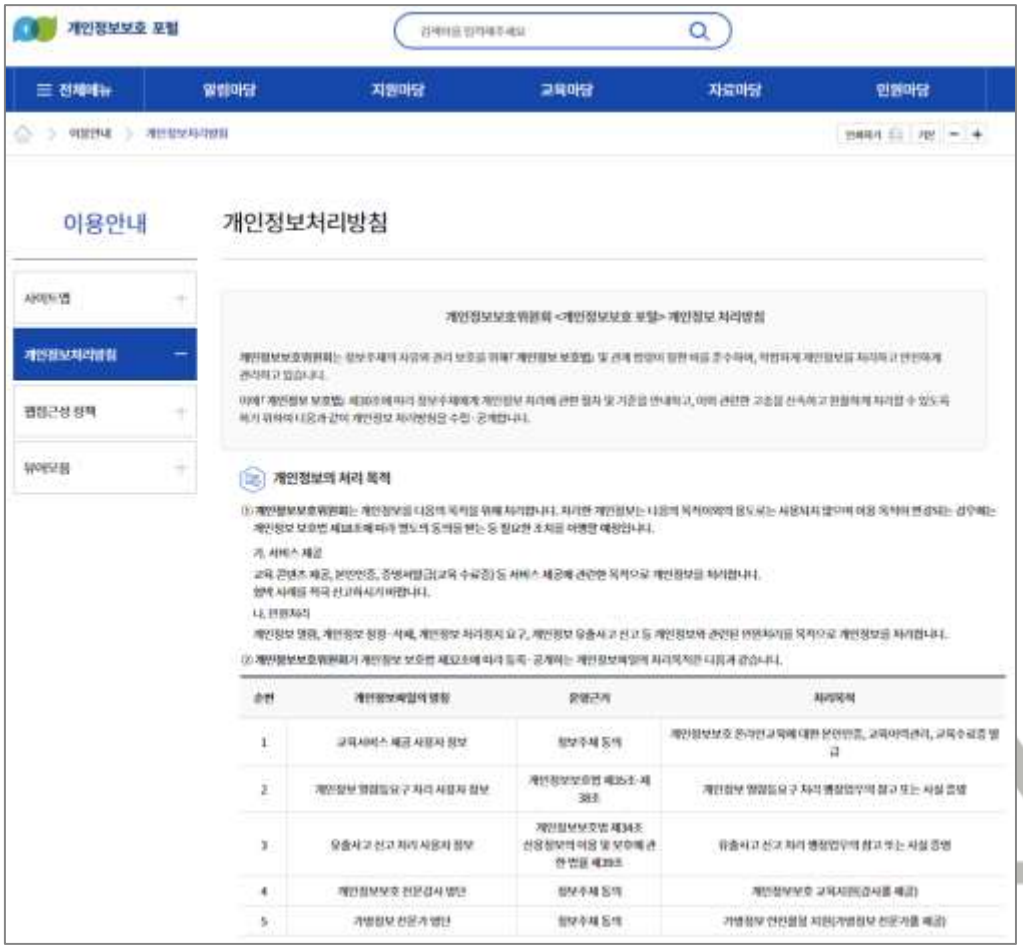
※ 출처: 개인정보보호포털 (https://www.privacy.go.kr)

※ 출처: 개인정보보호포털 (https://www.privacy.go.kr)

◇ 공공기관은 개인정보파일의 보유 현황을 개인정보처리방침에 공개하고 있는가?

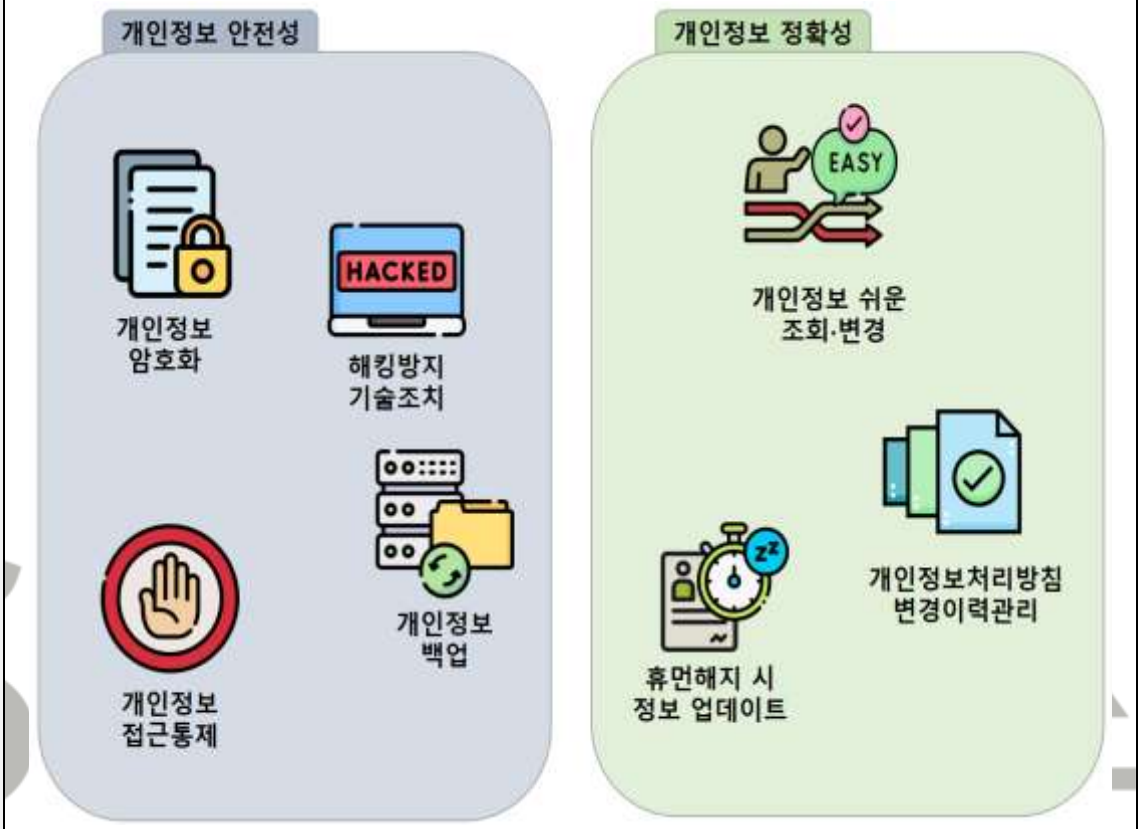
공공기관의 개인정보파일 공개

① 공공기관의 개인정보보호책임자는 개인정보파일의 보유·파기 현황을 주기적으로 조사하여 그 결과를 해당 공공기관의 개인정보처리방침에 공개



※ 출처: 개인정보보호포털 (https://www.privacy.go.kr)

3.2.2 개인정보 품질보장

세부분야	3.2.2 개인정보 품질보장
인증 기준	수집된 개인정보는 처리 목적에 필요한 범위에서 개인정보의 정확성·완전성·최신성이 보장되도록 정보주체에게 관리 절차를 제공하여야 한다.
주요 확인사항	• 개인정보를 최신의 상태로 정확하게 유지하기 위한 절차 및 방안을 수립·이행하고 있는가? • 정보주체가 본인의 개인정보에 대하여 정확성, 완전성 및 최신성을 유지할 수 있는 방법을 제공하고 있는가?
기준 요약도	
운영 방안	**◇ 개인정보를 최신의 상태로 정확하게 유지하기 위한 절차 및 방안을 수립·이행하고 있는가?** **(예시) 개인정보 안전성 확보를 위한 보안조치** ① 개인정보 위조·변조·훼손 방지 조치 1. 안전조치 적용: 접근통제, 암호화, 악성프로그램 방지 등 개인정보의 안전한 처리 및 관리를 위한 조치 2. 위조·변조·훼손 방지: 외부자 해킹, 내부자 권한 오·남용, 재난·재해 등에 의한 불법적인 개인정보 변경, 손상 등을 방지 3. 백업·복구 체계: 개인정보의 정확성, 완전성을 확보할 수 있도록 백업·복구 등의

체계 구축 및 이행

② 개인정보취급자에 의한 오입력 방지

1. 관리적 조치: 개인정보취급자에 의한 개인정보 변경 시 오입력 등이 발생하지 않도록 하는 관리적 조치

2. 기술적 조치: 데이터 검증 기능, 입력 제한 설정 등 기술적 방지 조치

3. 교육 및 점검: 정기적인 교육과 점검을 통한 인적 오류 최소화

③ 정기적인 정확성 확인

1. 주기적 점검: 개인정보의 정확성, 완전성, 최신성을 정기적으로 점검

2. 불일치 정보 관리: 발견된 부정확하거나 불완전한 정보에 대한 즉시 수정 조치

3. 기준 준수: 처리방침에 공개한 내용이 실제 개인정보 처리 현황과 일치하도록 정확성과 투명성, 최신성 유지

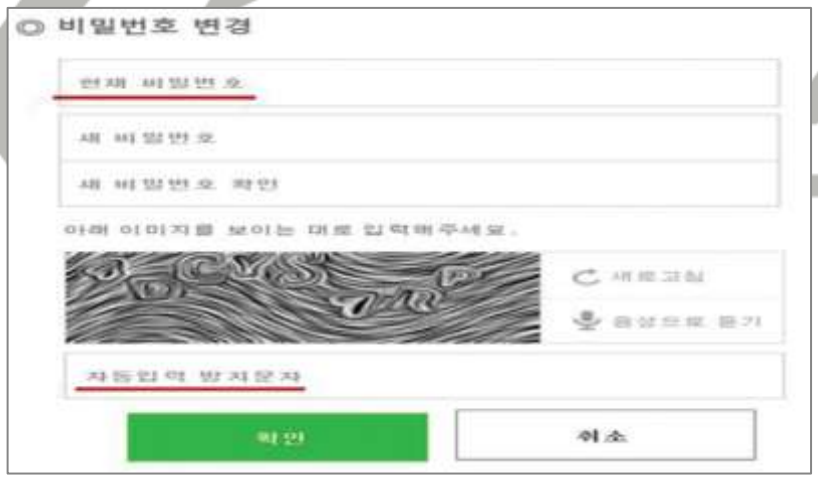
◇ 정보주체가 본인의 개인정보에 대하여 정확성, 완전성 및 최신성을 유지할 수 있는 방법을 제공하고 있는가?

(예시) 정보주체 본인의 정확성·완전성 및 최신성을 유지할 수 있는 방법 제공

① 홈페이지를 통한 개인정보 수정이 주기적으로 이루어질 수 있도록 공지

② 개인정보 등록 현황을 쉽게 조회하고 변경할 수 있도록 다양한 방법 제공

③ 개인정보 변경 시 안전한 본인확인 절차 마련 및 시행



※ 출처: 개인정보 영향평가 수행안내서(개인정보보호위원회•KISA)

④ 휴면 회원인 경우 휴면회원 해제 시 회원정보 업데이트 절차 마련

⑤ 정보주체가 수집 및 처리되는 개인정보의 현황을 쉽게 알 수 있도록 개인정보처리방침의 변경과 이력관련 내용을 쉽게 인지할 수 있도록 게시

3.2.3 이용자 단말기 접근 보호

세부분야	3.2.3 이용자 단말기 접근 보호
인증 기준	정보주체(이용자) 이외로부터 개인정보를 수집하거나 제공받는 경우에는 업무에 필요한 최소한의 개인정보만 수집·이용하여야 하고, 법령에 근거하거나 정보주체(이용자)의 요구가 있으면 개인정보의 수집 출처, 처리목적, 처리정지의 요구권리를 알려야 한다.
주요 확인사항	• 정보주체(이용자)의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한이 필요한 경우 명확하게 인지할 수 있도록 알리고 정보주체(이용자)의 동의를 받고 있는가? • 이동통신단말장치 내에서 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한이 아닌 경우, 정보주체(이용자)가 동의하지 않아도 서비스 제공을 거부하지 않도록 하고 있는가? • 이동통신단말장치 내에서 해당 접근권한에 대한 정보주체(이용자)의 동의 및 철회 방법을 마련하고 있는가?
기준 요약도	
운영 방안	**◇ 정보주체(이용자)의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한이 필요한 경우 명확하게 인지할 수 있도록 알리고 정보주체(이용자)의 동의를 받고 있는가?** **접근권한(필수·선택) 동의**

① 서비스 제공 시 필수 접근권한과 선택 접근권한을 구분하여 고지 및 동의절차 수행

1. 접근권한이 필요한 정보 및 기능의 항목
2. 접근권한이 필요한 이유
3. 접근권한 허용에 대하여 동의하지 아니할 수 있다는 사실

※ 출처: SK쉴더스 모바일가드 스마트폰 앱 (SK쉴더스)

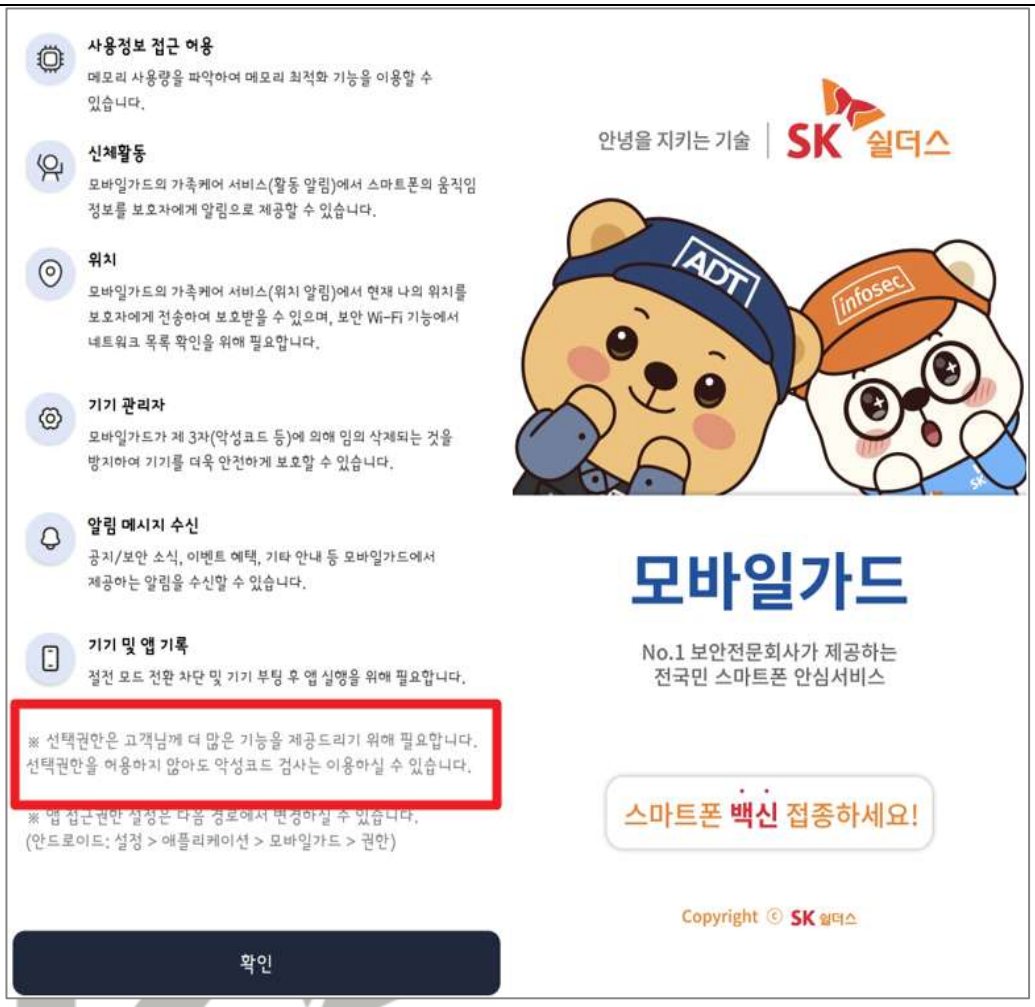
◇ 이동통신단말장치 내에서 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한이 아닌 경우, 정보주체(이용자)가 동의하지 않아도 서비스 제공을 거부하지 않도록 하고 있는가?

선택권한 미동의 시 서비스 제공 거부 금지

① 서비스 제공 보장

1. 선택적 접근권한은 해당 서비스 제공을 위해 반드시 필요하지 않은 접근권한

- 선택적 접근권한에 동의하지 않더라도 앱의 기본 기능을 사용할 수 있어야 함.



※ 출처: SK쉴더스 모바일가드 스마트폰 앱 (SK쉴더스)

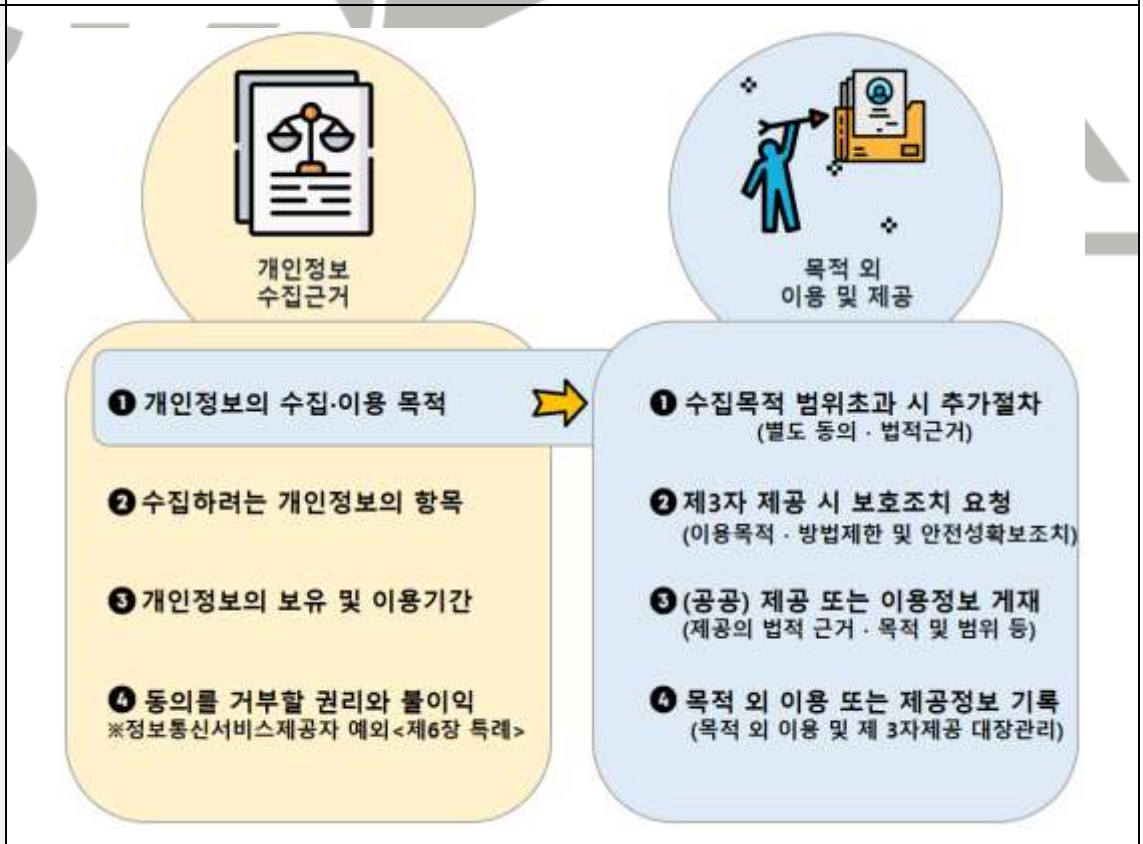
◇ 이동통신단말장치 내에서 해당 접근권한에 대한 정보주체(이용자)의 동의 및 철회방법을 마련하고 있는가?

동의철회 기능제공

① 운영체제(IOS, Android 등)별 동의 철회 기능 구현

※ 출처: 스마트폰 앱 접근권한 안내서 리플렛 (방송통신위원회•KISA)

3.2.4 개인정보 목적 외 이용 및 제공

세부분야	3.2.4 개인정보 목적 외 이용 및 제공
인증 기준	개인정보는 수집 시의 정보주체에게 고지·동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용·제공하려는 때에는 정보주체의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호 대책을 수립·이행하여야 한다.
주요 확인사항	• 개인정보는 최초 수집 시 정보주체로부터 동의받은 목적 또는 법령에 근거한 범위 내에서만 이용·제공하고 있는가? • 개인정보처리자로부터 개인정보를 제공받은 경우 제공받은 목적의 범위 내에서만 이용·제공하고 있는가? • 개인정보를 수집 목적 또는 개인정보처리자로부터 제공받은 목적의 범위를 초과하여 이용하거나 제공하는 경우 정보주체에게 별도의 동의를 받거나 법적 근거가 있는 경우로 제한하고 있는가? • 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우 제공받는 자에게 이용목적·방법 등을 제한하거나 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하고 있는가? • 공공기관이 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하는 경우 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 관보 또는 인터넷 홈페이지 등에 게재하고 있는가? • 공공기관 등이 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하는 경우 목적 외 이용 및 제3자 제공대장에 기록·관리하는 등 절차를 마련하고 있는가?
기준 요약도	

운영 방안

◇ 개인정보는 최초 수집 시 정보주체로부터 동의받은 목적 또는 법령에 근거한 범위 내에서만 이용·제공하고 있는가?

이용•제공 목적의 동의 받은 범위나 법령에 의해 이용

① 수집·이용 목적을 명확히 정의하고, 정보주체의 동의를 받은 범위 및 법령상 근거 이외의 용도로는 개인정보를 이용·제공 금지

※ 출처: SK쉴더스 문의사항 게시판(SK쉴더스)

◇ 개인정보처리자로부터 개인정보를 제공받은 경우 제공받은 목적의 범위 내에서만 이용·제공하고 있는가?

개인정보 목적외 용도 이용 및 제공 제한

① 개인정보를 제공받은 경우 다음 각 호를 제외하고는 다른 용도 이용 제한

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우

※ 다른 법률 규정 관련

① '법률'로 한정되어 있으므로 법률에 위임근거가 없고 시행령·시행규칙에만 관련 규정이 있는 경우에는 허용되지 않음.

② '특별한 규정'에 한하므로 '법령상 의무이행과 같이 포괄적으로 규정된 경우에도 허용되지 않음.

◇ 개인정보를 수집 목적 또는 개인정보처리자로부터 제공받은 목적의 범위를 초과하여 이용하거나 제공하는 경우 정보주체에게 별도의 동의를 받거나 법적 근거가 있는 경우로 제한하고 있는가?

목적 외 이용 및 제공 동의 사항

① 목적 외 이용 시

1. 개인정보의 이용목적
2. 이용하는 개인정보의 항목
3. 개인정보 보유 및 이용기간
4. 동의거부권이 있다는 사실 및 동의거부에 따른 불이익이 있을 시 그 내용

② 목적 외 제3자 제공 시

1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 이용 목적
3. 제공하는 개인정보의 항목
4. 제공받는 자의 개인정보 보유 및 이용기간
5. 동의거부권이 있다는 사실 및 동의거부에 따른 불이익이 있을 시 그 내용

◇ 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우 제공받는 자에게 이용목적·방법 등을 제한하거나 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하고 있는가?

안전성 확보조치를 통한 명확한 책임분류

① 개인정보를 제공하는 자와 개인정보를 제공받는 자는 개인정보의 안전성에 관한 책임관계를 명확화

② 이용목적, 이용방법, 이용기간, 이용형태 등에 일정한 제한

③ 안전성 확보에 필요한 구체적인 조치를 마련하도록 문서(전자문서 포함)로 요청

◇ 공공기관이 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하는 경우 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 관보 또는 인터넷 홈페이지 등에 게재하고 있는가?

목적 외 이용 및 제3자 제공 게재 방법

① 게재 일시

1. 목적 외 이용 등을 한날부터 30일 이내
2. 관보 또는 홈페이지 게재(홈페이지의 경우 10일 이상)

② 공개 사항

1. 목적 외 이용 등을 한 날짜
2. 목적 외 이용 등의 법적 근거
3. 목적 외 이용 등의 목적
4. 목적 외 이용 등을 한 개인정보의 항목

③ 공개 예외

1. 정보주체로부터 별도의 동의를 받은 경우
2. 범죄의 수사와 공소의 제기 및 유지 목적

○○ 공고 제 ○○호

개인정보의 목적 외 이용 또는 제3자 제공 공고

『개인정보 보호법』 제18조(개인정보의 이용·제공 제한) 및 『개인정보 보호법 시행규칙』 제2조(공공기관에 의한 개인정보의 목적 외 이용 또는 제3자 제공의 공고)에 의거 ○○○에서 개인정보의 목적 외 이용 또는 제3자 제공한 내역을 아래와 같이 공고합니다.

1. 관리부서 :
2. 개인정보파일명 :
3. 공고기간 : 게재일로부터 10일 이상
4. 공고 장소 : ○○○ 홈페이지 (고시/공고)
5. 개인정보 목적 외 이용 또는 제3자 제공일 :
6. 개인정보 목적 외 이용 또는 제3자 제공 법적근거 :
7. 개인정보 목적 외 이용 또는 제3자 제공 목적 :
8. 개인정보 목적 외 이용 또는 제3자 제공 항목 :

※ 출처: 개인정보 목적 외 이용 및 제3자 제공 업무처리절차서 (개인정보보호위원회)

◇ 공공기관 등이 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하는 경우 목적 외 이용 및 제3자 제공대장에 기록·관리하는 등 절차를 마련하고 있는가?

기록·관리 사항

① 이용하거나 제공하는 개인정보 또는 개인정보파일의 명칭
② 이용기관 또는 제공받는 기관의 명칭(성명, 연락처)
③ 이용목적 또는 제공받는 목적
④ 이용 또는 제공의 법적 근거

⑤ 이용 또는 제공하는 개인정보의 항목

⑥ 이용 또는 제공의 일자, 주기 또는 기간

⑦ 이용 또는 제공하는 형태

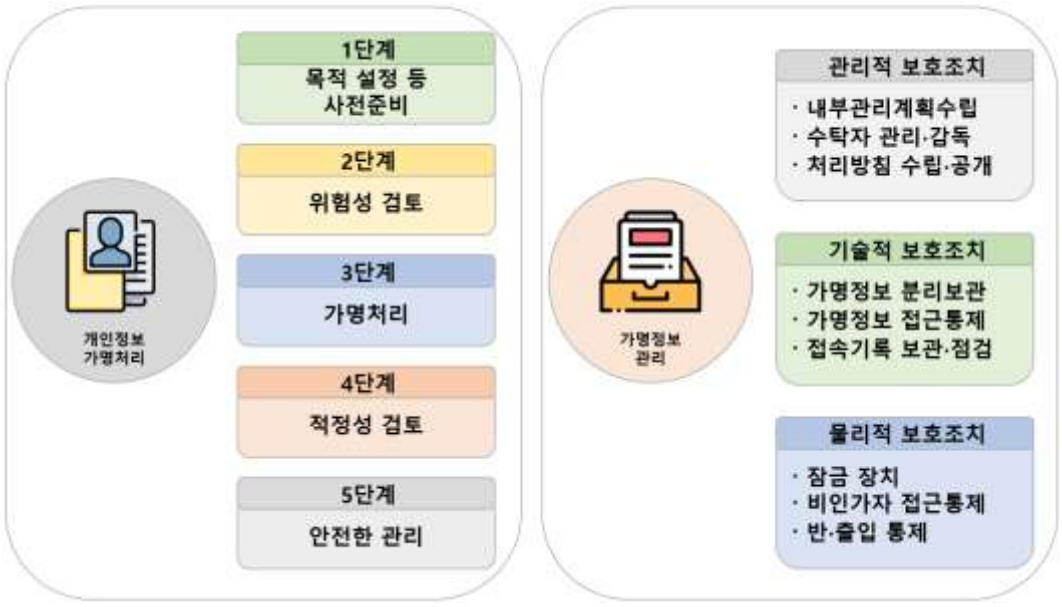
⑧ 개인정보를 제공받는 자에게 개인정보의 이용을 제한을 하거나 안전성 확보를 위하여 필요한 조치를 마련할 것을 요청한 경우에는 그 내용

개인정보의 목적 외 이용 및 제3자 제공 대장

개인정보 또는 개인정보파일 명칭			
이용 또는 제공 구분	[ ] 목적외 이용 [ ] 제3자 제공		
목적 외 이용기관의 명칭 (목적 외 이용의 경우)		담당자	소 속 성 명 전화번호
제공받는 기관의 명칭 (제3자 제공의 경우)		담당자	성 명 소 속 전화번호
이용하거나 제공한 날짜, 주기 또는 기간			
이용하거나 제공한 형태			

※ 출처: 개인정보보호법 시행규칙 [별지 제1호서식]

3.2.5 가명정보 처리

세부분야	3.2.5 가명정보 처리
인증 기준	가명정보를 처리하는 경우 목적제한, 결합제한, 안전조치, 금지의무 등 법적 요건을 준수하고 적정 수준의 가명처리를 보장할 수 있도록 가명처리 절차를 수립·이행하여야 한다.
주요 확인사항	• 가명정보를 처리하는 경우 목적 제한, 가명처리 방법 및 기준, 적정성 검토, 재식별 금지 및 재식별 발생 시 조치사항 등 가명정보를 적정하게 처리하기 위한 절차를 수립하고 있는가? • 개인정보를 가명처리하여 이용·제공 시 추가 정보의 사용·결합 없이는 개인을 알아볼 수 없도록 적정한 수준으로 가명처리를 수행하고 있는가? • 다른 개인정보처리자와 가명정보를 결합하는 경우 결합전문기관 또는 데이터전문기관을 통해 결합하고 있는가? • 가명정보를 처리하는 경우 추가 정보를 삭제 또는 별도로 분리하여 보관·관리, 관련 기록의 작성·보관 등 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하고 있는가? • 가명정보 처리목적 등을 고려하여 가명정보의 처리 기간을 적정한 기간으로 정하고 있으며, 해당 기간이 경과한 경우 지체 없이 파기하고 있는가? • 개인정보를 익명처리하는 경우 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 특정 개인을 알아볼 수 없도록 적정한 수준으로 익명처리하고 있는가?
기준 요약도	
운영 방안	◇ 가명정보를 처리하는 경우 목적 제한, 가명처리 방법 및 기준, 적정성 검토, 재식별 금지 및 재식별 발생 시 조치사항 등 가명정보를 적정하게 처리하기 위한

절차를 수립하고 있는가?

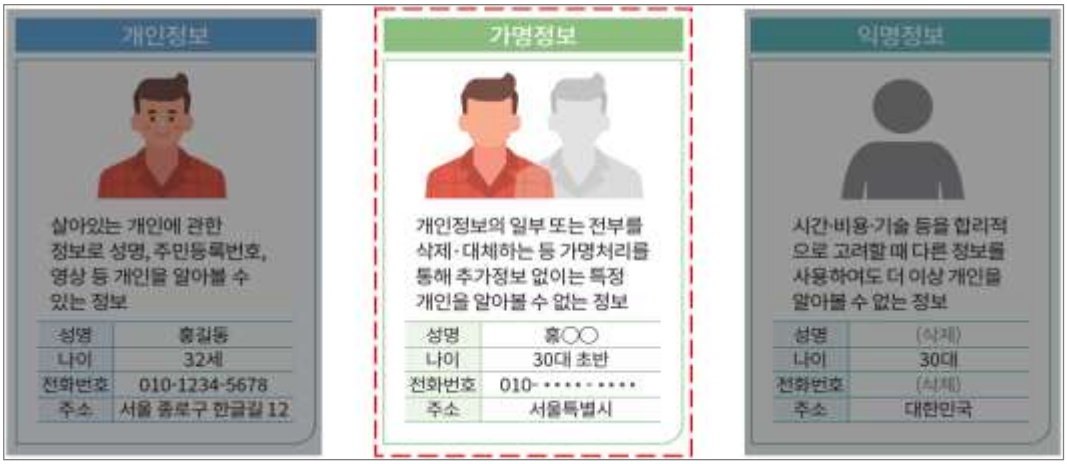
개인정보·가명정보·익명정보 구분

① 개인정보: 살아 있는 개인의 정보

② 가명정보: 일부·전부 삭제 또는 대체 처리

1. 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보 처리 가능

③ 익명정보: 개인을 알아볼 수 없는 정보



※ 출처: 가명정보 처리 가이드라인(개인정보보호위원회)

개인정보 가명처리 단계별 절차도

① 목적 설정 등 사전준비

② 위험성 검토

③ 가명처리

④ 적정성 검토

⑤ 안전한 관리

※ 출처: 가명정보 처리 가이드라인 (개인정보보호위원회)

목적 설정 등 사전준비(개인정보 가명처리 단계별 절차도)

① 목적 설정 등 사전준비:

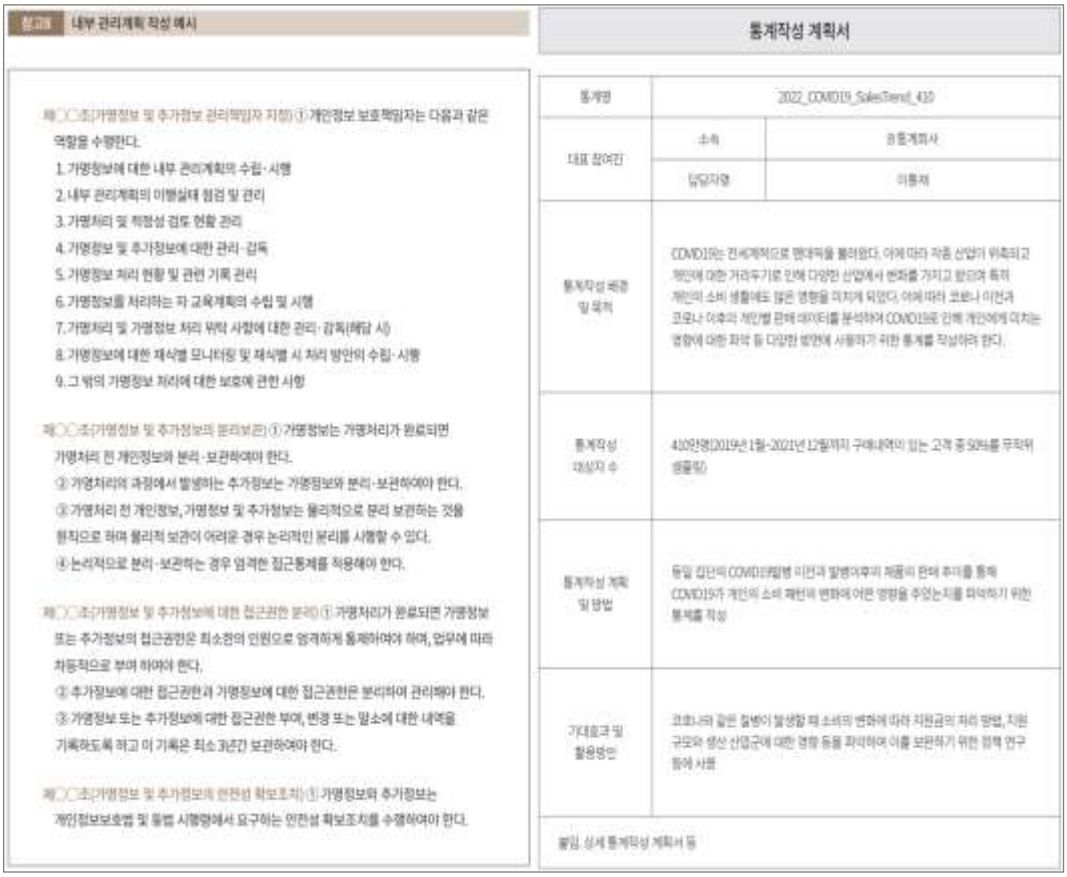
1. 개인정보보호법에서 정한 3가지(통계작성, 과학적 연구, 공익적 기록보존)통계 목적 명확화

2. 개인정보 종류, 범위 등 대상 선정

3. 처리목적의 적합성 검토

4. 내부관리 계획 수립 및 필요서류(위탁 계약서 등) 작성

※ 그 외 위험성검토, 가명처리, 적정성검토, 안전관리 등은 "가명정보 처리 가이드라인(개인정보보호위원회)" 참고



참고 내부 관리계획 작성 예시

제○○조(가명정보 및 추가정보 관리책임자 지정) ① 개인정보 보호책임자는 다음과 같은 역할을 수행한다.

1. 가명정보에 대한 내부 관리계획의 수립·시행
2. 내부 관리계획의 이행실태 점검 및 관리
3. 가명처리 및 적정성 검토 현황 관리
4. 가명정보 및 추가정보에 대한 관리·감독
5. 가명정보 처리 현황 및 관련 기록 관리
6. 가명정보를 처리하는 자 교육계획의 수립 및 시행
7. 가명처리 및 가명정보 처리 위탁 사항에 대한 관리·감독(해당 시)
8. 가명정보에 대한 재식별 모니터링 및 재식별 시 처리 방안의 수립·시행
9. 그 밖의 가명정보 처리에 대한 보호에 관한 사항

제○○조(가명정보 및 추가정보의 분리보관) ① 가명정보는 가명처리가 완료되면 가명처리 전 개인정보와 분리·보관하여야 한다.

② 가명처리의 과정에서 발생하는 추가정보는 가명정보와 분리·보관하여야 한다.

③ 가명처리 전 개인정보, 가명정보 및 추가정보는 물리적으로 분리 보관하는 것을 원칙으로 하며 물리적 보관이 어려운 경우 논리적인 분리를 시행할 수 있다.

④ 논리적으로 분리·보관하는 경우 엄격한 접근통제를 적용해야 한다.

제○○조(가명정보 및 추가정보에 대한 접근권한 분리) ① 가명처리가 완료되면 가명정보 또는 추가정보의 접근권한은 최소한의 인원으로 엄격하게 통제하여야 하며, 업무에 따라 차등적으로 부여 하여야 한다.

② 추가정보에 대한 접근권한과 가명정보에 대한 접근권한은 분리하여 관리해야 한다.

③ 가명정보 또는 추가정보에 대한 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하도록 하고 이 기록은 최소 3년간 보관하여야 한다.

제○○조(가명정보 및 추가정보의 안전성 확보조치) ① 가명정보와 추가정보는 개인정보보호법 및 동법 시행령에서 요구하는 안전성 확보조치를 수행하여야 한다.

통계작성 계획서

통계명	2022_COVID19_SalesTrend_430	
대표 참여인	소속	ㅇㅇ통계회사
	담당자명	이통계
통계작성 배경 및 목적	COVID19는 전세계적으로 팬데믹을 불러왔다. 이에 따라 각종 산업이 위축되고 개인에 대한 거래주기로 인해 다양한 산업에서 변화를 가지고 왔으며 특히 개인의 소비 생활에도 많은 영향을 미치게 되었다. 이에 따라 코로나 이전과 코로나 이후의 개인별 판매 데이터를 분석하여 COVID19로 인해 개인에게 미치는 영향에 대한 파악 등 다양한 방면에 사용하기 위한 통계를 작성하려 한다.	
통계작성 대상자 수	430만명(2019년 1월~2021년 12월까지 구매내역이 있는 고객 중 90%를 무작위 샘플링)	
통계작성 계획 및 방법	동일 집단의 COVID19발병 이전과 발병이후의 제품의 판매 추이를 통해 COVID19가 개인의 소비 패턴의 변화에 어떤 영향을 주었는지를 파악하기 위한 통계를 작성	
기대효과 및 활용방안	코로나와 같은 질병이 발생할 때 소비의 변화에 따라 지원금의 차등 방법, 지원 규모와 생산 산업군에 대한 영향 등을 파악하여 이를 보완하기 위한 정책 연구 등에 사용	

붙임 상세 통계작성 계획서 등

※ 출처: 가명정보 처리 가이드라인(개인정보보호위원회)

◇ 개인정보를 가명처리하여 이용·제공 시 추가 정보의 사용·결합 없이는 개인을 알아볼 수 없도록 적정한 수준으로 가명처리를 수행하고 있는가?

(예시) 개인정보 가명처리 기술종류

① 개인정보 삭제: 삭제, 부분삭제, 행항목삭제, 로컬삭제

② 개인정보 일부 또는 전부 대체: 마스킹, 총계처리, 부분총계, 일반화(범주화)기술

③ 개인정보 암호화: 양방향, 일방향, 순서보존, 형태보존, 동형, 다형성 암호화 등

④ 개인정보 무작위화: 잡음 추가, 순열(치환), 토큰화, 난수생성기

⑤ 기타기술: 표본추출, 해부화, 재현데이터, 동형비밀분산, 차분 프라이버시

❶ 삭제(Suppression) 수치형데이터 문자형데이터

- 원본정보에서 개인정보를 단순 삭제

※ 이때 남아 있는 정보 그 자체로도 분석의 유효성을 가져야 함과 동시에 개인을 식별할 수 없어야 하며, 인터넷 등에 공개되어 있는 정보 등과 결합하였을 경우에도 개인을 식별할 수 없어야 함

성명	성별	나이	핸드폰번호	주소	통신료	단말기금액	누적 포인트
김철수	남	41세	010-6666-8888	서울특별시 중구 무교동	98,700	1,198,700	356,800
이영희	여	61세	010-9999-2222	부산광역시 북구 화명동	69,400	505,400	203,000
박민호	남	30세	010-2222-7777	광주광역시 서구 금호동	104,400	1,604,400	198,000
이윤정	여	57세	010-3333-4444	전라남도 나주시 빛가람동	954,800	3,954,800	20,532,000
최동욱	남	28세	010-5555-6666	세종특별자치시 어진동	83,600	883,600	400,900

삭제

성별	나이	통신료	단말기금액	누적포인트
남	41세	98,700	1,198,700	356,800
여	61세	69,400	505,400	203,000
남	30세	104,400	1,604,400	198,000
여	57세	954,800	3,954,800	20,532,000
남	28세	83,600	883,600	400,900

※ 출처: 가명정보 처리 가이드라인 (개인정보보호위원회)

◇ 다른 개인정보처리자와 가명정보를 결합하는 경우 결합전문기관 또는 데이터전문기관을 통해 결합하고 있는가?

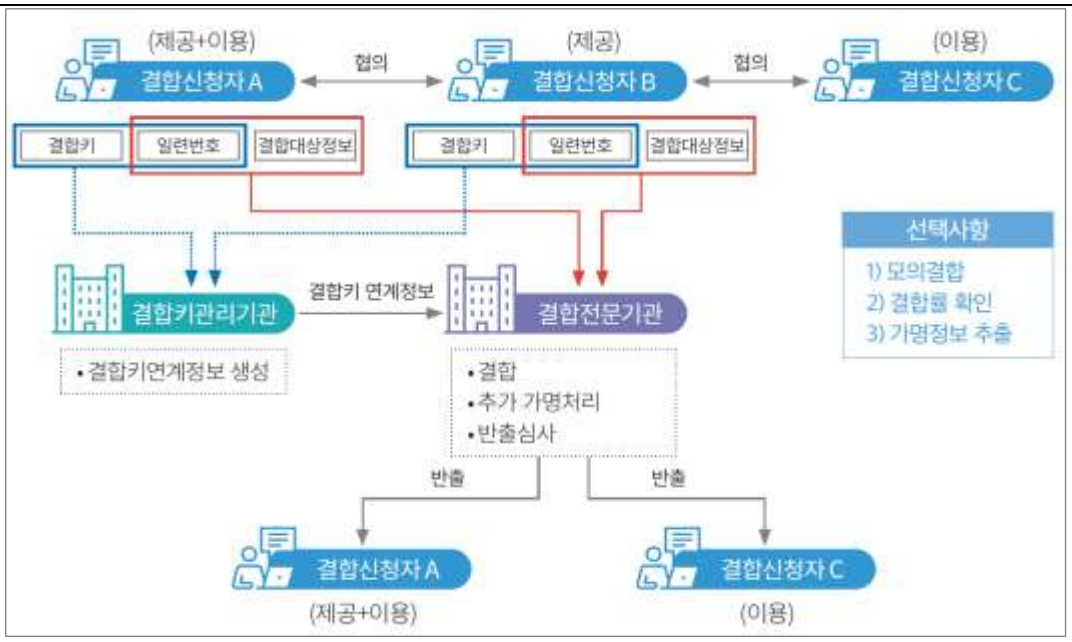
가명정보 결합 절차

① 결합신청: 신청자 간의 결합신청 필요사항 협의 및 결합신청서 작성

② 결합 및 추가처리: 결합키 관리 기관으로부터 받은 정보(Salt값) 이용해 결합기 생성 → 모의결합, 결합률 확인, 가명정보 추출 등 각 기관에 전송

③ 반출 및 활용: 결합정도 또는 분석결과 반출기관에 반출신청

④ 반출 신청한 결합정보 목적에 따라 처리 및 안전조치 의무 준수



※ 출처: 가명정보 처리 가이드라인 (개인정보보호위원회)

◇ 가명정보를 처리하는 경우 추가 정보를 삭제 또는 별도로 분리하여 보관·관리, 관련 기록의 작성·보관 등 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하고 있는가?

(예시) 관리적·기술적·물리적 보호 조치

① 관리적 보호조치: 내부관리계획 수립, 수탁자 관리·감독, 개인정보처리방침 공개 등

② 기술적 보호조치: 가명정보/추가정보 별도 분리저장·관리, 접근통제, 접속기록 보관 점검 등

③ 물리적 보호조치: 전산실·자료실 보관 시 접근통제, 잠금장치, 반·출입 통제 등

◇ 가명정보 처리목적 등을 고려하여 가명정보의 처리 기간을 적정한 기간으로 정하고 있으며, 해당 기간이 경과한 경우 지체 없이 파기하고 있는가?

가명정보 보유 및 이용기간 선정 및 파기

① 가명정보 활용 시 가명정보 보유 및 이용기간 산정 및 목적 달성 후 즉시파기

구분	수집·이용 목적	처리항목	보유 및 이용기간
△△△연구	연령대별 △△ 등 분석	휴대전화번호, △△일시, △△유형	결합데이터 분석 완료시까지

※ 출처: 가명정보 처리 가이드라인 (개인정보보호위원회)

◇ 개인정보를 익명처리하는 경우 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 특정 개인을 알아볼 수 없도록 적정한 수준으로 익명처리하고 있는가?

개인정보 익명처리

① 개인을 식별할 수 있는 모든 정보를 삭제하고 복원이 불가능하도록 처리

※ 출처: 가명정보 처리 가이드라인 (개인정보보호위원회)

3.3 개인정보 제공 시 보호조치

3.3.1 개인정보 제 3 자 제공

세부분야	3.3.1 개인정보 제3자 제공
인증 기준	개인정보를 제3자에게 제공하는 경우 법적 근거에 의하거나 정보주체의 동의를 받아야 하며, 제3자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호 대책을 수립·이행하여야 한다.
주요 확인사항	• 개인정보를 제3자에게 제공하는 경우 정보주체 동의, 법령상 의무준수 등 적법 요건을 명확히 식별하고 이를 준수하고 있는가? • 정보주체에게 개인정보 제3자 제공 동의를 받는 경우 관련 사항을 명확하게 고지하고 다른 동의 사항과 구분하여 적법하게 동의를 받고 있는가? • 정보주체에게 개인정보 제3자 제공 동의를 받는 경우 관련 내용을 명확하게 고지하고 법령에서 정한 중요한 내용에 대해 명확히 표시하여 알아보기 쉽게 하고 있는가? • 개인정보를 제3자에게 제공하는 경우 제공 목적에 맞는 최소한의 개인정보 항목으로 제한하고 있는가? • 개인정보를 제3자에게 제공하는 경우 안전한 절차와 방법을 통하여 제공하고 제공 내역을 기록하여 보관하고 있는가? • 제3자에게 개인정보의 접근을 허용하는 경우 개인정보를 안전하게 보호하기 위한 보호 절차에 따라 통제하고 있는가? • 정보주체의 동의 없이 개인정보의 추가적인 제공 시 당초 수집 목적과의 관련성, 예측 가능성, 이익 침해 여부, 안전성 확보조치 등의 고려사항에 대한 판단기준을 수립·이행하고, 추가적인 제공이 지속적으로 발생하는 경우 고려사항에 대한 판단기준을 개인정보처리방침에 공개하고 이를 점검하고 있는가?
기준 요약도	
운영 방안	◇ 개인정보를 제3자에게 제공하는 경우 정보주체 동의, 법령상 의무준수 등 적법

요건을 명확히 식별하고 이를 준수하고 있는가?

개인정보를 제3자에게 제공할 수 있는 경우

① 정보주체의 동의를 받은 경우

② 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우

③ 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우

④ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명·신체·재산의 이익을 위하여 필요하다고 인정되는 경우

⑤ 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우

⑥ 다른 법률에 특별한 규정이 있는 경우

◇ 정보주체에게 개인정보 제3자 제공 동의를 받는 경우 관련 사항을 명확하게 고지하고 다른 동의 사항과 구분하여 적법하게 동의를 받고 있는가?

개인정보의 제3자 제공 동의 시 알려야 할 사항

① 개인정보를 제공받는 자

② 개인정보를 제공받는 자의 개인정보 이용목적

③ 제공하는 개인정보의 항목

④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간

⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용

※ 출처: SK쉴더스 홈페이지 캡스홈 도어 가이드 온라인가입 화면 (SK쉴더스)

◇ 정보주체에게 개인정보 제3자 제공 동의를 받는 경우 관련 내용을 명확하게 고지하고 법령에서 정한 중요한 내용에 대해 명확히 표시하여 알아보기 쉽게 하고 있는가?

개인정보의 제3자 제공 동의는 수집·이용에 대한 동의 사항과 구분

① 제3자 제공 동의는 수집·이용에 대한 동의와 구분

※ 출처: SK쉴더스 홈페이지 캡스홈 도어 가이드 온라인가입 화면 (SK쉴더스)

② 제3자 제공에서 "선택 제공 동의" 거부 시에도 서비스 제공

1. 필수 제공 동의: 서비스 제공을 위해 필수적인 제공 동의
2. 선택 제공 동의: 사업자의 편의에 의한 제공 동의

◇ 개인정보를 제3자에게 제공하는 경우 제공 목적에 맞는 최소한의 개인정보 항목으로 제한하고 있는가?

목적에 맞는 최소한의 개인정보 제공

① 동의에 근거한 제3자 제공 시

1. 동의 시 고지한 제공 목적을 달성하기 위하여 필요한 최소한의 개인정보 항목만 제공

② 법령에 근거한 제3자 제공 시

1. 법률에서 구체적으로 명시
2. 해당 법령상 의무를 준수하기 위하여 필요한 범위 내에서 최소한의 개인정보 항목만 제공

◇ 개인정보를 제3자에게 제공하는 경우 안전한 절차와 방법을 통하여 제공하고 제공 내역을 기록하여 보관하고 있는가?

(예시) 개인정보 제3자 제공 시 안전한 절차

① 개인정보를 제공하는 자와 제공받는 자의 안전성 확보에 관한 책임관계 명확화(계약서 등)

② 제3자 제공과 관련된 승인 절차(담당자에 의한 제공 시)

③ 전송 또는 전달 과정의 암호화

④ 접근통제, 접근권한 관리 등 안전성 확보 조치 적용

⑤ 제공 기록의 보존 등

◇ 제3자에게 개인정보의 접근을 허용하는 경우 개인정보를 안전하게 보호하기 위한 보호절차에 따라 통제하고 있는가?

(예시) 제3자 제공 개인정보 보호절차

① 권한이 있는 자만 접근할 수 있도록 안전한 인증 및 접근통제 조치

② 전송구간에서의 도청을 방지하기 위한 암호화 조치

③ 책임 추적성을 확보할 수 있도록 접속기록 보존 등

◇ 정보주체의 동의 없이 개인정보의 추가적인 제공 시 당초 수집 목적과의 관련성, 예측 가능성, 이익 침해 여부, 안전성 확보조치 등의 고려사항에 대한 판단기준을 수립·이행하고, 추가적인 제공이 지속적으로 발생하는 경우

	고려사항에 대한 판단기준을 개인정보처리방침에 공개하고 이를 점검하고 있는가? **개인정보의 추가적인 제공 시 고려사항** ① 당초 수집 목적과 관련성이 있는지 여부 ② 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부 ③ 정보주체의 이익을 부당하게 침해하는지 여부 ④ 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

3.3.2 개인정보 처리 업무 위탁

세부분야	3.3.2 개인정보 처리 업무 위탁
인증 기준	개인정보 처리업무를 제3자에게 위탁하는 경우 위탁하는 업무의 내용과 수탁자 등 관련사항을 공개하여야 한다. 또한 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다.
주요 확인사항	• 개인정보 처리업무를 제3자에게 위탁(재위탁 포함)하는 경우 인터넷 홈페이지 등에 위탁하는 업무의 내용과 수탁자를 현행화하여 공개하고 있는가? • 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 서면, 전자우편, 문자전송 등의 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알리고 있는가?
기준 요약도	
운영 방안	**◇ 개인정보 처리업무를 제3자에게 위탁(재위탁 포함)하는 경우 인터넷 홈페이지 등에 위탁하는 업무의 내용과 수탁자를 현행화하여 공개하고 있는가?** **위탁 사실 공개** ① 위탁하는 업무의 내용 ② 개인정보 처리 업무를 위탁받아 처리하는 자

SK 쉴더스

blog

제4조(수집한 개인정보의 처리위탁)

① SK쉴더스는 다음과 같이 개인정보 처리업무를 위탁하고 있습니다. 향후 수탁자 및 위탁하는 업무의 내용이 변경될 경우 지체 없이 본 방침을 통해 고지하겠습니다. [상세보기]

다음과 같이 개인정보 처리 업무를 위탁합니다.

구분	수탁자	위탁업무
결제	토스페이먼츠(주)	카드이체 수금
	NICE 페이먼츠(주)	카드이체 수금
	효성에프엠에스(주)	계좌이체 수금
	효성타앤에스주식회사	전자세금계산서 발행
	엠지신용정보(주)	수납활동, 채권추심
	미래신용정보	채권추심

※ 출처: SK쉴더스 홈페이지 (SK쉴더스)

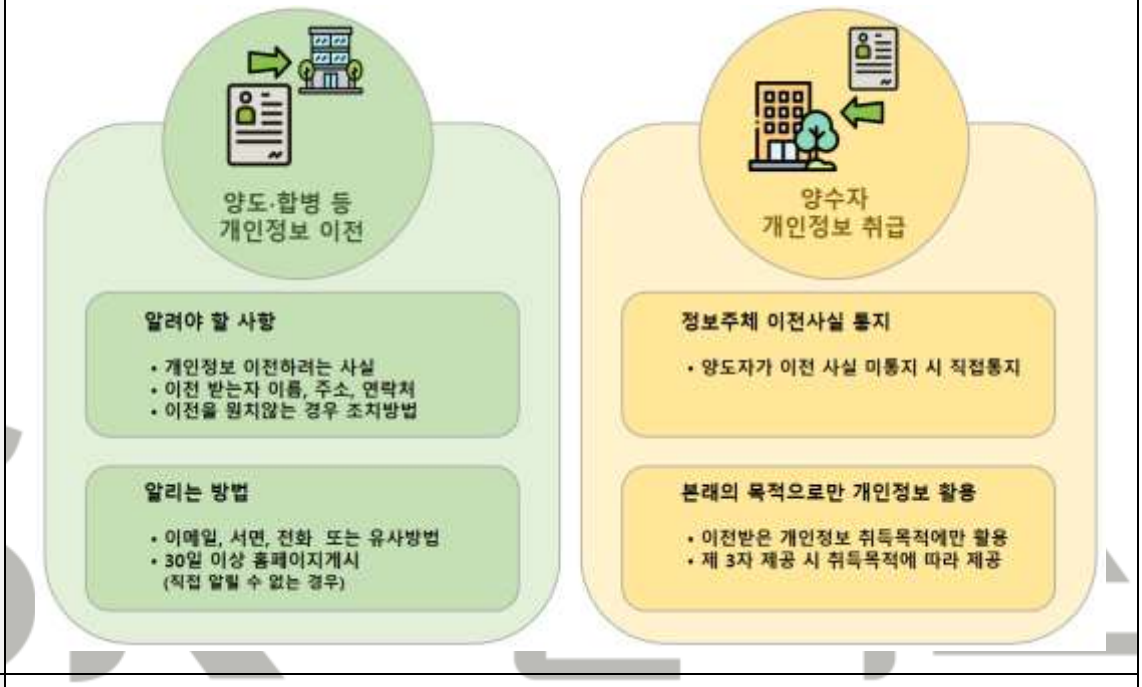
◇ 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 서면, 전자우편, 문자전송 등의 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알리고 있는가?

홍보 위탁 시 정보주체 고지

① 통지방법: 서면 등의 방법(서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법)

② 통지사항: 위탁하는 업무의 내용, 수탁자

3.3.3 영업의 양도 등에 따른 개인정보 이전

세부분야	3.3.3 영업의 양도 등에 따른 개인정보 이전
인증 기준	영업의 양도·합병 등으로 개인정보를 이전하거나 이전받는 경우 정보주체 통지 등 적절한 보호조치를 수립·이행하여야 한다.
주요 확인사항	• 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우 필요한 사항을 사전에 정보주체에게 알리고 있는가? • 개인정보를 이전받는 자는 법적 통지 요건에 해당될 경우 개인정보를 이전받은 사실 등 필요한 사항을 정보주체에게 지체 없이 알리고 있는가? • 개인정보를 이전받는 자는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공하고 있는가?
기준 요약도	
운영 방안	**◇ 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우 필요한 사항을 사전에 정보주체에게 알리고 있는가?** **양도·합병 등으로 정보주체(이용자)에게 알려야 하는 사항** ① 개인정보를 이전하려는 사실 ② 개인정보를 이전받는 자의 이름, 주소, 전화번호 및 그 밖의 연락처 ③ 개인정보의 이전을 원하지 않는 경우 조치할 수 있는 방법 및 절차

※ 출처: SK쉴더스 공식홈페이지 (SK쉴더스)

◇ 개인정보를 이전받는 자는 법적 통지 요건에 해당될 경우 개인정보를 이전받은 사실 등 필요한 사항을 정보주체에게 지체 없이 알리고 있는가?

개인정보를 이전받는 자의 통지요건 및 통지방법

① 개인정보 이전 사실 통지 요건

1. 양도자가 이전 사실을 정보주체에게 알린 경우 양수자는 추가로 알리지 않아도 됨.
2. 영업 양수 등에 따라 개인정보를 이전 받았으나 개인정보를 이전하는 자가 이전한 사실을 알리지 않은 경우, 이전 사실을 정보주체(이용자)에게 알려야 함.

② 통지 방법

1. 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법
2. 과실 없이 정보주체의 연락처를 알 수 없는 등의 이유로 정보주체에게 직접 알릴 수 없는 경우에는 인터넷 홈페이지에 30일 이상 기재

※ 출처: SK쉴더스 공식홈페이지 (SK쉴더스)

	◇ 개인정보를 이전받는 자는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공하고 있는가? **본래 이용 목적의 준수** ③ 개인정보를 이전받는 자는 이전 당시의 본래 목적 또는 법령에 명시된 범위 내에서만 개인정보를 이용·제공할 수 있음. 1. 별도의 추가 동의 없이 다른 목적으로 이용하거나 제3자에게 재제공 불가. 2. 단, 개인정보 보호법 등 관련 법령에 따라 추가 제공이 허용되는 예외 사유(법령상 의무 준수, 공익 목적 등)가 있는 경우에는 그 범위 내에서 가능

3.3.4 개인정보 국외 이전

세부분야	3.3.4 개인정보 국외 이전
인증 기준	개인정보를 국외로 이전하는 경우 국외 이전에 대한 동의, 관련 사항에 대한 공개 등 적절한 보호조치를 수립·이행하여야 한다.
주요 확인사항	• 개인정보를 국외로 이전하는 경우 정보주체에게 국외 이전에 관한 고지 사항을 모두 알리고 별도 동의를 받거나, 인증 또는 인정 등 적법 요건을 준수하고 있는가? • 정보주체와의 계약의 체결 및 이행을 위한 개인정보의 국외 처리위탁·보관에 대해 정보주체에게 알리는 경우 필요한 사항을 모두 포함하여 적절한 방법으로 알리고 있는가? • 개인정보보호 관련 법령 준수 및 개인정보보호 등에 관한 사항을 포함하여 국외 이전에 관한 계약을 체결하고 있는가? • 개인정보를 국외로 이전하는 경우 개인정보보호를 위하여 필요한 조치를 취하고 있는가?
기준 요약도	

운영 방안	**◇ 개인정보를 국외로 이전하는 경우 정보주체에게 국외 이전에 관한 고지 사항을 모두 알리고 별도 동의를 받거나, 인증 또는 인정 등 적법 요건을 준수하고 있는가?** **개인정보 국외 이전 요건** ① 별도 동의 1. 정보주체로부터 국외 이전에 관한 별도의 동의를 받은 경우 - 이전되는 개인정보 항목 - 개인정보가 이전되는 국가, 시기 및 방법 - 개인정보를 이전받는 자의 성명(법인인 경우 그 명칭과 연락처) - 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간' - 개인정보의 이전을 거부하는 방법, 절차 및 거부의 효과 ② 법률, 조약 등 근거 1. 법률, 대한민국을 당사자로 하는 조약 또는 그 밖의 국제협정에 개인정보의 국외 이전에 관한 특별한 규정이 있는 경우 ③ 개인정보 처리방침 공개(처리위탁 보관) 1. 정보주체와의 계약의 체결 및 이행을 위하여 개인정보의 처리위탁· 보관이 필요한 경우 - 관련 사항을 개인정보 처리방침에 공개하거나 전자우편 등으로 정보주체에게 알린 경우 ④ 인증 1. 개인정보 보호 인증(ISMS-P 인증) 등 보호위원회가 정하여 고시하는 인증을 받은 경우로서 다음 조치를 모두 한 경우 - 개인정보 보호에 필요한 안전조치 및 정보주체 권리보장에 필요한 조치 나. 인증받은 사항을 개인정보가 이전되는 국가에서 이행하기 위하여 필요한 조치 ⑤ 대상국 등 인정 요건 1. 이전되는 국가 또는 국제기구의 개인정보 보호체계, 정보주체 권리보장 범위, 피해구제 절차 등이 이 법에 따른 개인정보 보호 수준과 실질적으로 동등한 수준을 갖추었다고 보호위원회가 인정하는 경우 **◇ 정보주체와의 계약의 체결 및 이행을 위한 개인정보의 국외 처리위탁·보관에 대해 정보주체에게 알리는 경우 필요한 사항을 모두 포함하여 적절한 방법으로 알리고 있는가?**

이용자에게 알려야 할 사항

① 개인정보의 국외 이전(제공, 위탁, 보관)은 개인정보 관련 보호 체계가 다른 제3의 국가로 개인정보가 옮겨지는 것으로, 정보주체의 권리를 침해할 위험성이 높으므로, 개인정보의 제3자 제공, 위탁과 구분하여 처리방침에 기재하는 것을 권장

개인정보의 국외 이전

〈○○ 여행사〉은(는) ○○ 업무를 국외 법인인 ○○○○에 아래와 같이 위탁하고 있습니다.

1. 수탁업체: ○○○○ 법인
2. 수탁업체의 위치: ○국 ○시 ○구 ○동 건물명(국가, 도시 등 구체적 주소 작성)
3. 위탁 일시 및 방법: ○년 ○월 ○일 전용네트워크를 이용한 원격지 전송
4. 정보관리책임자의 연락처 : 전자우편 주소, 전화번호
5. 위탁하는 개인정보 항목 : 〈개인정보처리자의 위탁하는 개인정보의 항목〉복구에 필요한 이용자 데이터(○, ○, ○)
6. 위탁 업무 내용 : 〈개인정보처리자의 위탁하는 개인정보 처리업무〉 재난, 재해 등으로부터 이용자 데이터 보호를 위한 국가간 데이터 백업(보관)
7. 개인정보의 보유 및 이용기간 : ○년 ○월까지

※ 출처: 개인정보처리방침 작성지침-여행편 (개인정보보호위원회)

◇ 개인정보보호 관련 법령 준수 및 개인정보보호 등에 관한 사항을 포함하여 국외 이전에 관한 계약을 체결하고 있는가?

개인정보보호법 중 국외이전 관련 사항

「**개인정보보호법**」 제28조의8 4항(개인정보의 국외 이전)

④ 개인정보처리자는 제1항 각 호 외의 부분 단서에 따라 개인정보를 국외로 이전하는 경우 국외 이전과 관련한 이 법의 다른 규정, 제17조부터 제19조까지의 규정 및 제5장의 규정을 준수하여야 하고, 대통령령으로 정하는 보호조치를 하여야 한다.

「**개인정보보호법 시행령**」 제29조의10(개인정보의 국외 이전 시 보호조치 등)

① 개인정보처리자는 법 제28조의8제1항 각 호 외의 부분 단서에 따라 개인정보를 국외로 이전하는 경우에는 같은 조 제4항에 따라 다음 각 호의 보호조치를 해야 한다.

1. 제30조제1항에 따른 개인정보 보호를 위한 안전성 확보 조치
2. 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 조치
3. 그 밖에 정보주체의 개인정보 보호를 위하여 필요한 조치

② 개인정보처리자는 법 제28조의8제1항 각 호 외의 부분 단서에 따라 개인정보를 국외로 이전하는 경우에는 제1항 각 호의 사항에 관하여 이전받는 자와 미리 협의하고 이를 계약내용 등에 반영해야 한다.

	◇ 개인정보를 국외로 이전하는 경우 개인정보보호를 위하여 필요한 조치를 취하고 있는가? **(예시) 개인정보 국외 이전 시 보호조치** ① 안전성 확보조치 1. 전송 단계 및 저장 시 암호화 2. 접근통제(권한 관리, 인증·인가) 3. 침입 탐지·로그 관리 4. 정기적 보안 감사·위험성 평가 5. 클라우드 보안제공사항 점검 및 문서화 등

3.4 개인정보 파기 시 보호조치

3.4.1 개인정보 파기

세부분야	3.4.1 개인정보 파기
인증 기준	개인정보의 보유기간 및 파기 관련 내부 정책을 수립하고 개인정보의 보유기간 경과, 처리목적 달성 등 파기 시점이 도달한 때에는 파기의 안전성 및 완전성이 보장될 수 있는 방법으로 지체 없이 파기하여야 한다.
주요 확인사항	• 개인정보의 보유기간 및 파기와 관련된 내부 정책을 수립하고 있는가? • 개인정보의 처리목적이 달성되거나 보유기간이 경과한 경우 지체 없이 해당 개인정보를 파기하고 있는가? • 개인정보를 파기할 때에는 복구·재생되지 않도록 안전한 방법으로 파기하고 있는가? • 개인정보 파기에 대한 기록을 남기고 관리하고 있는가?
기준 요약도	
운영 방안	**◇ 개인정보의 보유기간 및 파기와 관련된 내부 정책을 수립하고 있는가?** **개인정보 파기 정책수립** ① 수집 항목, 수집 목적, 수집 경로별 보관 장소(데이터베이스, 백업데이터 등), 파기방법, 파기시점 법령근거 등 현황 관리

수집 항목

평가 업무명	수집					
	수집 항목	수집 경로	수집 대상	수집 주기	수집담당자	수집 근거
민원 처리	(필수) 성명, 주민등록번호, 전화번호, 이메일 주소, 민원 내용 (선택) 집전화번호	온라인 (홈페이지)	민원인	상시	-	이용자 동의/ OO법제0조0항 (주민등록번호)
		오프라인 (민원신청서 작성)	민원인	상시	안내창구 담당자	이용자 동의/ OO법제0조0항 (주민등록번호)

파기 절차

파기			
보관 기간	파기 담당자	파기 절차	분리 보관 여부
민원 처리 완료 후 1년	DB 관리자	일단위 DB 파기	별도 보존DB 구성
민원DB 입력 후 스캔 후 파기	통계 담당자	주단위 문서 절단	-

※ 출처: 개인정보 영향평가 수행안내서 (개인정보보호위원회•KISA)

◇ 개인정보의 처리목적이 달성되거나 보유기간이 경과한 경우 지체 없이 해당 개인정보를 파기하고 있는가?

(예시) 개인정보 기한 경과 및 목적 달성 시 파기기준 수립

① 간편 상담 업무 목적 개인정보 "이름", "전화번호" 수집 6개월 보관 삭제

※ 출처: SK쉴더스 대표홈페이지 간편상담 신청 (SK쉴더스)

※ 출처: SK쉴더스 대표홈페이지 개인정보처리방침 (SK쉴더스)

◇ 개인정보를 파기할 때에는 복구·재생되지 않도록 안전한 방법으로 파기하고 있는가?

개인정보 파기방법

① 하드 디스크 등 매체 전체의 데이터를 파기하는 경우

1. 논리적 파기

- 하드디스크, USB 메모리의 경우 '로우레벨포멧(Low level format)' 방법으로 파기

2. 물리적 파기

- 데이터가 저장되는 디스크 플레터에 강력한 힘으로 구멍을 내어 복구가 불가능하도록 하는 천공 방법으로 파기
- CD/DVD의 경우 가위 등으로 작은 입자로 조각 내거나, 전용 CD파쇄기나 CD 파쇄가 가능한 문서파쇄기 등을 이용하여 파기
- 고온에 불타는 종류의 매체는 소각하는 방법으로 파기
- 자기장치를 이용해 강한 자기장으로 데이터를 복구 불가능하게 하는 디가우저 파기

② 고객 서비스에 이용 중인 DB서버에 저장된 일부 데이터를 파기하는 경우

1. 서비스 중인 DB의 해당 개인정보 위에 임의의 값(Null값 등)을 덮어쓰기 한 후 삭제
2. DB의 특정부분에 덮어쓰기가 곤란한 경우에는 테이블 데이터에 대한 논리적인

삭제(delete)도 허용되나, 신속하게 다른 데이터로 덮어쓰기 될 수 있도록 운영

◇ 개인정보 파기에 대한 기록을 남기고 관리하고 있는가?

개인정보 파기 기록

① 개인정보 파기 시행 및 파기 결과 확인

1. 개인정보보호책임자 책임 하에 수행

② 파기 관리대장 기록 및 증적기록물 보관

③ 공공기관의 경우 개인정보파일 파기 관리대장 작성

1. 구분(이용·제공·열람·파기)
2. 일시
3. 파일명/형태
4. 담당자
5. 목적/사유
6. 이용·제공받은 제3자/열람 등 요구자
7. 이용·제공 형태
8. 기간 등

개인정보 파기 관리대장

번호	개인정보파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장

※ 개인정보 파기 관리대장 (이해를 돕기 위한 예시)

3.4.2 처리목적 달성 후 보유 시 조치

세부분야	3.4.2 처리목적 달성 후 보유 시 조치
인증 기준	개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 않고 보존하는 경우에는 해당 목적에 필요한 최소한의 항목으로 제한하고 다른 개인정보와 분리하여 저장·관리하여야 한다.
주요 확인사항	• 개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 않고 보존하는 경우, 관련 법령에 따른 최소한의 기간으로 한정하여 최소한의 정보만을 보존하도록 관리하고 있는가? • 개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 않고 보존하는 경우 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장·관리하고 있는가? • 분리 보관하고 있는 개인정보에 대하여 법령에서 정한 목적 범위 내에서만 처리 가능하도록 관리하고 있는가? • 분리 보관하고 있는 개인정보에 대하여 접근권한을 최소한의 인원으로 제한하고 있는가?
기준 요약도	
운영 방안	**◇ 개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 않고 보존하는 경우, 관련 법령에 따른 최소한의 기간으로 한정하여 최소한의 정보만을 보존하도록 관리하고 있는가?** **(예시) 타 법령에 따른 보유 시 최소한의 정보만 보존**

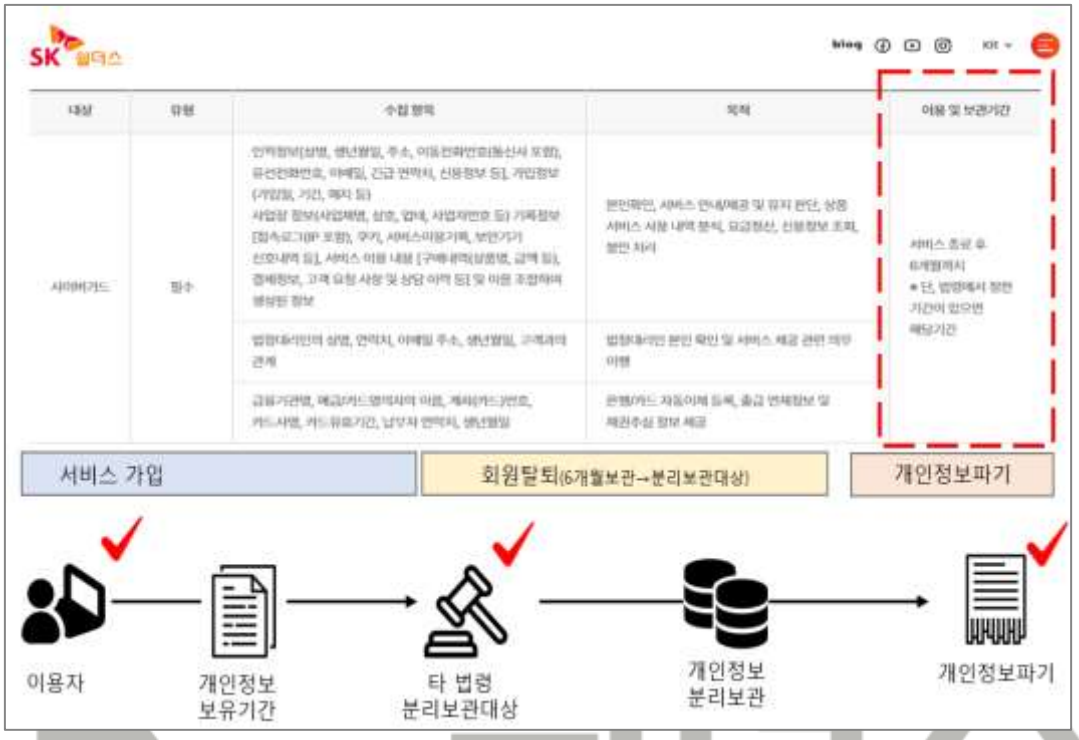
① 보존 근거 확인

1. 관련 법령(세법, 상법, 전자금융거래법 등)에서 요구하는 보존 항목과 기간 파악

② 최소화 원칙 적용

1. 타 법령에 의한 보존 항목 중 반드시 필요한 정보(예: 거래일시, 금액, 거래 상대)만 선별

2. 개인 식별이 불필요한 정보는 익명화·비식별화 처리 후 보존



※ 출처: SK쉴더스 공식 홈페이지 (SK쉴더스)

전자상거래 등에서의 소비자보호에 관한 법률 시행령 (약칭: 전자상거래법 시행령)

[시행 2021. 3. 2.] [대통령령 제31516호, 2021. 3. 2., 타법개정]

제6조(사업자가 보존하는 거래기록의 대상 등) ① 법 제6조제3항에 따라 사업자가 보존하여야 할 거래기록의 대상 · 범위 및 기간은 다음 각 호와 같다. 다만, 법 제20조제1항에 따른 통신판매중개자(이하 "통신판매중개자"라 한다)는 자신의 정보처리시스템을 통하여 처리한 기록의 범위에서 다음 각 호의 거래기록을 보존하여야 한다. <개정 2016. 9. 29.>

1. 표시 · 광고에 관한 기록: 6개월
2. 계약 또는 청약철회 등에 관한 기록: 5년
3. 대금결제 및 재화등의 공급에 관한 기록: 5년
4. 소비자의 불만 또는 분쟁처리에 관한 기록: 3년

※ 출처: 국가법령정보센터 (https://www.law.go.kr)

◇ 개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 않고 보존하는 경우 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여 저장·관리하고 있는가?

(예시) 개인정보 분리보관

① 물리적·논리적 분리

1. 별도 DB·서버, 컨테이너 분리 등
2. 운영 데이터와 완전 분리된 스토리지·폴더 구조 구축

② 식별자 관리

1. 분리 보관 대상 파일 내 주요 식별자(암호화 된 주민등록번호 등)는 별도 키 관리 시스템에서 분리

- 키 접근은 별도 권한·로그로 통제

③ 분리 데이터베이스에 대한 접속기록을 남기고 정기적으로 검토

◇ 분리 보관하고 있는 개인정보에 대하여 법령에서 정한 목적 범위 내에서만 처리 가능하도록 관리하고 있는가?

분리 보관 관련 규정 확인

① 전자상거래 등에서 소비자 보호에 관한 법률

1. 표시·광고에 관한 기록: 6개월
2. 계약 또는 청약철회 등에 관한 기록: 5년
3. 대금결제 및 재화 등의 공급에 관한 기록: 5년
4. 소비자의 불만 또는 분쟁처리에 관한 기록: 3년 법령에서 정한 목적 범위 내에서만 처리

⑤ 국세기본법

1. 모든 거래에 관한 장부 및 증거서류 : 과세기간 신고기한 지난 날부터 5년

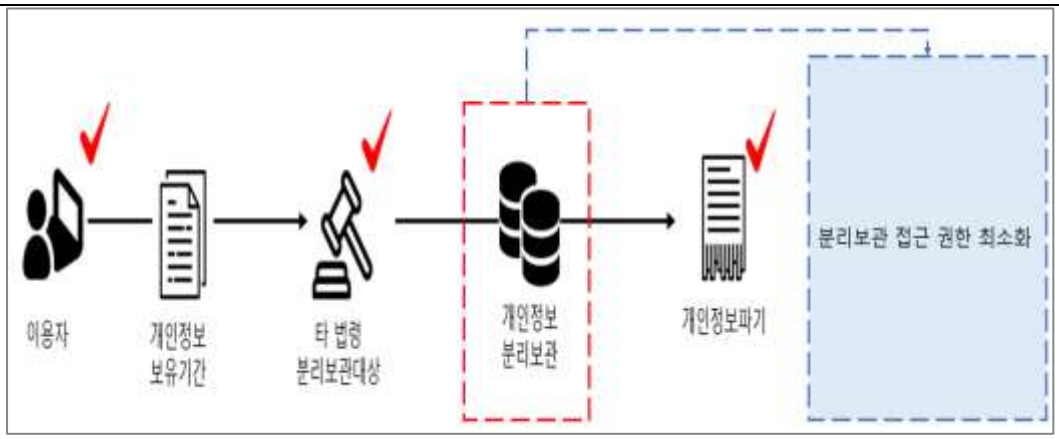
- 역외거래의 경우: 7년

◇ 분리 보관하고 있는 개인정보에 대하여 접근권한을 최소한의 인원으로 제한하고 있는가?

분리보관 개인정보 접근제한

① 분리 데이터베이스의 접속 권한을 최소인원으로 제한하는 등 접근권한 최소화

② 분리 데이터베이스에 대한 접속기록을 남기고 정기적으로 검토



※ 법령에 의한 개인정보 분리보관 시 보호조치 (이해를 돕기 위한 예시)

3.5 정보주체 권리보호

3.5.1 개인정보처리방침 공개

세부분야	3.5.1 개인정보처리방침 공개
인증 기준	개인정보의 처리 목적 등 필요한 사항을 모두 포함하여 정보주체가 알기 쉽도록 개인정보처리방침을 수립하고, 이를 정보주체가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하고 지속적으로 현행화하여야 한다.
주요 확인사항	• 개인정보처리방침에는 법령에서 요구하는 내용을 모두 포함하여 알기 쉬운 용어로 구체적이고 명확하게 작성하였는가? • 개인정보처리방침을 정보주체가 쉽게 확인할 수 있도록 인터넷 홈페이지 등에 지속적으로 현행화하여 공개하고 있는가? • 개인정보처리방침이 변경되는 경우 사유 및 변경 내용을 지체 없이 공지하고 정보주체가 언제든지 변경된 사항을 쉽게 알아볼 수 있도록 조치하고 있는가?
기준 요약도	
운영 방안	**◇ 개인정보처리방침에는 법령에서 요구하는 내용을 모두 포함하여 알기 쉬운 용어로 구체적이고 명확하게 작성하였는가?** **개인정보처리방침에 포함하여야 할 필수 사항** ① 개인정보의 처리 목적 ② 개인정보의 처리 및 보유 기간 ③ 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다) 3의 2. 개인정보의 파기절차 및 파기방법(제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다) 3의 3. 제23조제3항에 따른 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당되는 경우에만 정한다) ④ 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)

4의 2. 제28조의2 및 제28조의3에 따른 가명정보의 처리 등에 관한 사항(해당되는 경우에만 정한다)

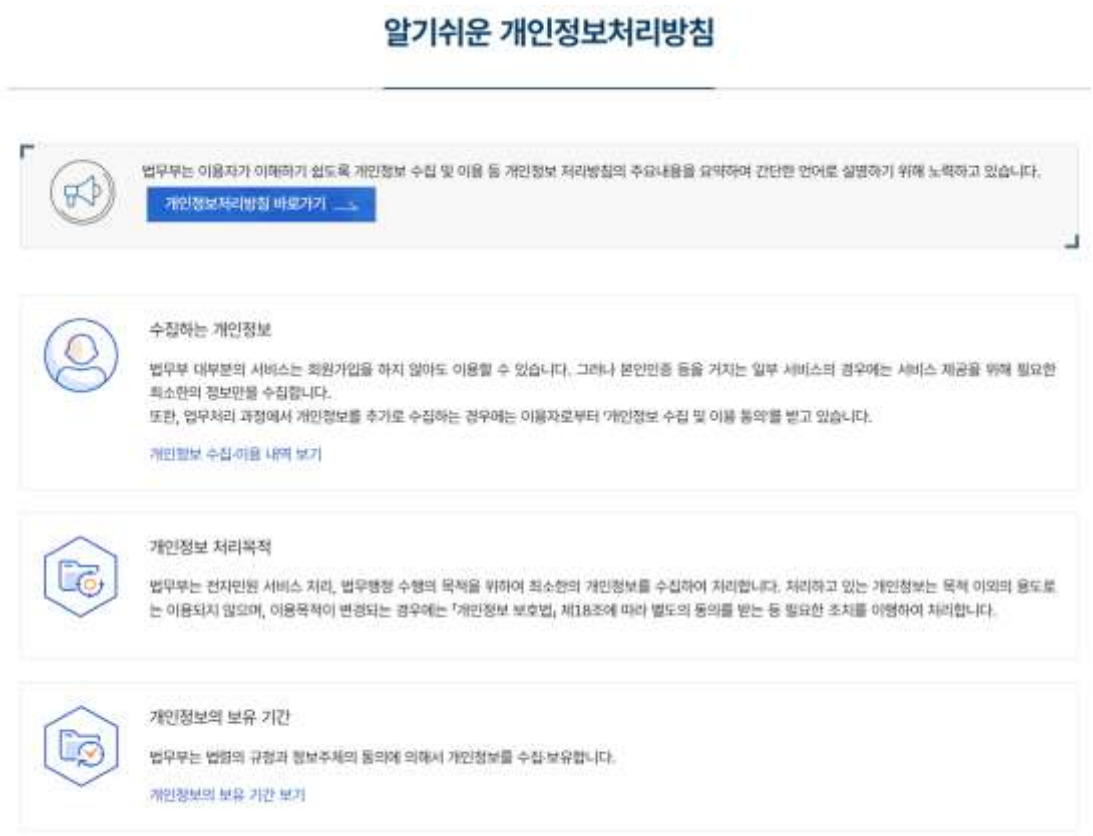
⑤ 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항

⑥ 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처

⑦ 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)

⑧ 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항

(예시) 알기쉬운 개인정보처리방침



※ 출처: 법무부. 알기쉬운 개인정보처리방침 (moj.go.kr)

◇ 개인정보처리방침을 정보주체가 쉽게 확인할 수 있도록 인터넷 홈페이지 등에 지속적으로 현행화하여 공개하고 있는가?

개인정보처리방침 공개방법

① 인터넷 홈페이지 첫 화면 또는 첫 화면과의 연결화면을 통하여 지속적으로 게재

② 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분

③ "개인정보처리방침"이라는 표준화된 명칭을 사용

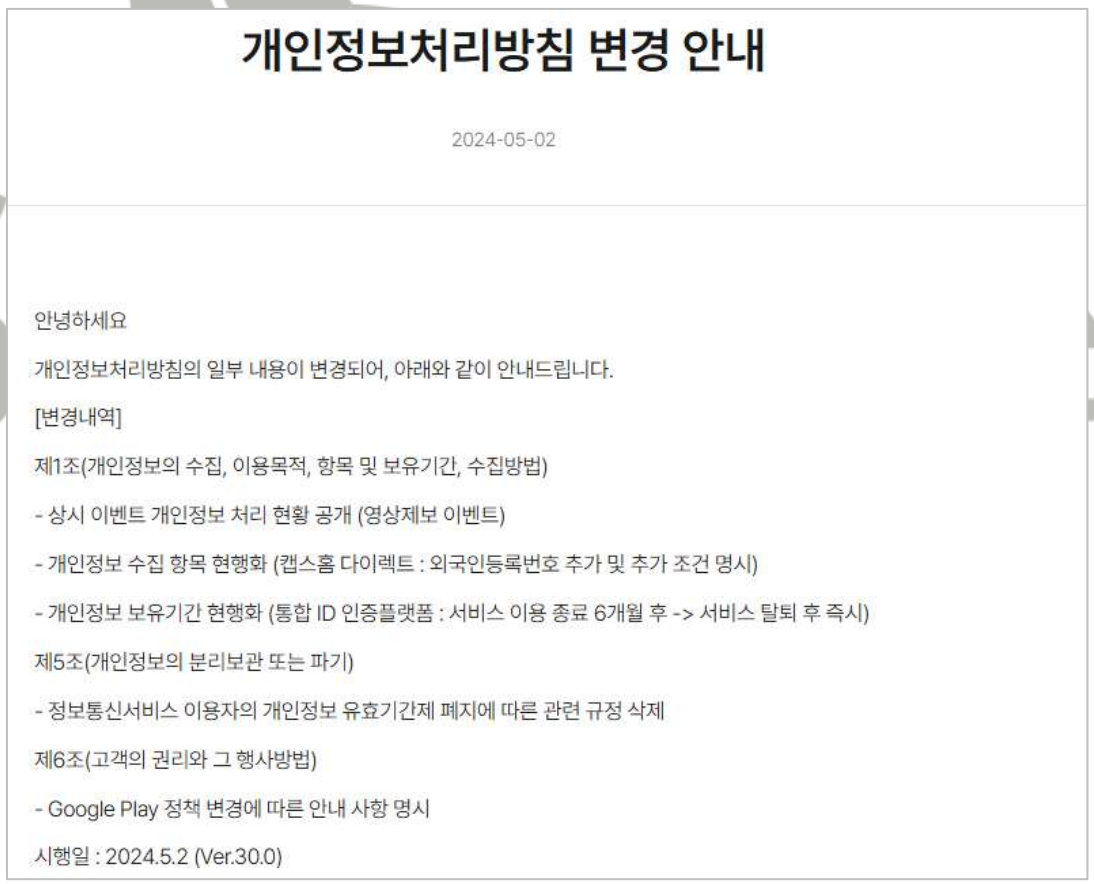
※ 출처: SK쉴더스 홈페이지 (SK쉴더스)

◇ 개인정보처리방침이 변경되는 경우 사유 및 변경 내용을 지체 없이 공지하고 정보주체가 언제든지 변경된 사항을 쉽게 알아볼 수 있도록 조치하고 있는가?

개인정보 변경 내용공지

① 개인정보처리방침이 변경되는 경우 사유 및 변경 내용 공지

1. 인터넷 홈페이지의 첫 화면의 공지사항란 또는 별도의 창을 통하여 공지하는 방법
2. 서면·모사전송·전자우편 또는 이와 비슷한 방법으로 이용자에게 공지하는 방법
3. 점포·사무소 안의 보기 쉬운 장소에 써 붙이거나 비치하는 방법



개인정보처리방침 변경 안내

2024-05-02

안녕하세요

개인정보처리방침의 일부 내용이 변경되어, 아래와 같이 안내드립니다.

[변경내역]

제1조(개인정보의 수집, 이용목적, 항목 및 보유기간, 수집방법)

- 상시 이벤트 개인정보 처리 현황 공개 (영상제보 이벤트)

- 개인정보 수집 항목 현행화 (캡스홈 다이렉트 : 외국인등록번호 추가 및 추가 조건 명시)

- 개인정보 보유기간 현행화 (통합 ID 인증플랫폼 : 서비스 이용 종료 6개월 후 -> 서비스 탈퇴 후 즉시)

제5조(개인정보의 분리보관 또는 파기)

- 정보통신서비스 이용자의 개인정보 유효기간제 폐지에 따른 관련 규정 삭제

제6조(고객의 권리와 그 행사방법)

- Google Play 정책 변경에 따른 안내 사항 명시

시행일 : 2024.5.2 (Ver.30.0)

※ 출처: SK쉴더스 홈페이지 (SK쉴더스)

② 변경된 사항을 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개

※ 출처: SK쉴더스 홈페이지 (SK쉴더스)

3.5.2 정보주체 권리보장

세부분야	3.5.2 정보주체 권리보장
인증 기준	정보주체가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 등 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체의 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다.
주요 확인사항	• 정보주체 또는 그 대리인이 개인정보에 대한 열람, 정정·삭제, 처리정지 및 동의 철회 등(이하 '열람등요구'라 함)을 개인정보 수집방법·절차보다 어렵지 아니하도록 권리 행사 방법 및 절차를 마련하여 공개하고 있는가? • 정보주체 또는 그 대리인이 열람등요구를 하는 경우 규정된 기간 내에 열람등요구에 따른 필요한 조치를 하고 있는가? • 정보주체 또는 그 대리인이 개인정보 수집·이용·제공 등의 동의를 철회하는 경우 지체 없이 수집된 개인정보를 파기하는 등 필요한 조치를 취하고 있는가? • 정보주체의 열람 등 요구에 대한 조치에 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하여 안내하고 있는가? • 정보주체의 열람 등 요구 및 처리 결과에 대하여 기록을 남기고 있는가? • 정보통신망에서 사생활 침해 또는 명예훼손 등 타인의 권리를 침해한 경우 침해를 받은 자가 정보통신서비스 제공자에게 정보의 삭제 요청 등을 할 수 있는 절차를 마련하여 시행하고 있는가?
기준 요약도	

운영 방안

◇ 정보주체 또는 그 대리인이 개인정보에 대한 열람, 정정·삭제, 처리정지 및 동의 철회 등(이하 '열람등요구'라 함)을 개인정보 수집방법·절차보다 어렵지 아니하도록 권리 행사 방법 및 절차를 마련하여 공개하고 있는가?

열람, 정정, 삭제, 처리정지, 이의제기, 동의철회 등의 방법 공개

① 정보주체에게 구체적인 방법과 절차를 공개

② 다양한 권리 행사 방법을 마련하여 제공

③ 열람 등을 요구한 자가 본인이거나 정당한 대리인인지 확인 수단 적용

제6조(고객의 권리와 그 행사방법)

① 고객은 SK쉴더스가 처리하는 정보들에 대하여 자신 및 14세 미만 아동(법정대리인인 해당)의 개인정보의 열람•제공을 아래 제9조에 명시된 연락처로 요구할 수 있습니다. 세부적인 정보는 아래와 같습니다.

1. 본 처리방침 제1조(수집하는 개인정보의 목적, 항목 및 수집방법, 보유 및 이용기간)에 명시한 정보
2. 제3조(개인정보의 제3자 제공)에 명시한 정보
3. 제4조(수집한 개인정보의 위탁)에 명시한 정보
4. 제8조(인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항)에 명시한 정보
5. 고객님께서 개인정보 수집·이용·제공에 동의하신 현황

② 자신의 개인정보를 열람한 고객은 사실과 다르거나 확인할 수 없는 개인정보에 대하여 SK쉴더스에 정정 또는 삭제를 요구할 수 있습니다. 다만, 다른 법령에서 그 개인정보가 보존 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없습니다.

③ 고객은 SK쉴더스에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있습니다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 SK쉴더스는 해당 사유를 고객에게 알리고, 처리정지 요구를 거절할 수 있습니다.

1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
2. 다른 사람의 생명•신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 개인정보를 처리하지 아니하면 고객과 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 고객이 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우

※ 출처: SK쉴더스 홈페이지(SK쉴더스)

◇ 정보주체 또는 그 대리인이 열람등요구를 하는 경우 규정된 기간 내에 열람등요구에 따른 필요한 조치를 하고 있는가?

(예시) 열람 등 요구에 따른 조치

① 처리 기간:

1. 요청 접수일부터 10일 이내 완료
2. 부득이한 사유가 있으면 최대 10일 추가 연장 가능

- 연장 사유·기간 정보주체에 통지

② 절차:

1. 본인확인 후 즉시 조회 권한 부여 또는 별도 뷰어 제공
2. 요청 범위(전체·부분열람) 및 제공 방식(다운로드·화면 표시) 선택

개인정보 전송요구권

① 개인정보 전송요구권의 정의 및 법적 근거

1. 개인정보 보호법 제35조의2(개인정보의 전송 요구) 근거

- 정보주체가 개인정보처리자에게 자신의 개인정보를 컴퓨터로 처리 가능한 형태로 자신 또는 제3자에게 전송하도록 요구할 수 있는 권리

② 전송요구권의 구분

1. 본인전송 요구

- 정보주체가 자신의 개인정보를 본인에게 직접 전송하도록 요구하는 권리

2. 제3자전송 요구

- 개인정보관리 전문기관이나 일반수신자에게 정보를 전송하도록 요구하는 권리

③ 대상 개인정보의 요건

1. 전송 요구 대상이 되는 개인정보는 다음 요건을 모두 충족해야 함.

- 정보주체 본인에 관한 개인정보로서 다음 중 하나에 해당할 것:
- 정보주체의 동의를 받아 처리되는 개인정보
- 계약의 체결·이행을 위해 처리되는 개인정보
- 정보주체의 이익이나 공익적 목적을 위해 보호위원회가 지정한 개인정보
- 개인정보처리자가 수집한 정보를 기초로 분석·가공하여 별도로 생성한 정보가 아닐 것
- 컴퓨터 등 정보처리장치로 처리되는 개인정보일 것

2. 전송 요구 제외 대상

- 제3자의 권리나 정당한 이익을 침해하는 정보
- 일방향 암호화하여 저장된 정보
- 시간·비용·기술 등을 고려 시 합리적 범위를 벗어나는 정보
- 정보전송자가 시스템 내부 관리 목적으로 보유하는 등 명백히 정보주체의 권리와 관련성이 없는 정보

④ 정보전송자

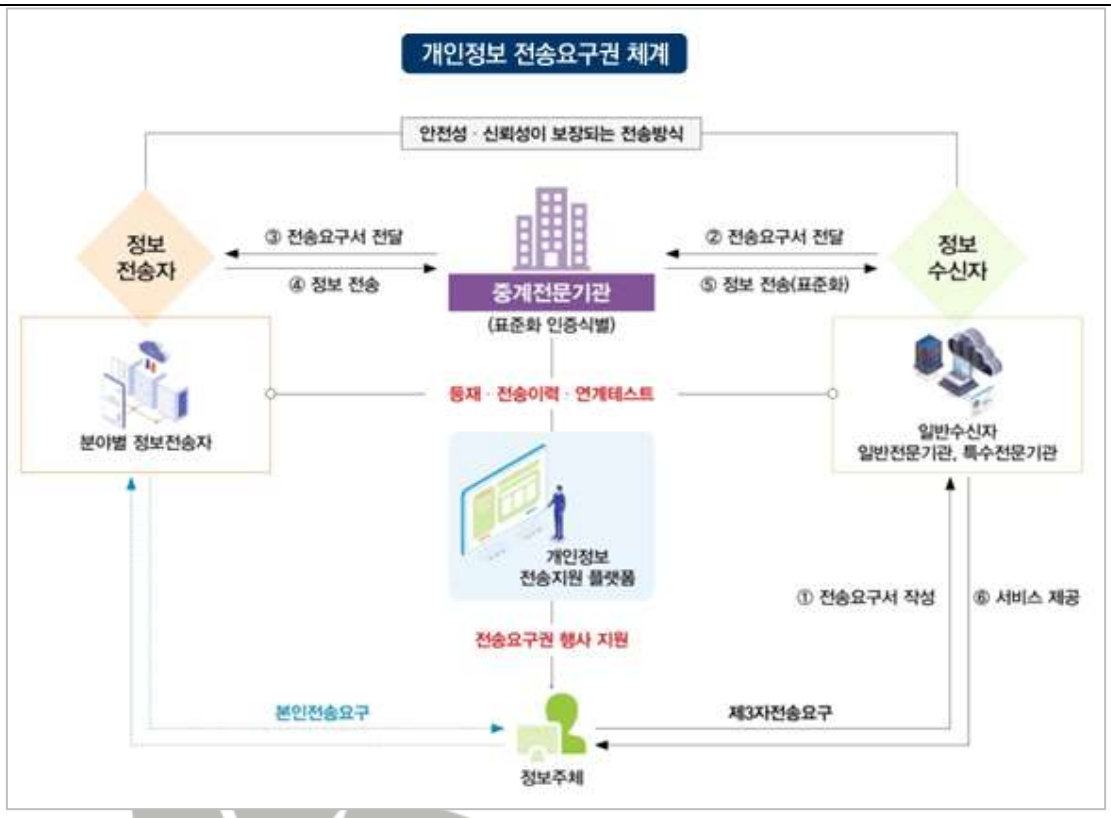
1. 정보전송자 기준

- 정보주체 수가 10만 명 이상인 대기업·중견기업
- 정보주체 수가 100만 명 이상인 기관·법인·단체
- 제3자전송 요구 대상(보건의료, 통신, 에너지 분야부터 우선 시행 중)
- 향후 유통 등 다른 분야로 확대 예정

2. 정보수신자

1. 개인정보관리 전문기관
2. 중계전문기관: 개인정보 전송 중계 기능 제공
3. 일반전문기관: 보건의료전송정보 외 개인정보 관리·분석
4. 특수전문기관: 보건의료전송정보 관리·분석

	5. 일반수신자 :고유 업무 수행 과정에서 수집한 정보의 진위 여부 등을 확인하기 위해 정보를 전송받는 자 ⑤ 전송요구 절차 및 방법 1. 본인전송 요구 절차 - 요구 방법: 정보전송자가 인터넷 홈페이지에 게재한 방법에 따라 요구 - 특정 사항: 전송 요구 목적과 전송을 원하는 개인정보 항목 특정 - 전송 형식: PDF, XLS, CSV, HTML, JSON 등 컴퓨터로 편집 가능한 파일 형식 - 대리인 행사: 정보주체는 대리인을 통해서도 권리 행사 가능 2. 제3자전송 요구 절차 - 전송요구서 작성: 전송 요구 목적, 정보전송자 및 정보수신자, 전송을 요구하는 개인정보, 정기적 전송 요구 여부 및 주기, 전송 요구 종료시점, 보유 및 이용기간 3. 정기 전송: 일반전문기관 및 특수전문기관에 대해 1주일~1개월 사이의 주기로 정기적 전송 요구 가능 ⑥ 안전성 및 보안 조치 1. 정보전송자의 의무 - 본인확인: 정보주체 본인 여부 또는 정당한 대리인인지 반드시 확인 - 암호화 전송: SSL/TLS와 같은 안전한 암호 알고리즘으로 암호화하여 전송 - 보안조치: 크리덴셜 스터핑, 심 스와핑 등 침해 위협에 대응하는 방안 마련 2. 권장 보안 조치 - 다중 인증(MFA): 휴대폰 인증 외 보조적 여러 인증 수단 제공 - 캡챠(CAPTCHA) 적용 - 비정상 로그인 시도 탐지 및 차단 등 ⑦ 전송 기한 및 거절 사유 1. 전송 기한 - 정보전송자는 정당한 사유가 없는 한 지체 없이 개인정보를 전송해야 하며, 지연 사유발생 시 정보주체에게 통지해야 함. 2. 전송 거절·중단 사유 - 본인 또는 대리인 여부가 확인되지 않는 경우 - 제3자 기망·협박에 의한 전송요구로 의심되는 경우 - 전송 요구 사항이 특정되지 않은 경우 - 열람 제한·거절 사유에 해당하는 경우



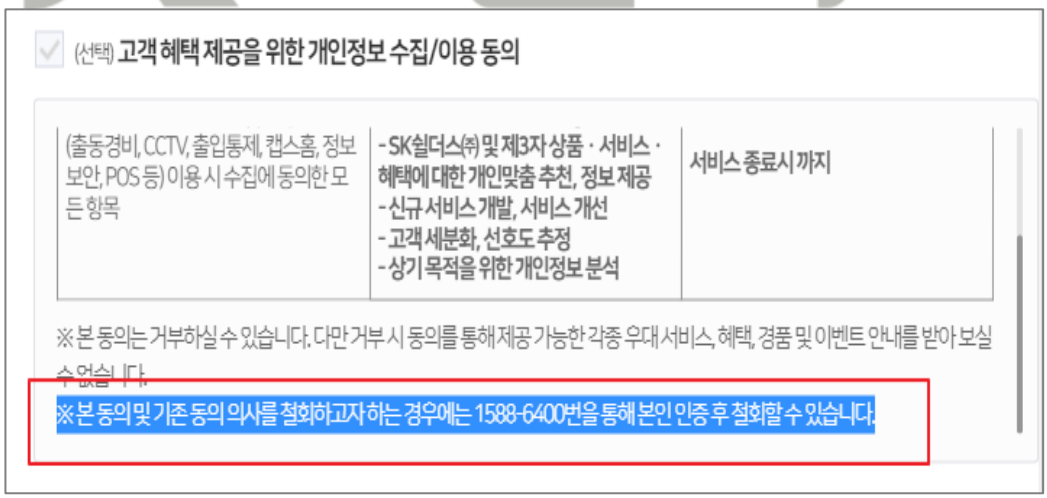
※ 출처 : 개인정보 전송요구권 체계 (개인정보보호위원회)

◇ 정보주체 또는 그 대리인이 개인정보 수집·이용·제공 등의 동의를 철회하는 경우 지체 없이 수집된 개인정보를 파기하는 등 필요한 조치를 취하고 있는가?

동의 철회 시 조치

① 동의 철회 방법 제공

1. 동의 철회 시 홍보 마케팅·제3자 제공 등 개인정보가 활용되지 않도록 조치



※ 출처: SK쉴더스 홈페이지 캡스홈 도어 가이드 온라인가입 화면 (SK쉴더스)

※ 출처: SK쉴더스 모바일가드 스마트폰 앱 (SK쉴더스)

◇ 정보주체의 열람요구에 대한 조치에 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하여 안내하고 있는가?

(예시) 이의제기 방법 안내 및 접근성 확보

① 온라인: 전용 이의제기 양식, FAQ, 챗봇 또는 1:1 문의 게시판

② 오프라인: 서면, 팩스, 이메일 주소, 콜센터 전화번호

개인정보 열람 등 요구 결정 이의신청서

접수번호		접수일		처리기간	
정보주체	성명		전화번호		
	생년월일		주소		
대리인	성명		전화번호		
	생년월일		정보주체와의 관계		
	주소				
이의신청 내용					

개인정보보호법 제38조제5항에 따라 개인정보 열람등 요구 통지결과에 대한 이의를 위와같이 작성하여 제출합니다

OOOO 년 OO 월 O일

OOO (서명 또는 인)

※ 개인정보 열람 등 요구결정 이의신청서(이해를 돕기 위한 예시)

◇ 개인정보 열람 등의 요구 및 처리 결과에 대하여 기록을 남기고 있는가?

개인정보 열람 등의 요구 처리결과 기록

① 기록 대상

1. 정보주체 또는 대리인 요청 내역
2. 요청 접수 일시, 요청 유형(열람·정정·삭제·처리정지·전송요구 등)
3. 본인 확인 방법 및 결과
4. 처리 결과(승인·거절·부분 처리 등) 및 처리 일시
5. 처리 담당자 및 근거 법령·사유
6. 정보의 제공 방식 및 범위(파일 형식, 조회 링크 등)

개인정보 열람 요구서

정보주체	성 명	전화번호	
	생년월일		
	주 소		
대리인	성 명	전화번호	
	생년월일	정보주체와의 관계	
	주 소		
요구내용	[ ] 개인정보의 항목 및 내용 [ ] 개인정보 수집·이용의 목적 [ ] 개인정보 보유 및 이용 기간 [ ] 개인정보의 제3자 제공 현황 [ ] 개인정보 처리에 동의한 사실 및 내용		

개인영상정보(□ 존재확인 □ 열람) 청구서

청구인	성 명	전화번호	
	생년월일	정보주체와의 관계	
	주 소		
정보주체의 인적사항	성 명	전화번호	
	생년월일		
	주 소		
청구내용 (구체적으로 요청하지 않으면 처리가 곤란할 수 있음)	영상정보 기록기간	예 : 2011.01.01 18:30 ~ 2011.01.01 19:00	
	영상정보 처리기기 설치장소	예 : 00시 00구 00대로 0 인근 CCTV1	
	청구 목적 및 사유		

출처: 개인정보 처리방법에 관한 고시 별지 제2호·제8호

◇ 정보통신망에서 사생활 침해 또는 명예훼손 등 타인의 권리를 침해한 경우 침해를 받은 자가 정보통신서비스 제공자에게 정보의 삭제 요청 등을 할 수 있는 절차를 마련하여 시행하고 있는가?

정보통신망에서의 권리 보호

①「정보통신망법」제44조2 (정보의 삭제요청 등) 기준

1. 삭제 등 요청권

- 정보통신망을 통하여 일반에게 공개된 정보로 인해 사생활 침해·명예훼손 등 타인의 권리가 침해된 경우, 피해자는 해당 정보를 처리한 정보통신서비스 제공자에게 침해 사실을 소명하여 삭제등을 요청할 수 있다. 요청자는 처리 경과 및 결과를 통지받을 수단을 지정할 수 있다.

2. 제공자의 조치 의무

- 제공자는 요청을 받으면 지체 없이 삭제·임시조치 등 필요한 조치를 취하고, 그 사실을 신청인과 정보게재자에게 즉시 알려야 한다. 또한 조치 사실을 게시판 공시 등으로 이용자가 알 수 있도록 해야 한다.

3. 임시조치

- 권리 침해 여부 판단이 어렵거나 이해당사자 간 분쟁이 예상되는 경우, 제공자는 해당 정보에 대한 접근을 최대 30일 이내로 임시 차단할 수 있다.

4. 약관 기재

- 필요한 조치의 내용·절차를 약관에 구체적으로 명시해야 하며, 조치를 이행하면 배상책임을 줄이거나 면제받을 수 있다

3.5.3 정보주체에 대한 통지

세부분야	3.5.3 정보주체에 대한 통지
인증 기준	개인정보의 이용·제공 내역 등 정보주체에게 통지하여야 할 사항을 파악하여 그 내용을 주기적으로 통지하여야 한다.
주요 확인사항	• 법적 의무 대상자에 해당하는 경우 개인정보 이용·제공 내역 또는 그 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 정보주체에게 주기적으로 통지하고 있는가? • 개인정보 이용·제공 내역 통지 항목은 법적 요구항목을 모두 포함하고 있는가?
기준 요약도	
운영 방안	**◇ 법적 의무 대상자에 해당하는 경우 개인정보 이용·제공 내역 또는 그 내역을 확인할 수 있는 정보시스템에 접속하는 방법을 정보주체에게 주기적으로 통지하고 있는가?** **통지 의무 대상 및 방법** ① 통지 의무 대상 : 1. 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만 명 이상 2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다.) 매출액이 100억 원 이상인 정보통신서비스 제공자 등 ② 통지 주기 : 연 1회 이상 ③ 통지 방법 : 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법 ④ 통지 예외 : 연락처 등 이용자에게 통지할 수 있는 개인정보를 수집하지 않은 경우

◇ 개인정보 이용·제공 내역 통지 항목은 법적 요구항목을 모두 포함하고 있는가?

개인정보 이용내역 통지 항목

① 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목

② 개인정보를 제공받은 자와 그 제공 목적 및 제공한 개인정보의 항목

- 단「통신비밀보호법」제13조, 제13조의2, 제13조의4 및「전기통신사업법」제83조제3항에 따라 제공한 정보는 제외

※ 출처: SK쉴더스 모바일 카드 서비스 개인정보 이용내역 통지 내용(SK쉴더스)

안녕을 지키는 기술 | SK 쉴더스

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 ICT취약점진단팀