SK 쉴더스

정보보호 및 개인정보보호관리체계(ISMS-P) 운영 가이드

정보보호 및 개인정보보호관리체계(ISMS-P) 운영 가이드

안녕하십니까? SK쉴더스입니다.

정보보호 및 개인정보보호관리체계(ISMS-P) 인증기준은 "정책/ 조직/ 서비스/ 시스템/ 정보보호시스템/ 준법사항" 등을 하나의 통합한 "관리체계"로 그 범위가 넓어 "관리적/기술적" 담당자들의 전문성을 하나로 통합하기가 어려운 실정입니다.
또한, 다양한 조직의 정책 및 대/내외 환경, 시스템(자산) 등의 빠른 변화로 인해 더욱 어렵게 느낄 수 있습니다.

ICT사업그룹에서는 “22년도 개인정보보호 가이드”를 발간한 바 있습니다. 세부적인 항목은 각 조직의 정책과 환경에 따라 다를 수 있지만, 항목이 요구하는 사항을 예시와 이미지로 구성하여 관리체계를 쉽게 이해할 수 있도록 직관적인 “정보보호 및 개인정보보호관리체계(ISMS-P) 운영 가이드”를 발간하게 되었습니다.

본 가이드는 인증기준 항목별 대상과 범위를 구분 짓고, 시작과 끝맺음을 제시하므로 단계별 인증기준 달성을 통해 최종적으로 하나의 관리체계로 연결될 수 있도록 구성하였으며, “관리체계 수립 및 운영(16개)”, “보호대책 요구사항(64개)”, “개인정보 처리 단계별 요구사항(22개)” 총 102개의 인증기준과 그 하위에 각 “인증기준별 주요 확인사항”을 토대로 전반적 관리체계를 설명하였습니다.

앞으로도 SK쉴더스는 보안 담당자 및 운영자가 다양한 환경에서 발생할 수 있는 위협을 발빠르게 대응할 수 있도록 가이드를 발간할 계획입니다.
감사합니다.

더불어, 정보보호 및 개인정보보호관리체계(ISMS-P) 운영 가이드 발간에 많은 시간과 노력을 투자한 팀원들에게 감사인사를 드립니다.

ICT사업그룹 취약점진단팀 팀장
김 상 춘

목 차

I. 정보보호 및 개인정보보호관리체계(ISMS-P) 진단항목

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. 보호대책 요구사항 (64개)		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
		2.4.6 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

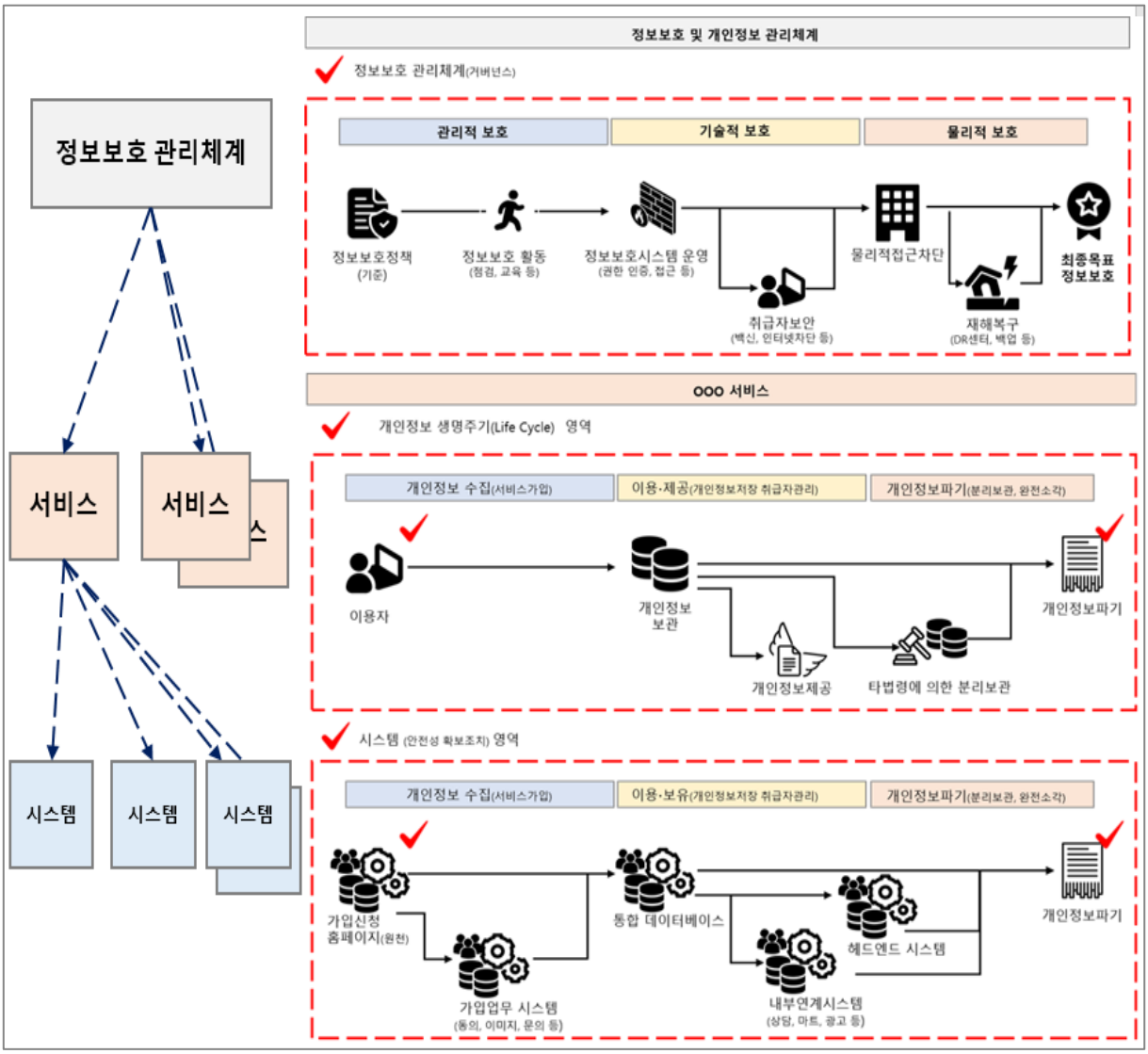
		2.6.4 데이터베이스 접근
2. 보호대책 요구사항 (64개)		2.6.5 무선 네트워크 접근
		2.6.6 원격접근 통제
		2.6.7 인터넷 접속 통제
	2.7 암호화 적용	2.7.1 암호정책 적용
		2.7.2 암호키 관리
	2.8 정보시스템 도입 및 개발 보안	2.8.1 보안 요구사항 정의
		2.8.2 보안 요구사항 검토 및 시험
		2.8.3 시험과 운영 환경 분리
		2.8.4 시험 데이터 보안
		2.8.5 소스 프로그램 관리
		2.8.6 운영환경 이관
	2.9 시스템 및 서비스 운영관리	2.9.1 변경관리
		2.9.2 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. 보호대책 요구사항 (64개)		2.10.7 보조저장매체 관리
		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 (22개)	**3.1 개인정보 수집 시 보호조치**	3.1.1 개인정보 수집 제한
		3.1.2 개인정보의 수집 동의
		3.1.3 주민등록번호 처리 제한
		3.1.4 민감정보 및 고유식별정보의 처리 제한
		3.1.5 간접수집 보호조치
		3.1.6 영상정보처리기기 설치·운영
		3.1.7 홍보 및 마케팅 목적 활용 시 조치
	3.2 개인정보 보유 및 이용 시 보호조치	3.2.1 개인정보 현황관리
		3.2.2 개인정보 품질보장
		3.2.3 개인정보 표시제한 및 이용 시 보호조치
		3.2.4 이용자 단말기 접근 보호
		3.2.5 개인정보 목적 외 이용 및 제공

	3.3 개인정보 제공 시 보호조치	3.3.1 개인정보 제3자 제공
3. 개인정보 처리 단계별 요구사항 (22개)		3.3.2 업무 위탁에 따른 정보주체 고지
		3.3.3 영업의 양수 등에 따른 개인정보의 이전
		3.3.4 개인정보의 국외 이전
	3.4 개인정보 파기 시 보호조치	3.4.1 개인정보의 파기
		3.4.2 처리목적 달성 후 보유 시 조치
		3.4.3 휴면 이용자 관리
	3.5 정보주체 권리보호	3.5.1 개인정보처리방침 공개
		3.5.2 정보주체 권리보장
		3.5.3 이용내역 통지

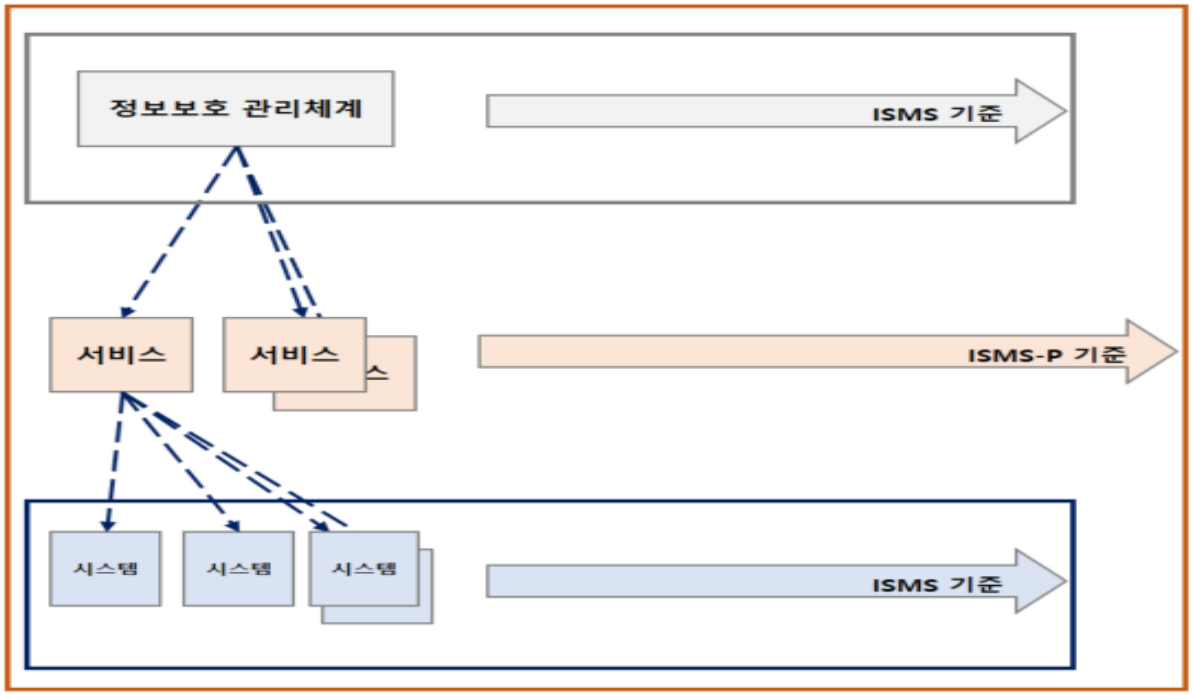
II. 정보보호 및 개인정보보호관리체계 운영

정보보호 및 개인정보보호관리체계의 개요



- **정보보호 및 개인정보보호 관리체계**의 최종 목표는 보유한 정보자산을 안전하게 운영하기 위함이며, 이를 위해 "정보보호정책 → 정보보호활동 → 정보보호시스템운영 → 물리보안" 등의 과정이 필요합니다.
- 정보보호 관리체계에서 "범위산정"은 중요한 요소로써 서비스와 정보시스템에 대한 기준에 명확하지 않아 관리하기가 쉽지 않은 영역입니다.
- **서비스:** 이용자를 위해 제공되는 편의 기능입니다.
- **정보시스템:** 서비스의 기반이 되는 하위 개념에 속합니다.
- **정보보호시스템:** 정보시스템을 안전하게 운영하기 위해 필요한 시스템으로 정보보호시스템의 초기 구성 및 운영에 필요한 설정이 보안정책에 맞게 적용하였다 하더라도 **관리/운영 인력의 보안 인식**이 없다면 무용지물이 될 수밖에 없습니다.

- 무인경비란 재화(財貨) 서비스(예시) "ADT캡스 무인경비"를 제공하기 위해 "① 회원가입시스템, ② 경비운영시스템, ③고객지원시스템 등등(예시)" 실제로 각각의 시스템들이 각자의 운영체제와 데이터베이스 등으로 운영되고 있으며, 관리하고 있는 정보시스템, 인력, 정보보호시스템, 네트워크장비 등이 하나의 관리체계 범위에 속하게 됩니다.
- **"시스템 단위(ISMS)"**로 관리체계에 중심을 두면 개인정보 생명주기가 제외한 **정보시스템운영**이 되며 **"서비스 단위(ISMS-P)"** 로 관리체계에 중심을 두면 **"개인정보보호 + 정보시스템운영"**으로 관리 항목이 확장됩니다.



III. 개인정보 처리 단계별 요구사항

1. 관리체계 수립 및 운영

1.1 관리체계 기반 마련

1.1.1 경영진의 참여

<table>
<tr><th>세부분야</th><th>1.1.1 경영진의 참여</th></tr>
<tr><td>인증
기준</td><td>최고경영자는 정보보호 및 개인정보보호 관리체계의 수립과 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 체계를 수립하여 운영하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 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</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 정보보호 및 개인정보보호 관리체계의 수립 및 운영활동 전반에 경영진의 참여가 이루어질 수 있도록 보고 및 의사결정 등의 책임과 역할을 문서화하고 있는가?

→ 정보보호 정책서 경영진 참여 문서화 (예시)</td></tr>
</table>

「**정보보호 정책서**」 제 ○○조 (정보보호 조직구성)

① 최고경영자(CEO)는 전자정보와 정보통신망 보호를 위해 정보통신망의 보안대책을 수립·시행 해야하며 정보보호에 대한 책임을 진다.

② 최고경영자(CEO)는 전사의 정보보호 업무를 원활히 수행하기 위해 업무를 총괄하는 정보보호 최고책임자(CISO)를 포함한 정보보호 전담조직을 구성한다.

③ 최고책임자(CISO)는 정보보호 관련 심의 및 의결을 위한 최상위 기구인 '정보보호 위원회'를 구성·운영 한다.

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

→ 정보보호 활동 참여(예시)

「**정보보호 조직 관리지침**」 제 ○○조 (정보보호 최고책임자 역할)

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

≫ 정보보호 관리체계 계획 수립에 관한 업무

≫ 정보보호 정책 지침 제·개정 업무

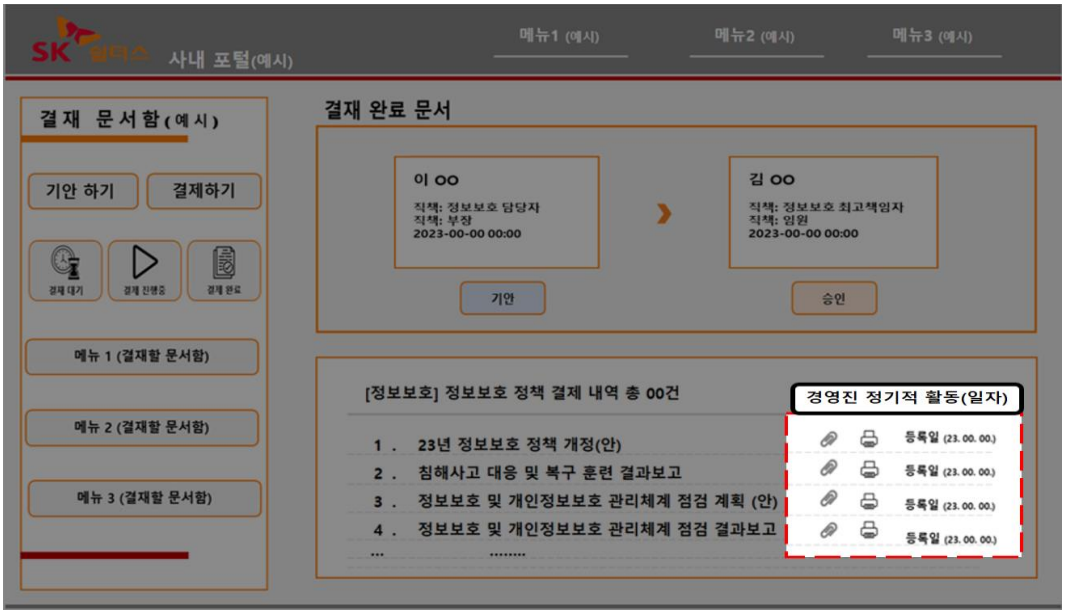
≫ 취약점 분석·평가 및 침해사고 예방 지원업무

≫ 침해사고 대응 및 복구 업무

≫ 정보보호의 날 운영 업무

≫ 정보보호에 필요한 예상 및 설비 등 자산 확보에 관한 업무

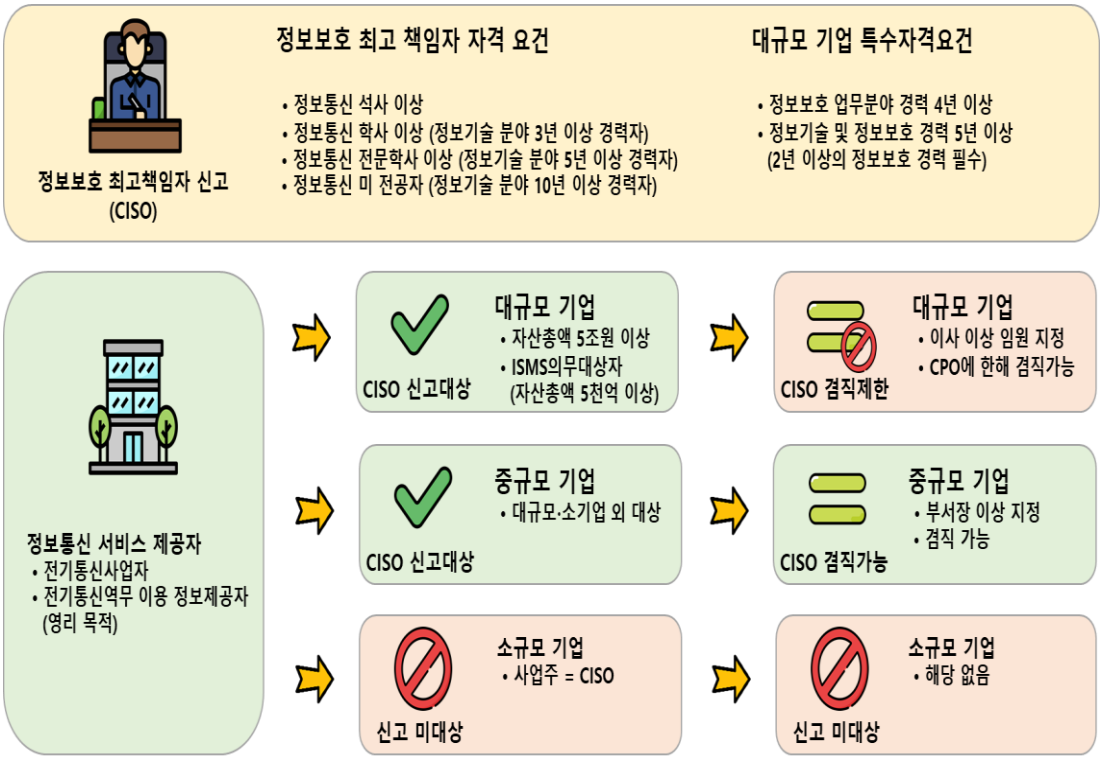
≫ 그 밖에 정보보호를 위해 필요한 업무



※ 경영진 정보보호 활동(이해를 돕기 위한 예시)

	「**정보보호 조직 관리지침**」 제 ○○조 (정보보호 위원회 심의) ① 정보보호 위원회는 다음 각 호에 대하여 심의한다. ≫ 정보보호제도 개선에 관한 사항 ≫ 정보보호 업무 기획·조정·감독·통제에 관한 사항 ≫ 정보보호 위규자 심의처리에 관한 사항 ≫ 그밖에 정보보호 활동에 중요하다고 인정되는 사항

1.1.2 최고 책임자 지정

<table>
<tr><th>세부분야</th><th>1.1.2 최고 책임자 지정</th></tr>
<tr><td>인증
기준</td><td>최고경영자는 정보보호 업무를 총괄하는 정보보호 최고책임자와 개인정보보호 업무를 총괄하는 개인정보보호 책임자를 예산·인력 등 자원을 할당할 수 있는 임원급으로 지정하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 최고경영자는 정보보호 및 개인정보보호 처리에 관한 업무를 총괄하여 책임질 최고책임자를 공식적으로 지정하고 있는가?
• 정보보호 최고책임자 및 개인정보 보호책임자는 예산, 인력 등 자원을 할당할 수 있는 임원급으로 지정하고 있으며, 관련 법령에 따른 자격요건을 충족하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 최고경영자는 정보보호 및 개인정보보호 처리에 관한 업무를 총괄하여 책임질 최고책임자를 공식적으로 지정하고 있는가?

→ 정보보호 최고책임자(CISO)와 개인정보보호 책임자(CPO) 직무
① 정보보호최고책임자(CISO) 역할
≫ 정보보호관리체계의 수립 및 관리·운영
≫ 정보보호 취약점 분석·평가 및 개선
≫ 침해사고의 예방 및 대응
≫ 사전 정보보호대책 마련 및 보안조치 설계·구현 등</td></tr>
</table>

≫ 정보보호 사전 보안성 검토

≫ 중요 정보의 암호화 및 보안서버 적합성 검토

≫ 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

② 개인정보보호책임자(CPO)

≫ 개인정보 보호 계획의 수립 및 시행

≫ 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선

≫ 개인정보 처리 관련 불만 처리 및 피해 구제

≫ 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템 구축

≫ 개인정보 보호 교육 계획의 수립 및 시행

≫ 개인정보파일의 보호 및 관리·감독

≫ 개인정보 처리방침의 수립·변경 및 시행

≫ 개인정보 보호 관련 자료 관리

≫ 목적이 달성되거나 보유기간이 지난 개인정보 파기

→ 정보보호 최고책임자(CISO) 임명

「**정보보호 조직 관리지침**」 제 ○○조 (최고책임자 지정)

① 조직 내에서 정보보호 관리 활동을 효과적으로 추진하기 위해 정보보호 최고책임자(CISO)를 지정해야 한다.

② 개인정보책임자(CPO)는 신고의무는 없지만, 내부에 해당 직무 지정 필요


SK 쉴더스

안녕을 지키는 기술

참고자료

문서번호: SK쉴더스 인사발령 제 01 - 001호

수 신 : 수신처 참조

제 목 : 인사 발령 (2023 -01호)

ON	소 속	직능	직급	성명	발령내용	발령구분	발령일자	비고
1	정보보호그룹	기업정보보안	임원	김 ○ ○	명) 정보보호최고책임자 (CISO)	전보	2023-01-01	
2	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	
3	***	***	***	***	***	***	***	

해당 예시는 참고자료로 실제 문서가 아닙니다. SK 쉴더스

※ 인사명령 내용(이해를 돕기 위한 예시)

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

→ 정보보호 최고책임자 지정·신고 의무대상

「**정보통신망법**」 제35조의 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.**

≫ 자본금 1억 이하 정보통신서비스 제공자

≫ 중소기업법 제2조제2항에 따른 소기업

≫ "정보통신사업자", "정보통신 관리체계 인증 대상자" "개인정보처리자 중 통신판매업자" 중 해당하지 않는 자

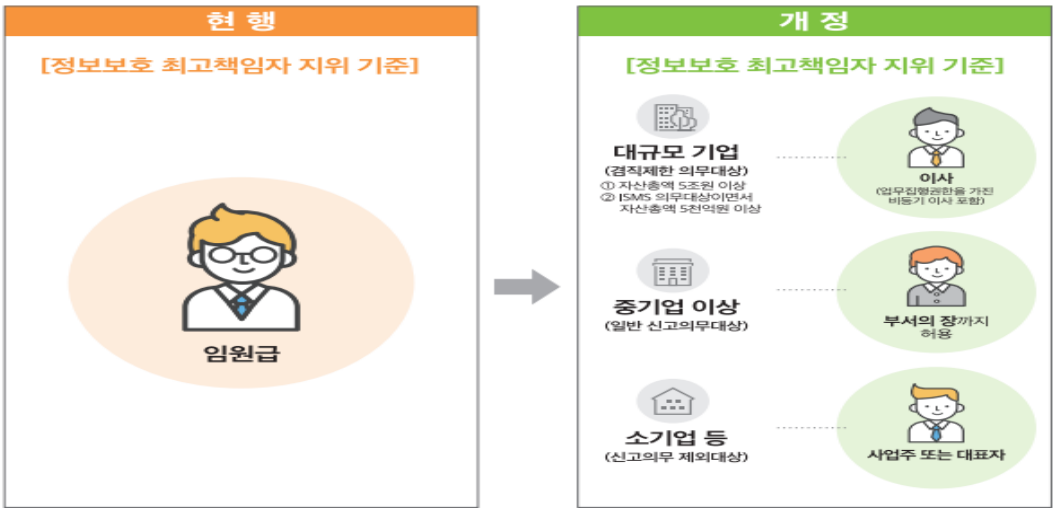
※ 출처: 정보보호최고책임자 지정 신고제도 안내서(과학기술정보통신부•KISA)

→ **정보보호 최고책임자 신고 의무대상자 분류 별 지정 기준**

① 대규모 기업(겸직제한 의무대상): 직전연도 말 자산총액 5조 이상 이거나, 인증의무대상 중 자산총액 5천억 이상

② 중기업 이상: 대규모 기업 외 정보통신 서비스 제공자

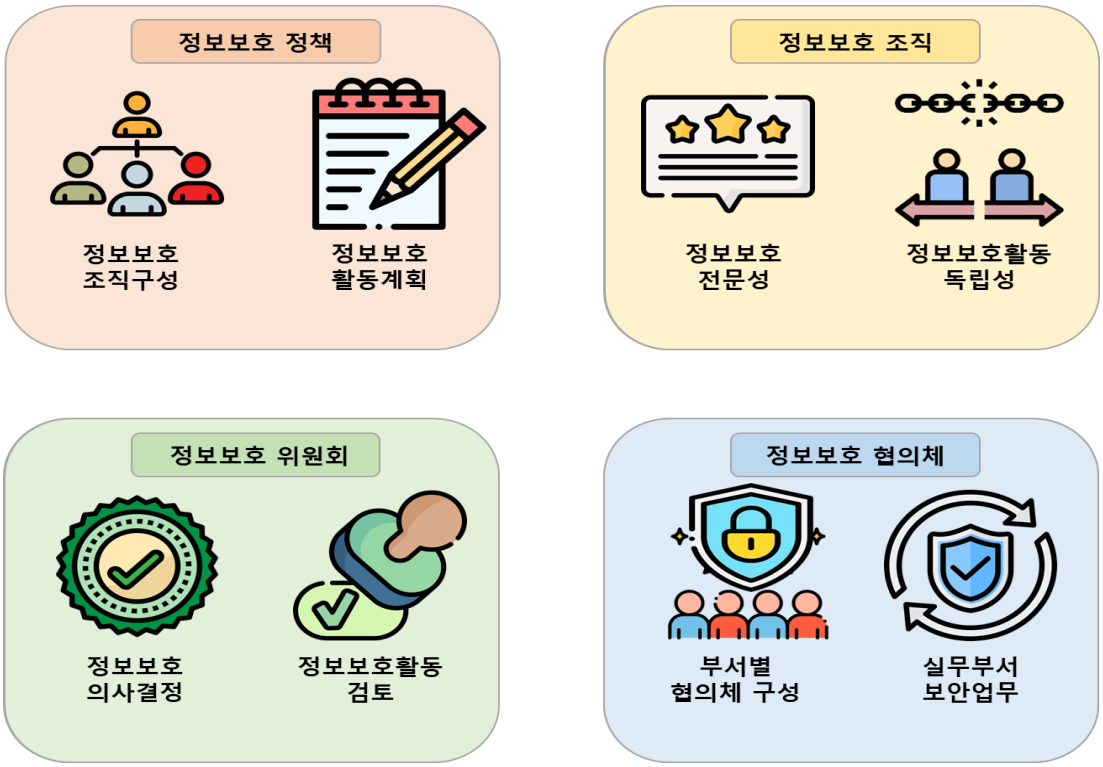
③ 소기업 등 (신고의무 제외)



※ 출처: 정보보호최고책임자 지정 신고제도 안내서(과학기술정보통신부•KISA)

	→ **정보보호 최고책임자 자격요건** ① **일반자격요건: (중기업 기업 신고 의무대상자)** ≫ 정보보호 또는 정보기술분야 석사 이상 ≫ 정보보호 또는 정보기술분야 학사 3년 이상 경력 ≫ 정보보호 또는 정보기술분야 전문학사 5년 이상 경력 ≫ 정보보호 또는 정보기술분야 10년 이상 경력 ② **특별자격요건: (대규모 기업 겸직제한 의무대상자)** ≫ 정보보호 업무 경력 4년 이상 ≫ 정보보호 또는 정보기술분야 5년 이상 경력 중 2년은 정보보호 분야 업무경력

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 개인정보보호 담당자로 구성된 협의체를 구성하여 운영하여야 한다.
주요 확인사항	• 정보보호 최고책임자 및 개인정보 보호책임자의 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 개인정보 보호책임자의 업무를 지원하고 조직의 정보보호 및 개인정보보호 활동을 체계적으로 이행하기 위하여 전문성을 갖춘 실무조직을 구성하여 운영하고 있는가? → 정보보호 조직 문서화

「**정보보호 조직 관리지침**」 제 ○○조 (정보보호 조직구성)

① 사내 정보보호 활동을 효율적으로 수행하기 위해 전문지식을 보유한 정보보호 전담팀(이하 정보보호팀)을 구성하고 각 호의 활동을 담당한다.

≫ 정보보호팀은 자산에 대한 위협 및 위험분석, 주기적 모니터링을 통한 정보보호 관리 수행

≫ 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

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

→ 정보보호 정책서 경영진 참여 문서화 (예시)

「**정보보호 조직 관리지침**」 제 ○○조 (정보보호 위원회 구성)

① 정보보호최고책임자(CISO)는 정보보호 및 개인정보보호를 관련 중요사항 심의 및 의결을 위한 정보보호 위원회를 구성·운영한다.

≫ 위원장: 정보보호최고책임자

≫ 위원: 각 부서 업무팀장

≫ 간사: 정보보호 팀장

「**정보보호 조직 관리지침**」 제 ○○조 (정보보호 위원회 심의)

① 정보보호 위원회는 다음 각 호에 대하여 심의한다.

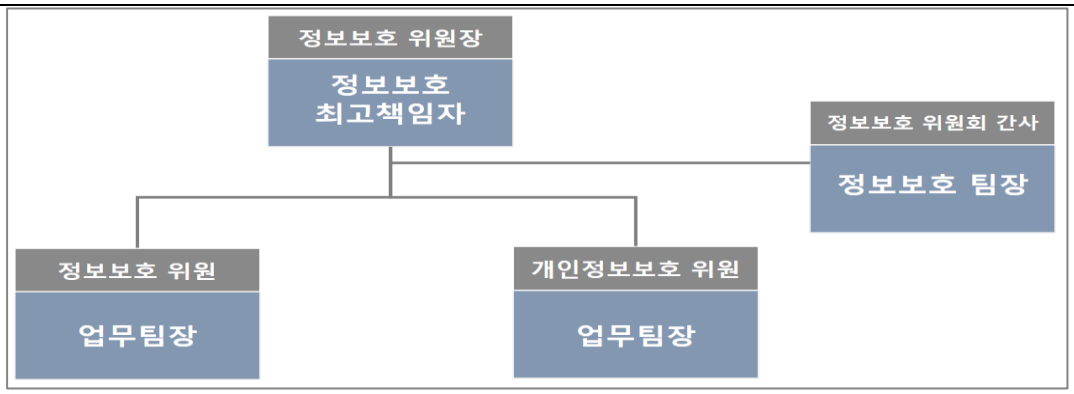
≫ 정보보호제도 개선에 관한 사항

≫ 정보보호 업무 기획·조정·감독·통제에 관한 사항

≫ 정보보호 위규자 심의처리에 관한 사항

≫ 그밖에 정보보호 활동에 중요하다고 인정되는 사항

② 정보보호 위원회의 의결사항은 '정보보호위원회 의사록'을 첨부하여 정보보호최고책임자(CISO)의 공표한다.



※ 정보보호 위원회 조직도(이해를 돕기 위한 예시)

※ 정보보호위원회 의사록(이해를 돕기 위한 예시)

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

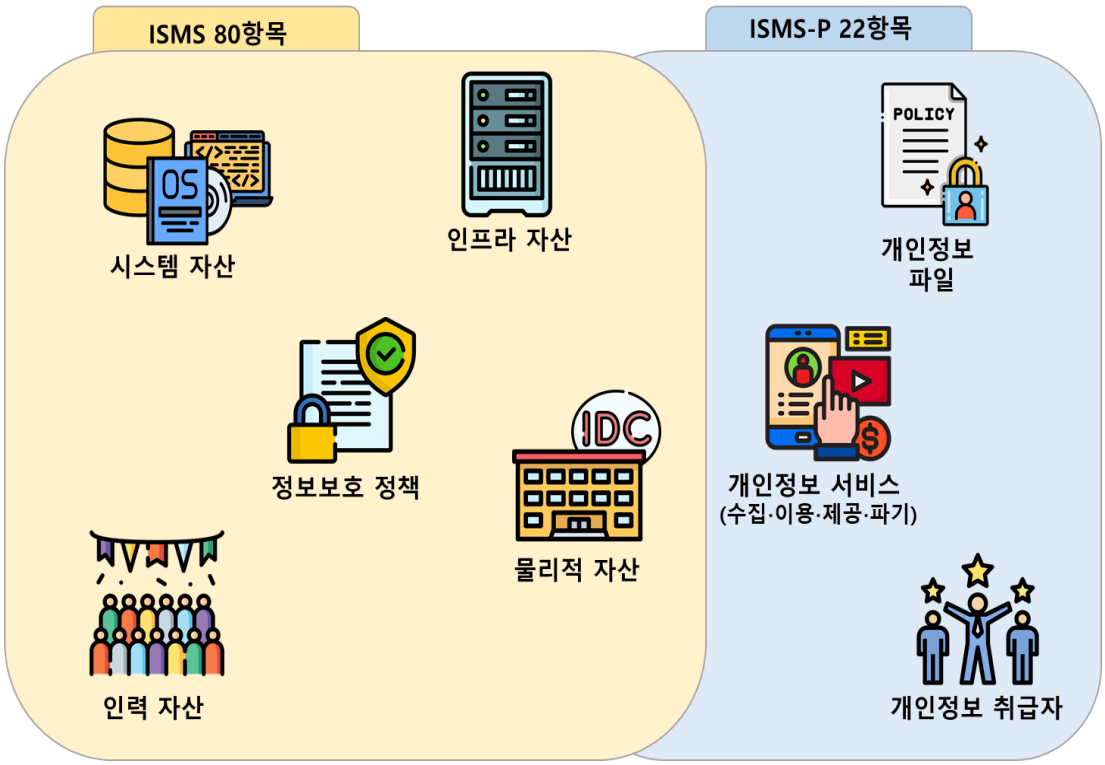
→ 정보보호 실무 협의체 구성

「정보보호 조직 관리지침」 제 ○○조 (정보보호 실무 협의체 구성)

① 정보보호 실무 협의체는 정보보호관리자을 의장으로 하여 부서정보보호책임자와 정보시스템책임자를 구성하여 정보보호 실무협의 회의를 진행한다

② 정보보호 실무 협의회는 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 내에서 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, 문서목록 등)이 포함된 문서를 작성하여 관리하고 있는가?
기준 요약도	
운영 방안	**◇ 조직의 핵심 서비스 및 개인정보 처리에 영향을 줄 수 있는 핵심자산을 포함하고 범위 내에 시스템 현황을 파악 있는가?** **→ 유·무형 자산 상세(예시)** ① ISMS 인증범위 (예시) ≫ 「**DMZ**」 웹사이트, 서버(WAS, API, 연계, 스트레밍 DNS 등)

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

≫「**서버존**」서버, 데이터베이스, 보안시스템

≫「**정보통신서비스 관리시스템**」관리시스템(back office), 모니터링시스템 등

≫「**개발 환경**」개발 및 테스트 서버, 테스트 데이터베이스 등

≫「**업무 환경**」인증범위 내 인력, IT운영자 정보통신 관리자, 개발자 등 단말

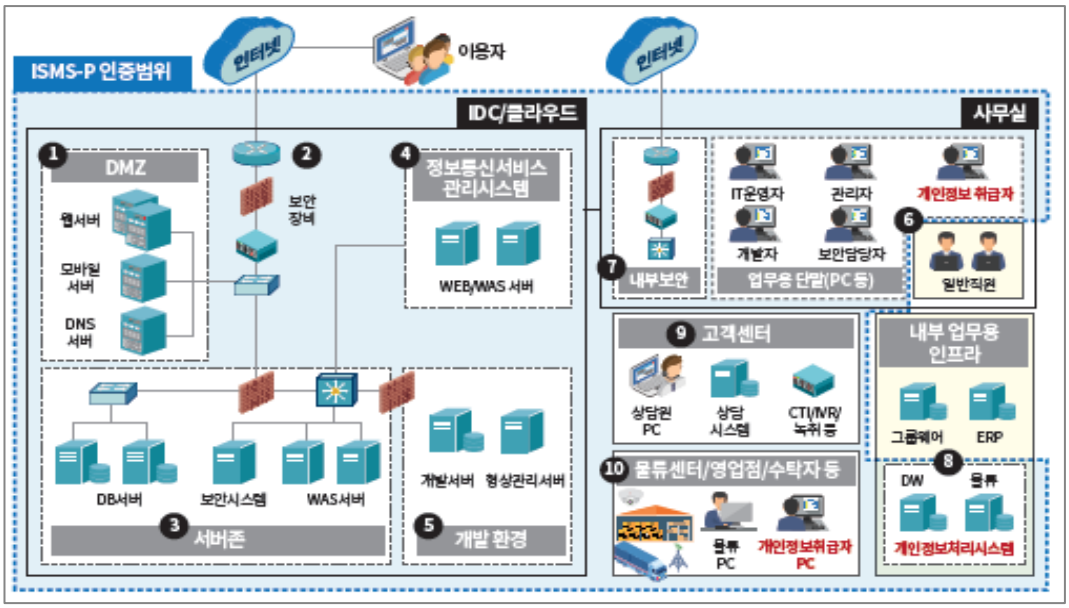
≫「**내부용 네트워크 및 보안 시스템**」라우터, 스위치, DRM, DLP, PMS 등

≫「**내부 업무용 인프라**」그룹웨어, ERP 등

② ISMS + P 추가 인증범위 (예시)

≫「**고객센터**」상담원, 팩스시스템, 녹취시스템 등

≫「**물류 센터**」영업점·개인정보수탁사 등: 대리점, POS, 업무용 단말 등



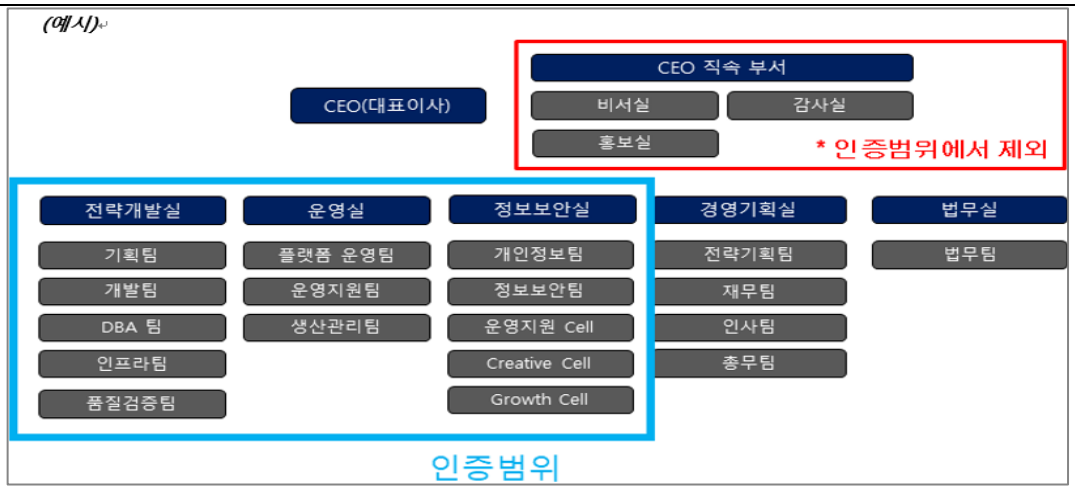
※ 출처: 정보보호 및 개인정보보호 관리체계 인증제도 안내서(KISA)

◇ 정의된 범위 내에서 예외사항이 있을 경우 명확한 사유 및 관련자 협의 · 책임자승인 등 관련 근거를 기록·관리하고 있는가?

→ 범위 내 예외 사항(예시)

① 정보보호 및 개인정보보호에 업무 범위를 벗어난 자산 및 조직 제외

≫ 비서실 감사실 홍보실 등 서비스 제공을 위한 업무조직이 아닌경우 (예시)



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

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

→ 정보보호 및 개인정보보호관리체계 범위 문서화

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

≫ 주요 서비스 및 업무 현황(개인정보 처리 업무 현황 포함)

≫ 서비스 제공과 관련된 조직 현황(조직도 등)

≫ 정보보호 및 개인정보보호 조직 현황

≫ 주요 설비 목록

≫ 정보시스템 목록 및 네트워크 구성도

≫ 정보자산, 개인정보 관련 자산식별 기준 및 자산현황

≫ 정보보호 및 개인정보보호 시스템 목록

≫ 서비스(시스템) 구성도 및 개인정보(수집, 이용, 제공, 저장, 관리, 파기) 처리

≫ 문서 목록(예: 정책, 지침, 매뉴얼, 운영명세서 등)

≫ 정보보호 및 개인정보보호 관리체계 수립 방법 및 절차, 관련 법적 준거성 검토, 내부감사

≫ 고객센터, IDC, IT 개발 및 운영 등 외주(위탁)업체 현황 등

Ⅱ 인증의 범위

□ 전체 서비스(사업) 현황

① 인증희망 이유

인증희망 이유	☞ 법적요구, 고객요구, 내부 정책 등 고려사항을 기술		
의무대상 여부	Y/N	사유	의무대상자만 작성

※ 컨설팅 업체명 / 기간 / PM명:

② 인증심사 담당자

직급(업무)	부서	성명/직호	연락처	이메일
정보보호 책임자(CISO), 개인정보보호 책임자(CPO)	정보보호관리본부	홍길동 이사	01-1234-1234	abc@_____.kr
정보보호 책임자	정보보호관리실	성준창	01-1234-1234	abc@_____.kr
정보보호 담당자	정보보호관리팀	이몽룡	01-1234-1234	abc@_____.kr
정보보호 담당자	정보보호관리팀			

③ 현재 제공 중인 전체 서비스(사업)

☞ 인증범위 포함여부와 상관없이 신청인이 제공하는 전체 서비스를 모두 기술

No	서비스명	서비스설명 및 URL	인증범위대상	제외사유
1	㈜조선시대 홍길동 쇼핑몰		Y	-
2	㈜고조선 대표 홈페이지		Y	-
3	㈜고조선 그룹웨어		Y	내부망 전용 서비스
4			N	
			N	
			N	

□ 서비스 현황

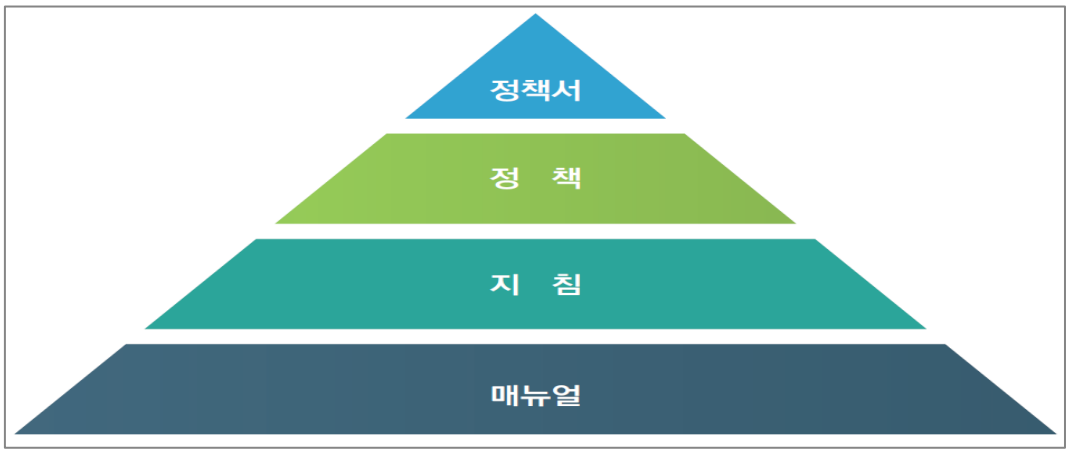
구분	인증을 받고자하는 서비스(사업) 현황
서비스명	☞ (대국민 또는 이용자 대상 서비스)포털 서비스, 인터넷 쇼핑몰 서비스, 대국민홈페이지서비스 등 ☞ (임직원 또는 사내 서비스)출입통제, 출입자관리, 인사노무, 재무회계 서비스 등
서비스 상세 설명	☞ 서비스 상세 설명 ☞ 주요 이용자 또는 고객, 회원수 등
인증범위내 중요정보 식별	☞ 인증범위내 중요정보 식별 ※ 중요정보: 내부적으로 식별/분류한 기준에 따른 주요 정보(기업 기밀 정보, 개인정보 등)
정보분류 기준	☞ 중요 정보 분류 기준
기타	☞ 특이사항 기술

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

1.1.5 정책 수립

세부분야	1.1.5 정책 수립
인증 기준	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.
주요 확인사항	• 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, 주기등을 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?
기준 요약도	
운영 방안	**◇ 조직이 수행하는 모든 정보보호 및 개인정보보호 활동의 근거를 포함하는 최상위 수준의 정보보호 및 개인정보보호 정책을 수립하고 있는가?** **→ 정보보호 규정 체계 (예시)** ① 정보보호 정책서: 정보보호에 대한 최상위 수준의 목표 및 방향, 원칙을 경영진이 제시하는 문서

② 지침·메뉴얼: 정보보호 이행활동 및 수행절차를 제시하는 문서



※ 출처: CISO 길라잡이 기본편(KISA)

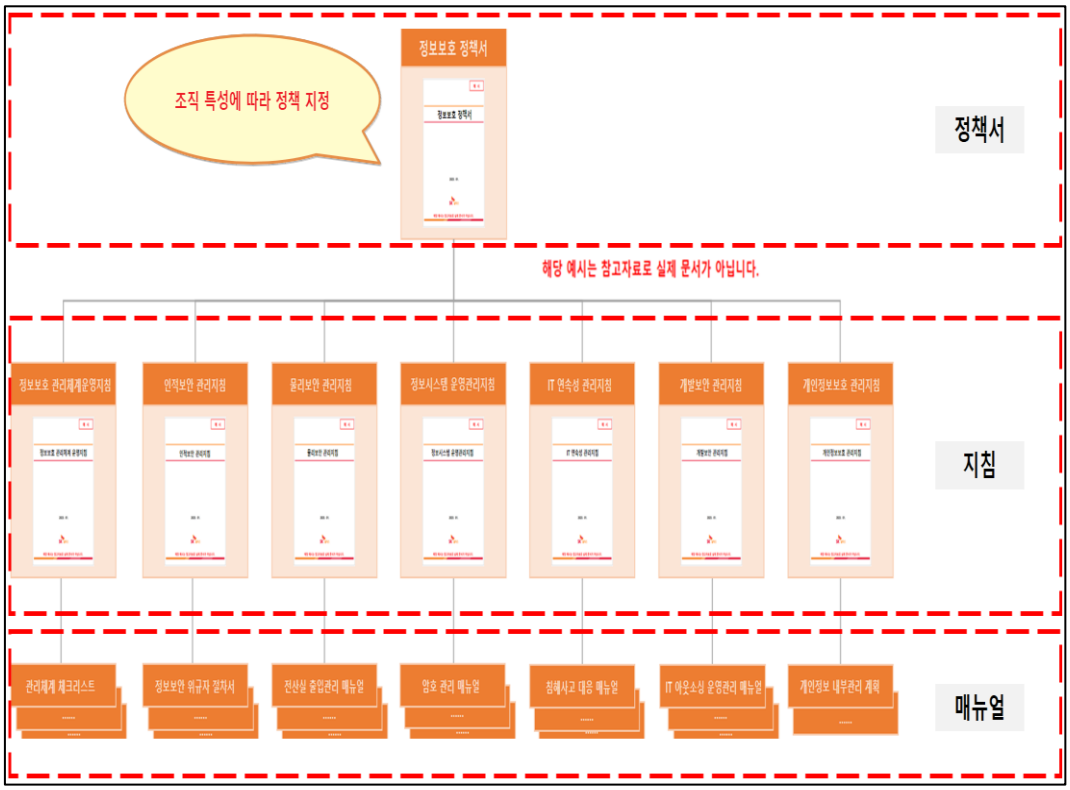
◇ 정보보호 및 개인정보보호 정책의 시행을 위하여 필요한 세부적인 방법, 절차, 주기등을 규정한 지침, 절차, 매뉴얼 등을 수립하고 있는가?

→ 하위 문서 세부적인 방법 및 절차 주기 작성

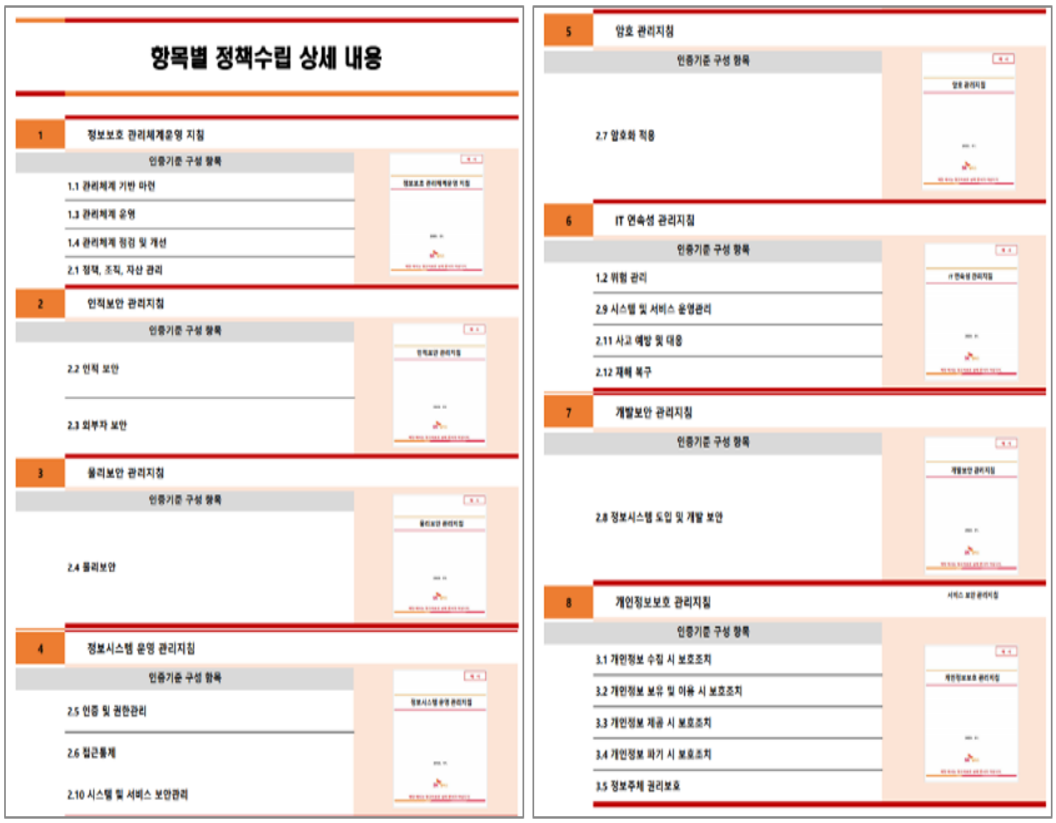
① 정보보호 관리지침: 정보보호 조직, 교육, 감사, 임직원 보안, 위수탁 계약 등 규정

② 서버운영 보안지침: 서버 보안성검토, 취약점점검, 패스워드정책, 접근권한검토 규정

③ 임직원 보안지침: 계정 및 패스워드, PC지급 및 사용, 인터넷, 이메일 사용 등등
그 외 세부 사항에 대한 지침 작성



※ 내부 지침서 수립 (이해를 돕기 위한 예시)



※ 요구사항에 맞춰 가이드 편집(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 (정보보호 위원회 심의)

① 정보보호 위원회는 다음 각 호에 대하여 심의한다.

≫ 정보보호제도 개선에 관한 사항

≫ 정보보호 업무 기획·조정·감독·통제에 관한 사항

≫ 정보보호 위규자 심의처리에 관한 사항

≫ 그밖에 정보보호 활동에 중요하다고 인정되는 사항

※ 지침 정책 경영진 승인(이해를 돕기 위한 예시작성)

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

→ 보안지침 내부 직원 공유(예시)

① 임직원이 접근하기 쉬운 방법으로 지침 및 가이드 제공

※ 사내 게시판을 통한 정책과 시행문서 제·개정 사항 전파 (이해를 돕기 위한 작성 예시)

1.1.6 자원 할당

<table>
<tr><th>세부분야</th><th>1.1.6 자원 할당</th></tr>
<tr><td>인증
기준</td><td>최고경영자는 정보보호와 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고,
관리체계의 효과적 구현과 지속적 운영을 위한 예산 및 자원을 할당하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 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?</td></tr>
<tr><td>기준
요약도</td><td> 
정보보호 계획수립
· 세부계획 수립 시행
· 정보보호 적정성
· 정보보호 효과성
· 경영진 심의 승인
 
정보보호 조직구성
· 정보보호 업무이력
· IT 기술 이해
· 수행 경험
 
정보보호 자원할당
· 정보보호 보완 예산 편성
· 정보보호 전문 인력 지원</td></tr>
<tr><td>운영
방안</td><td>◇ 정보보호 및 개인정보보호 분야별 전문성을 갖춘 인력을 확보하고 있는가?

→ 정보보호 전문성을 갖춘 인력을 확보
① 전문 지식 및 관련 자격 보유
② 정보보호 및 개인정보보호 관련 실무 경력 보유
③ 정보보호 및 개인정보보호 관련 직무교육 이수 등</td></tr>
</table>

직무 기술서

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

직무상세내용
» 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 .....

필요지식
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 수칙에 대한 지식 » 연간손실예상(ALE, Annual Loss Expectancy)에 대한 지식 » 국내 정보보호 관련 법과 규정에서 정의된 보호조치 기준에 관한 지식 » 침해사고 대응절차에 관한 지식 .....

학력	경력
정보통신 또는 정보보호 관련학과 졸	정보보호 업무 경력 3년 이상
기타사항	
정보보호 기술 자격 우대(ISMS, 정보보안기사, CISA, CISSP 등)	

※ 직무기술서(이해를 돕기 위한 예시)

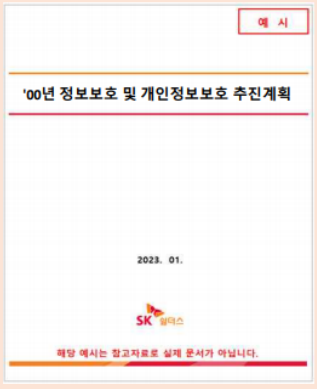
◇ 정보보호 및 개인정보보호 관리체계의 효과적 구현과 지속적 운영을 위하여 필요한 자원을 평가하여 필요한 예산과 인력을 지원하고 있는가?

→ 정보보호 및 개인정보보호 관리체계 지속 지원

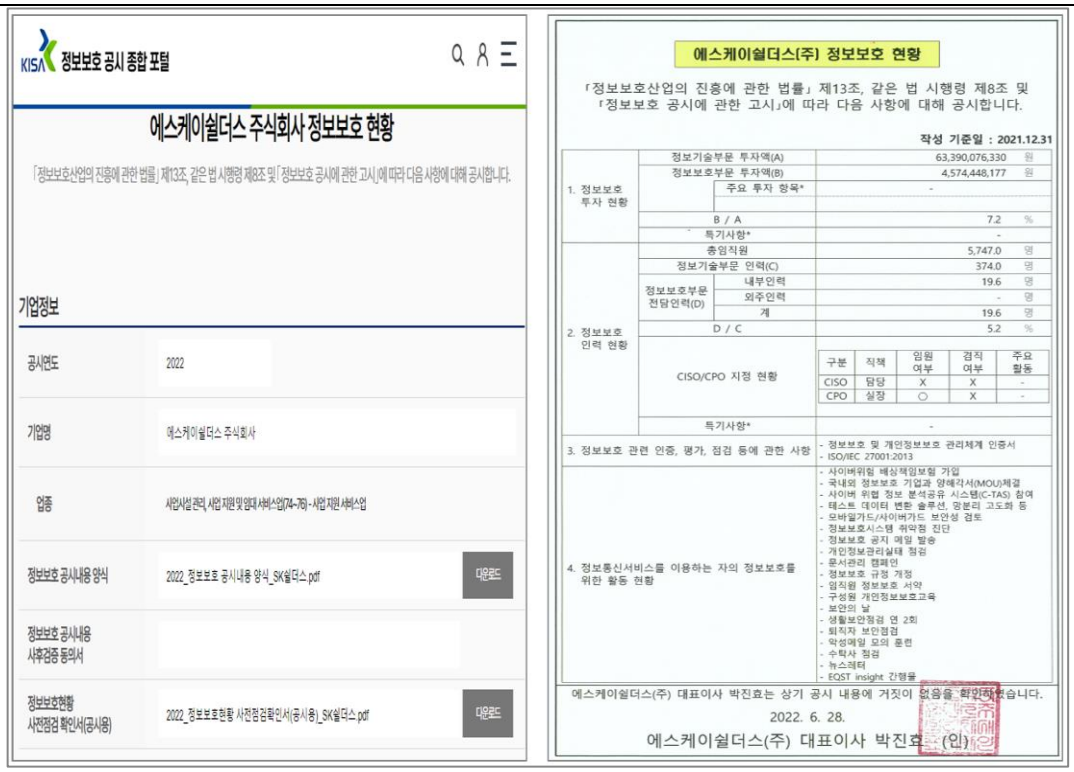
① 예산과 자원을 평가하여 예산 및 인력운영 계획 수립 및 승인 필요

'00년 정보보호 및 개인정보보호 추진계획

순번	내용			
1	추친 개요			
2	정보보호 조직			
3	정보보호업무 활동지침			
4	정보보호업무 세부추진계획			
구분	직위	성명	일자	서명
승인	정보보호 최고책임자	OOO	2023-01-01	승인
상신	정보보호 담당자	OOO	2022-12-20	-



※ 정보보호 및 개인정보보호 추진계획(이해를 돕기 위한 예시)



KISA 정보보호 공시 종합 포털

에스케이쉴더스 주식회사 정보보호 현황

「정보보호산업의 진흥에 관한 법률」 제13조, 같은 법 시행령 제8조 및 「정보보호 공시에 관한 고시」에 따라 다음 사항에 대해 공시합니다.

기업정보

공시연도	2022
기업명	에스케이쉴더스 주식회사
업종	사업시설관리, 사업지원및임대서비스업(74~76) - 사업지원서비스업
정보보호 공시내용 양식	2022_정보보호 공시내용 양식_SK쉴더스.pdf 다운로드
정보보호 공시내용 사후점검 동의서	
정보보호현황 사전점검 확인서(공시용)	2022_정보보호현황 사전점검확인서(공시용)_SK쉴더스.pdf 다운로드

에스케이쉴더스(주) 정보보호 현황

「정보보호산업의 진흥에 관한 법률」 제13조, 같은 법 시행령 제8조 및 「정보보호 공시에 관한 고시」에 따라 다음 사항에 대해 공시합니다.

작성 기준일 : 2021.12.31

1. 정보보호 투자 현황	정보기술부문 투자액(A)		63,390,076,330 원
	정보보호부문 투자액(B)		4,574,448,177 원
		주요 투자 항목*	-
	B / A		7.2 %
	특기사항*		-
2. 정보보호 인력 현황	총임직원		5,747.0 명
	정보기술부문 인력(C)		374.0 명
	정보보호부문 전담인력(D)	내부인력	19.6 명
		외주인력	- 명
		계	19.6 명
	D / C		5.2 %
	CISO/CPO 지정 현황		구분 / 직책 / 임원 여부 / 겸직 여부 / 주요 활동 CISO / 담당 / X / X / - CPO / 실장 / ○ / X / -
	특기사항*		-
3. 정보보호 관련 인증, 평가, 점검 등에 관한 사항			- 정보보호 및 개인정보보호 관리체계 인증서 - ISO/IEC 27001:2013
4. 정보통신서비스를 이용하는 자의 정보보호를 위한 활동 현황			- 사이버위험 배상책임보험 가입 - 국내외 정보보호 기업과 양해각서(MOU)체결 - 사이버 위협 정보 분석공유 시스템(C-TAS) 참여 - 테스트 데이터 변환 솔루션, 망분리 고도화 등 - 모바일기드/사이버가드 보안성 검토 - 정보보호시스템 취약점 진단 - 정보보호 공지 메일 발송 - 개인정보관리실태 점검 - 문서관리 캠페인 - 정보보호 규정 개정 - 임직원 정보보호 서약 - 구성원 개인정보보호교육 - 보안의 날 - 생활보안점검 연 2회 - 퇴직자 보안점검 - 악성메일 모의 훈련 - 수탁사 점검 - 뉴스레터 - EQST insight 간행물

에스케이쉴더스(주) 대표이사 박진효는 상기 공시 내용에 거짓이 없음을 확인하였습니다.

2022. 6. 28.

에스케이쉴더스(주) 대표이사 박진효 (인)

※ 출처: 22년 에스케이쉴더스 주식회사 정보보호 현황 (정보보호 공시 종합포털)

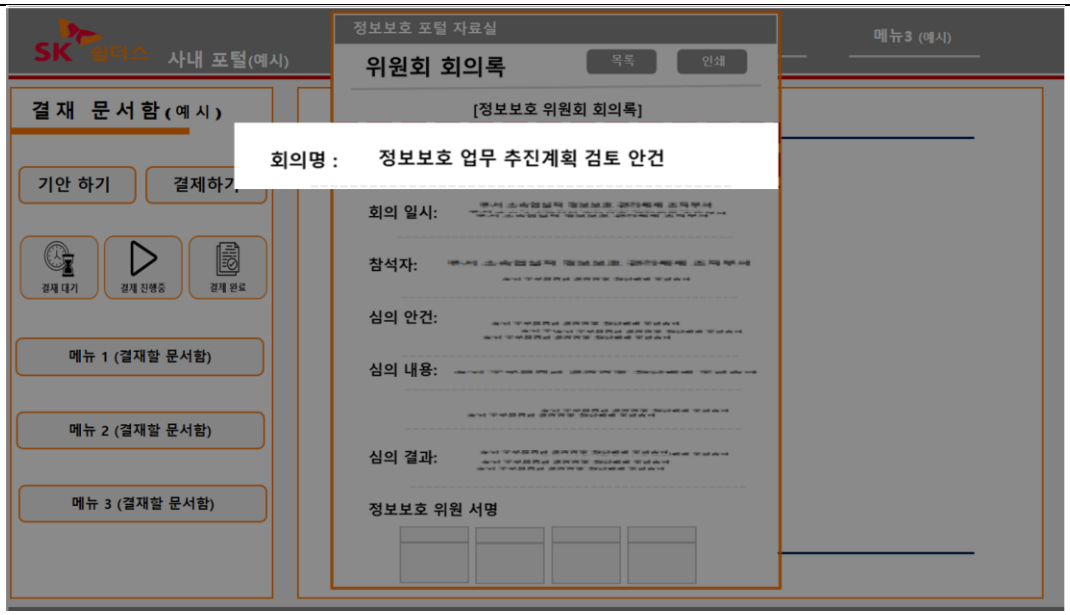
◇ 연도별 정보보호 및 개인정보보호 업무 세부추진 계획을 수립·시행하고, 그 추진결과에 대한 심사분석 · 평가를 실시하고 있는가?

→ 정보보호 및 개인정보보호 활동 효과성 검토

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

① 정보보호 최고책임자(CISO)는 해당 년도 정보보안 세부 추진계획을 수립 당해년도 정보보호 업무에 대해 심사 분석하여 부진 사항에 대한 시정대책을 강구한다.

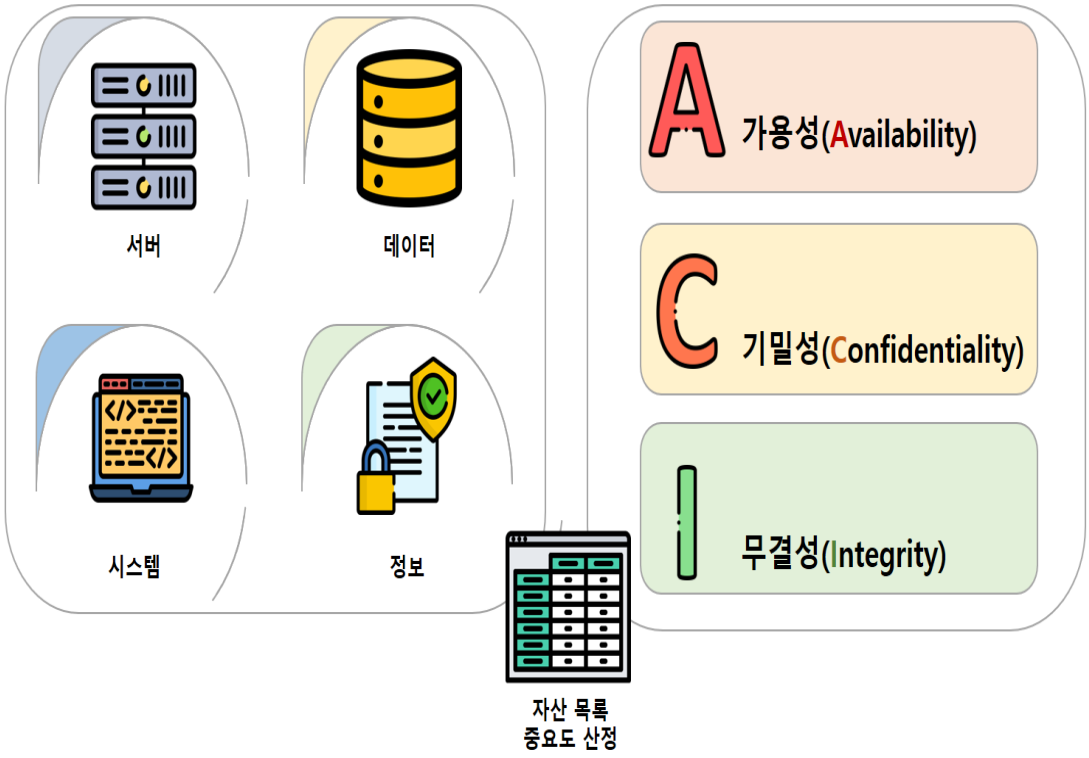
② 정보보호 최고책임자(CISO)는 당해 년도 정보보호업무 추진계획 수립 후 정보보호 위원회의 심의를 거쳐 공표한다.



※ 경영진 정보보호 활동(이해를 돕기 위한 예시작성)

1.2 위험관리

1.2.1 정보자산 식별

세부분야	1.2.1 정보자산 식별
인증 기준	조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.
주요 확인사항	• 정보자산의 분류기준을 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 정보자산목록을 최신으로 유지하고 있는가?
기준 요약도	
운영 방안	**◇ 정보자산의 분류기준을 수립하고 정보보호 및 개인정보보호 관리체계 범위 내의 모든 자산을 식별하여 목록으로 관리하고 있는가?** **→ 정보자산 분류 및 식별** 「**정보 자산관리지침**」 제 ○○조 (정보자산의 분류) ① 정보자산은 다음 각 호와 같이 분류하고 최신화 관리해야한다. ≫ 정보(전자문서, 종이문서)

≫ 서버, 스토리지

≫ 네트워크, 정보보안시스템

≫ 응용프로그램(소프트웨어)

≫ 업무용단말기(노트북, 테블릿, 모바일 등)

≫ 보조기억매체(USB, 외장형하드디스크)

≫ 물리적시설(출입통제 설비, 항온항습기, UPS, 소화설비, 냉.난방 설비, 발전기 등)

정보자산 관리대장

정보보호담당자	정보보호최고책임자

구분			호스트명	자산명	IP주소	자산위치	장비 성능 상세내역					관리번호	관리부서	담당자	자산 가치평가		
							CPU	메모리	HDD	OS	모델명				기밀성	무결성	가용성
무형자산	정보																
	응용프로그램																
유형자산	서버	DNS															
		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 성능 상세내역	관리번호	관리부서	관리자	자산 가치평가		
							기밀성	무결성	가용성
발전기									
항온항습기									
소방시설									
UPS									

※ 자산관리대장(이해를 돕기 위한 예시 작성)

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

→ 정보자산 목록 및 중요도 산정

「정보 자산관리지침」제 ○○조 (정보자산 중요도 평가 및 재검토)

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(Availabilty)	중요도	상세 기준
심각	3	• 치명적인 영향을 초래할 수 있는 경우 (예시)
주위	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)
주위	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)
주위	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 정보자산목록을 최신으로 유지하고 있는가?

→ 부서별 정보시스템 자산 현행화

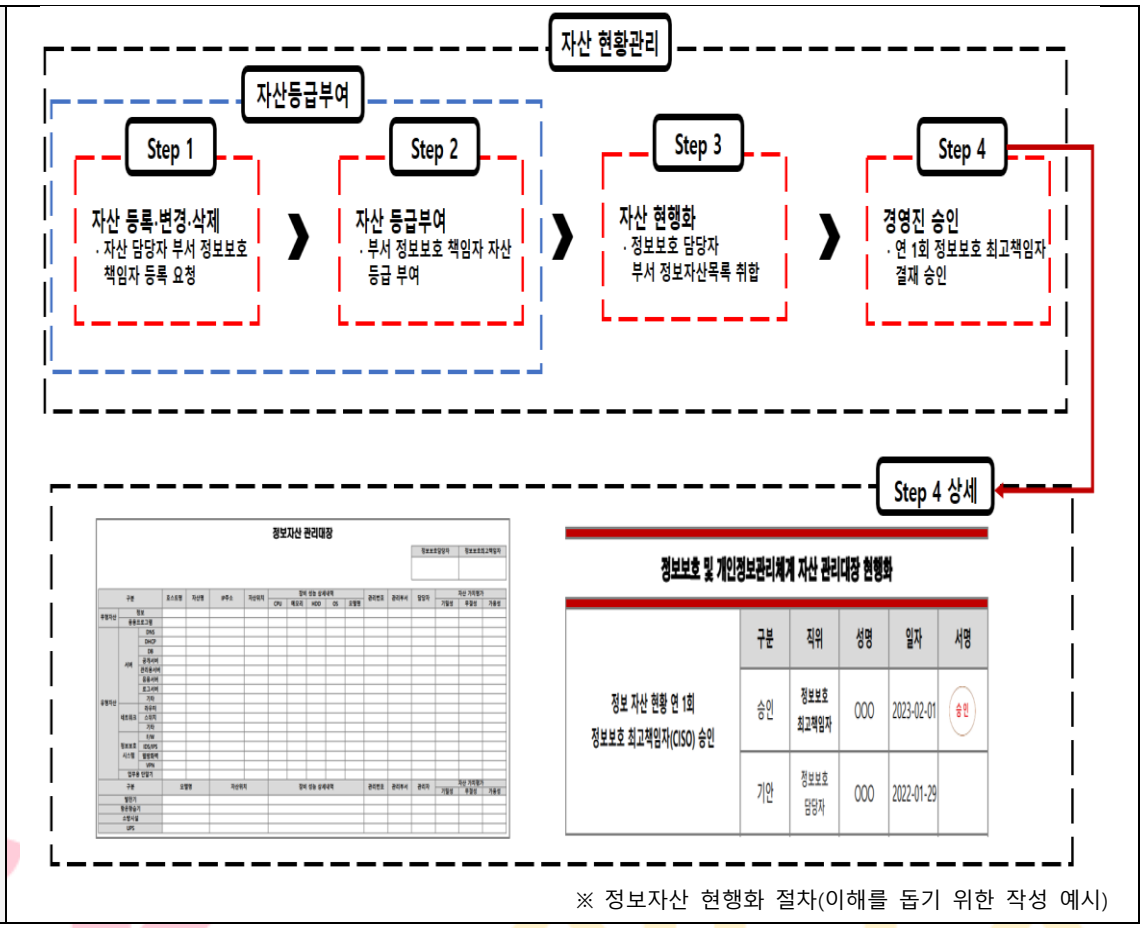
「**정보보호 관리체계 운영지침**」 제 ○○조 (정보자산 등록)

① 자산 등록·변경·삭제 은 정보 소유자가 필요 시 부서 정보보호책임자에 허가를 득하고 부서 자산목록에 직접등록한다.

② 부서 정보보호책임자는 등록자산에 보안등급에 따라 자산코드를 부여하여야 한다.

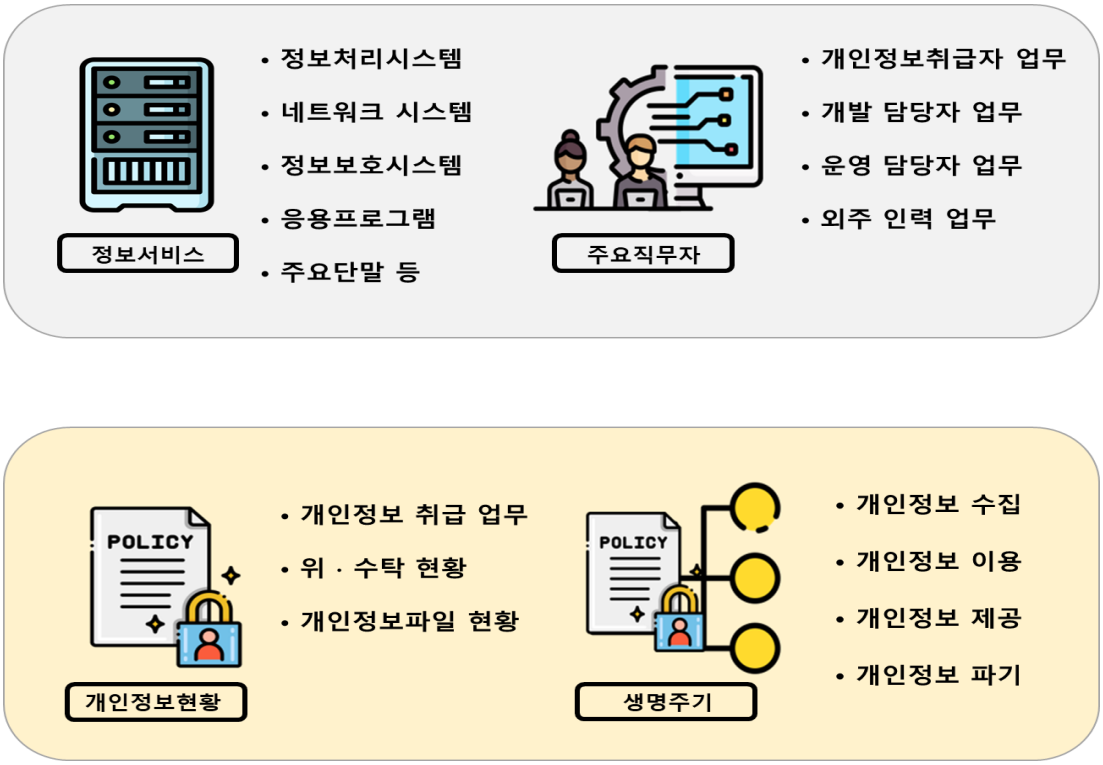
③ 정보보호담당자는 분기별 각 부서의 자산목록을 검토 취합 현행화 한다.

④ 정보보호담당자는 년 1회 자산 실사하여야 하며, 그 결과를 정보보호최고책임자에 보고해야 한다.



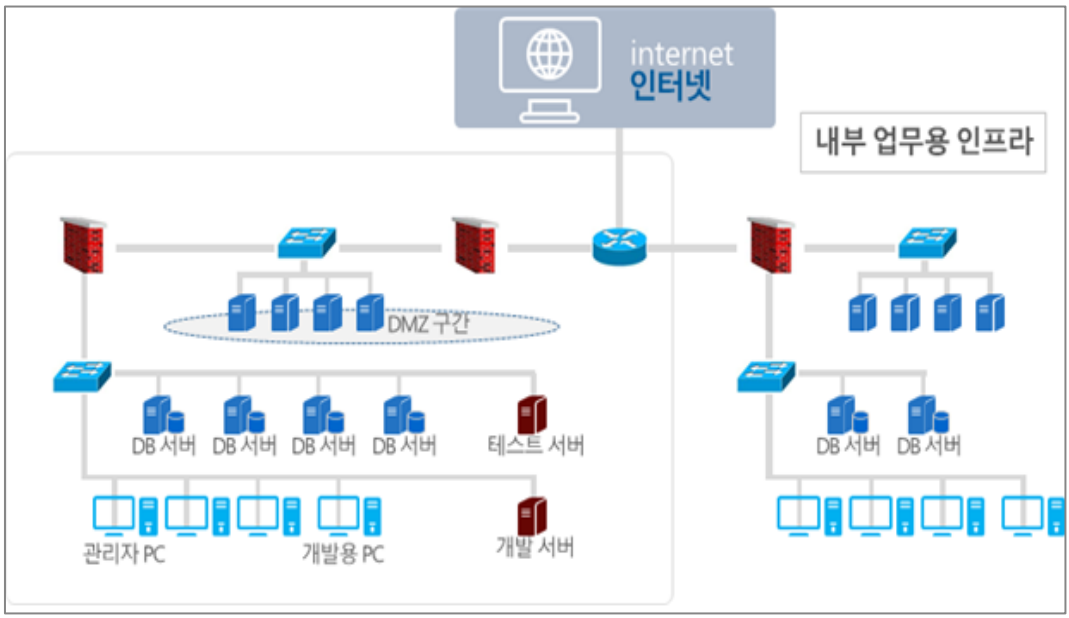
※ 정보자산 현행화 절차(이해를 돕기 위한 작성 예시)

1.2.2 현황 및 흐름분석

<table>
<tr><th>세부분야</th><th>1.2.2 현황 및 흐름분석</th></tr>
<tr><td>인증기준</td><td>관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 관리체계 전 영역에 대한 정보서비스 현황을 식별하고 업무 절차와 흐름을 파악하여 문서화하고 있는가?
• 관리체계 범위 내 개인정보 처리 현황을 식별하고 개인정보의 흐름을 파악하여개인정보 흐름도 등으로 문서화하고 있는가?
• 서비스 및 업무, 정보자산 등의 변화에 따른 업무절차 및 개인정보 흐름을 주기적으로 검토하여 흐름도 등 관련 문서의 최신성을 유지하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 관리체계 전 영역에 대한 정보서비스 현황을 식별하고 업무 절차와 흐름을 파악하여 문서화하고 있는가?

→ 정보시스템 흐름 파악
① 관리체계 범위 내 모든 정보서비스 현황
≫ DB 서버, 웹서버, 로그 모니터링 시스템 등
≫ 네트워크 장비(예. 라우터, 스위치 등)
≫ 정보보호 관련 장비 (예. 방화벽, 침입탐지시스템, 침입방지시스템 등)</td></tr>
</table>

≫ DMZ 구역, VPN 구간 등



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

② 정보서비스별 업무 절차 및 흐름 파악

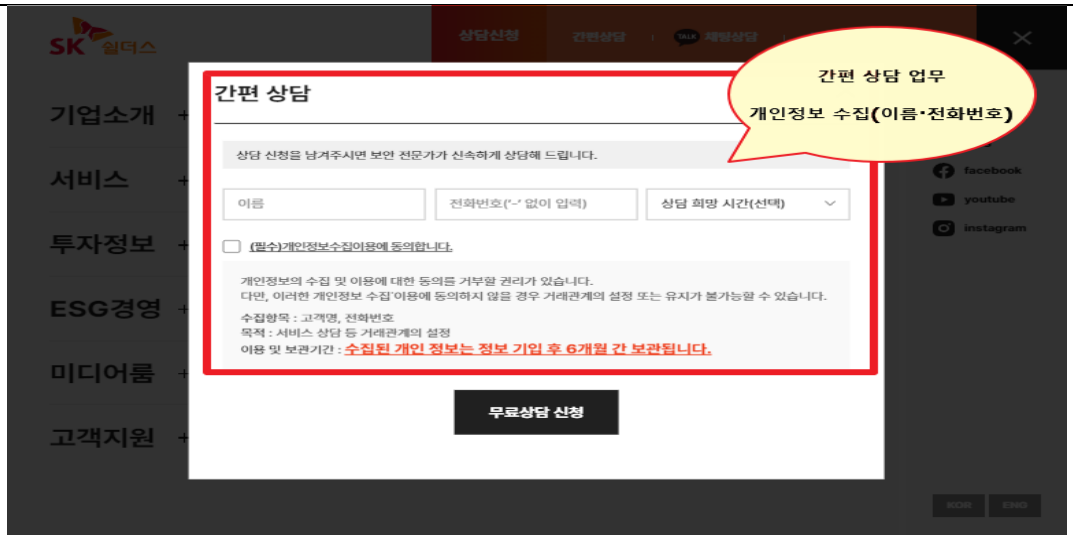
③ 업무 절차 및 흐름에 대한 문서화

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

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

→ 개인정보 생명주기(Life Cycle)

① 개인정보 활용 업무 파악(간편상담 업무 예시)



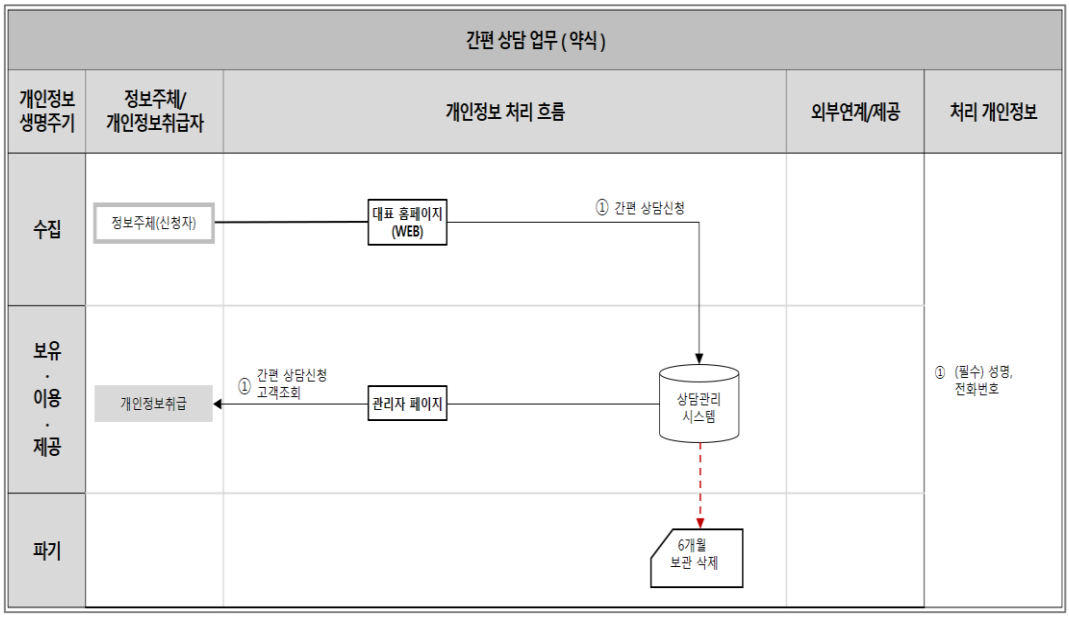
※ 출처: SK쉴더스 홈페이지(SK쉴더스)

≫ "간편 상담"업무 개인정보 흐름표 약식

개인정보 흐름표 (약식 예시)

번호	업무	수집항목	수집경로	수집주기	수집부서	보관기간
1	간편상담	이름 / 전화번호	대표 홈페이지	상시	고객상담팀	6개월보관
2	…	…	…	…	…	…

≫ "간편 상담" 업무 개인정보 흐름도



※ 개인정보흐름도(이해를 돕기 위한 예시)

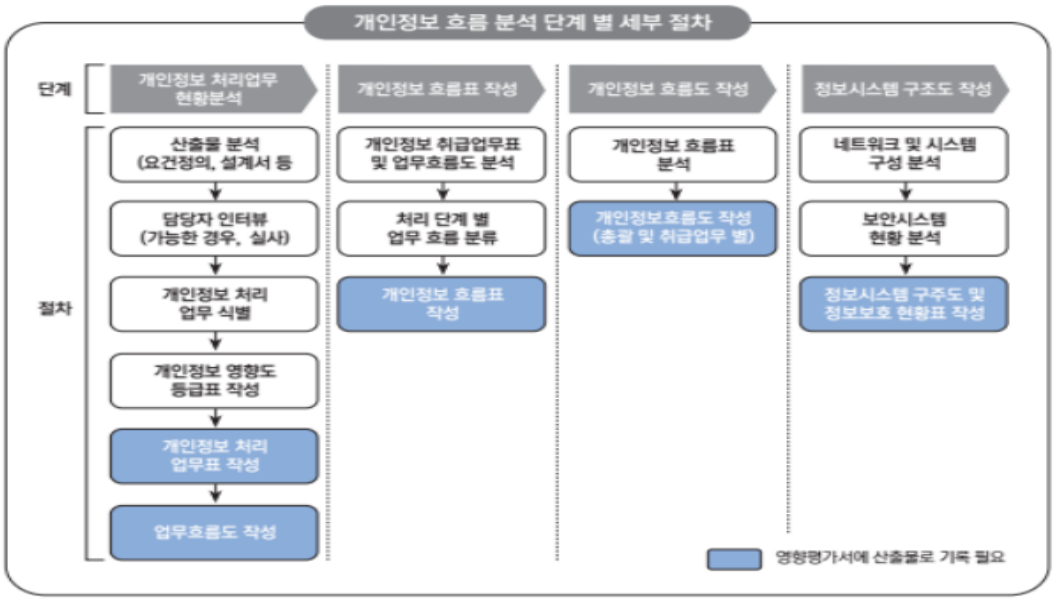
→ 개인정보 흐름 분석 단계별 세부절차

① 개인정보 처리 업무 현황분석

② 개인정보 흐름표 작성

③ 개인정보 흐름도 작성

④ 정보시스템 구성도 작성



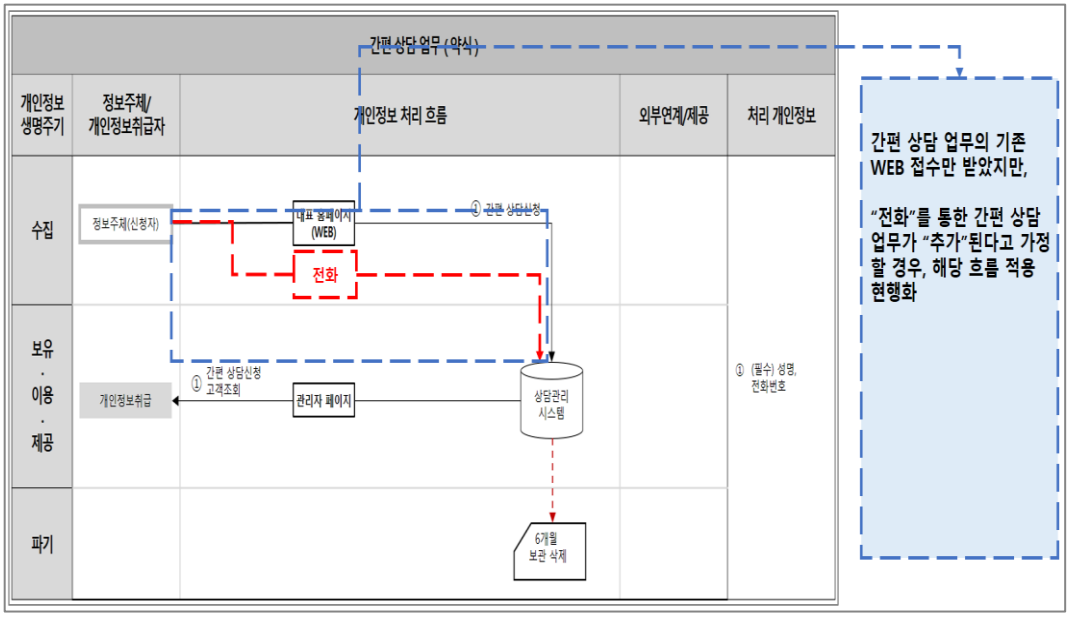
※ 출처: 개인정보 영향평가 수행안내서((개인정보보호위원회·KISA)

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

→ 연 1회 이상 정보 흐름 최신성 유지

① 기존 서비스, 업무 및 개인정보 흐름의 변화 여부

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



※ 개인정보흐름도 변경사항 반영(이해를 돕기 위한 예시)

1.2.3 위험 평가

<table>
<tr><th>세부분야</th><th>1.2.3 위험 평가</th></tr>
<tr><td>인증
기준</td><td>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.</td></tr>
<tr><td>주요
확인사항</td><td>• 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 위험관리계획을 매년 수립하고 있는가?
• 위험관리계획에 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?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 조직 또는 서비스의 특성에 따라 다양한 측면에서 발생할 수 있는 위험을 식별하고 평가할 수 있는 방법을 정의하고 있는가?

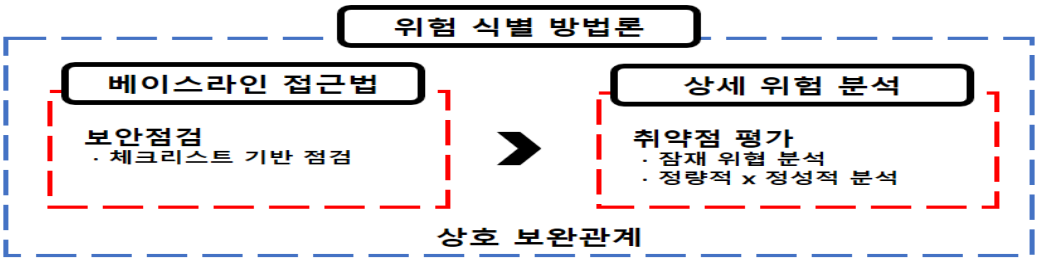
→ 위험평가 방법 문서화 (예시)

「위험평가 관리지침」 제 ○○조 (위험식별)</td></tr>
</table>

① 정보 자산의 위험평가 방법은 각 호와 같이 적용한다.

≫ 베이스라인 접근법: 식별 정보자산 공통적용(Gap analysis)

≫ 상세 위험 분석: 자산분석·위협평가·취약성 평가를 거쳐 위험식별



※ 위험관리방법론 (이해를 돕기 위한 예시)

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

→ 수행인력, 기간 대상, 방법, 예산 등 계획 반영

「위험평가 관리지침」 제 ○○조 (위험평가)

① 위험관리계획을 수립하고 위험관리계획에 따라 연 1회 이상 위험평가를 실시한다.

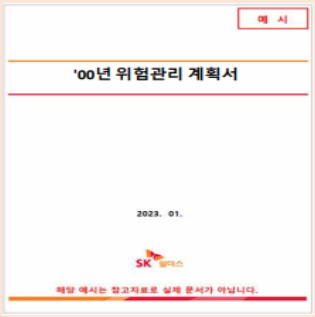
≫ 인력·대상·방법·예산 포함

≫ 정보서비스 현황분석 및 흐름분석이 반영된 위험평가

≫ 법적 요구사항 및 정보보호 관리체계 인증 기준 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	승 인
상신	정보보호 담당자	OOO	2022-12-20	-


예 시
'00년 위험관리 계획서
2023. 01.
SK 쉴더스
해당 예시는 참고자료로 실제 문서가 아닙니다.

※ 위험관리계획서 (이해를 돕기 위한 예시)

◇ 위험관리계획에 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

≫ 위험평가는 연 1회 이상 정기적으로 수행하되 조직의 변화, 신규시스템 도입 등 중요한 사유가 발생한 경우 해당 부분에 대하여 정기적인 위험평가 이외에 별도로 위험평가 수행

≫ 서비스 및 정보자산의 현황과 흐름분석 결과 반영

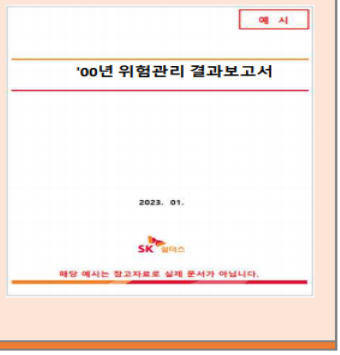
≫ 최신 법규를 기반으로 정보보호 및 개인정보보호 관련 법적 요구사항 준수 여부 확인

≫ 정보보호 및 개인정보보호 관리체계 인증기준의 준수 여부 확인

≫ 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	승 인
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?

→ 위험도 산정기준 마련

「**위험평가 관리지침**」 제 ○○조 (위험 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)

→ 위험수준(DOA) 산정

「**위험평가 관리지침**」 제 ○○조 (위험 관리)

① 정보보호대책 수립 단계에서는 우선 위험을 허용 가능한 위험수준(DoA) 이하로 감소시키기 위해 필요한 정보보호 대책을 선택하고, 이 중 유사한 대책들은 필요 시 하나의 이행과제로 묶는다.

≫ **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 것이 심각도보다 먼저 고려한다.

≫ **수용**: 위험도가 수용 단계이면, 사건발생의 심각도나 가능성을 검토하여 위험을 "현실적으로 타당한 최저수준"으로 경감하기 위한 수단을 강구해야 한다. 잔여 위험은 비용등을 고려하여 효과적으로 적용하고 정보보호책임자의 승인하에

수용 가능하게 한다.

≫ 위험이 허용가능하면 위험 가능성이 없거나 또는 우려할 만큼 심각하지 않다는 것이다. 위험을 더 감소시키기 위한 검토가 지속적으로 이루어져야 한다

위험도 및 조치수준

위험도			위험조치수준
심각	수용불가	6 ~ 9 점	• 문제점 개선되지 않으면 운영중단
주위	수용	3 ~ 5 점	• 위험경감조치를 통한 수용 가능
경미	허용가능	1 ~ 2 점	• 별다른 조치없이 운영

위험 관리대장

자산명	우려사항	잠재 위험 수준		위험평가 (위험도*자산등급)	조치 계획	조치비용	위험완화 기대등급
		위험도	자산등급				
AA- 00	위탁사 보안 필요수준 미흡	2(중)	3(상)	6(심각)	위탁사 점검	0000천원	3(주위)
....	....	...	...	...	...	...	...

※ DOA 선정 예시(이해를 돕기 위한 예시)

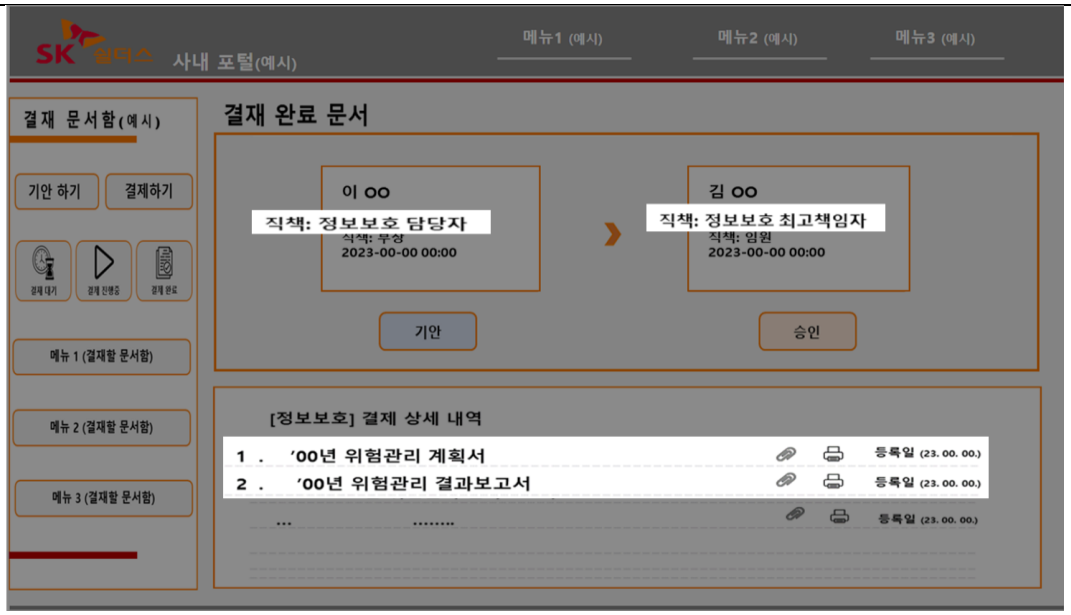
◇ 위험식별 및 평가 결과를 경영진에게 보고하고 있는가?

→ 식별 위험에 대한 경영진 차원의 보호대책 수립

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

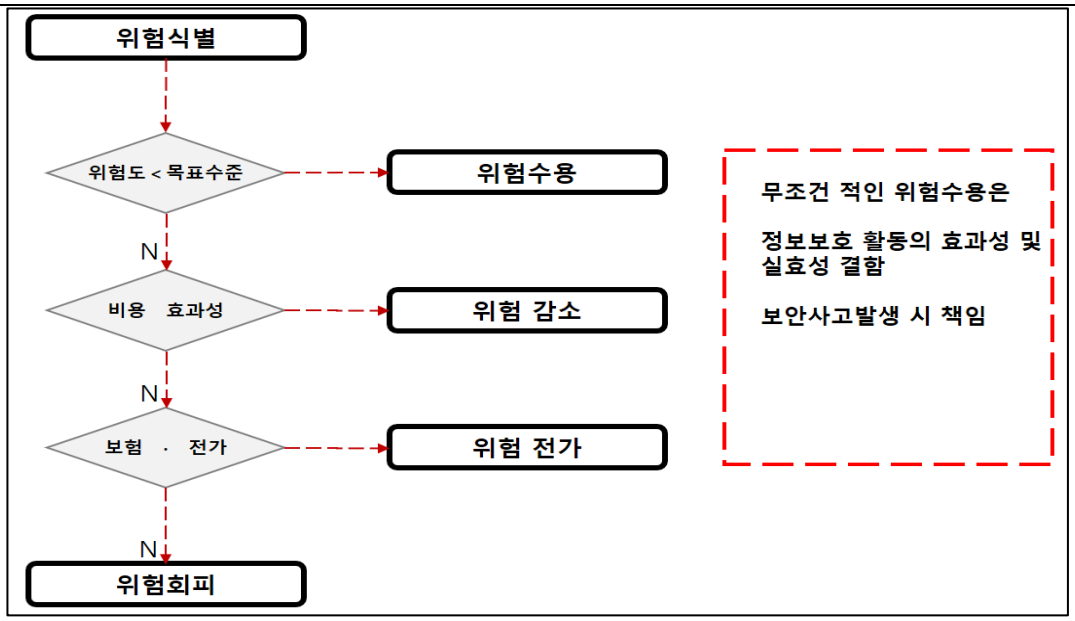


※ 경영진 보고 승인(이해를 돕기위한 예시)

1.2.4 보호대책 선정

<table>
<tr><th>세부분야</th><th>1.2.4 보호대책 선정</th></tr>
<tr><td>인증
기준</td><td>위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 조직에 적합한 보호대책을 선정하고, 보호대책의 우선순위와 일정·담당자·예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다</td></tr>
<tr><td>주요
확인사항</td><td>• 식별된 위험에 대한 처리 전략(감소, 회피, 전가, 수용 등)을 수립하고 위험처리를 위한 보호대책을 선정하고 있는가?
• 보호대책의 우선순위를 고려하여 일정, 담당부서 및 담당자, 예산 등의 항목을 포함한 보호대책 이행계획을 수립하고 경영진에 보고하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 식별된 위험에 대한 처리 전략(감소, 회피, 전가, 수용 등)을 수립하고 위험처리를 위한 보호대책을 선정하고 있는가?

→ 위험 처리 전략 수립
① 수용 가능한 목표 위험 수준과 비교(목표위험 수준과 같거나 이하일 경우 수용)
② 목표 위험보다 높을 경우 목표 위험 수준까지 감소시킬 대책 구현절차 수립
③ 대책 구현 및 유지에 대한 비용과 감소되는 위험을 비교하여 가치평가
④ 대책구현으로 목표 위험수준 이하고 감소될 경우 대책 선정</td></tr>
</table>



※ 위험선정 기준(이해를 돕기 위한 예시)

◇ 보호대책의 우선순위를 고려하여 일정, 담당부서 및 담당자, 예산 등의 항목을 포함한 보호대책 이행계획을 수립하고 경영진에 보고하고 있는가?

→ 보호대책 구현을 위한 우선 순위 결정

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

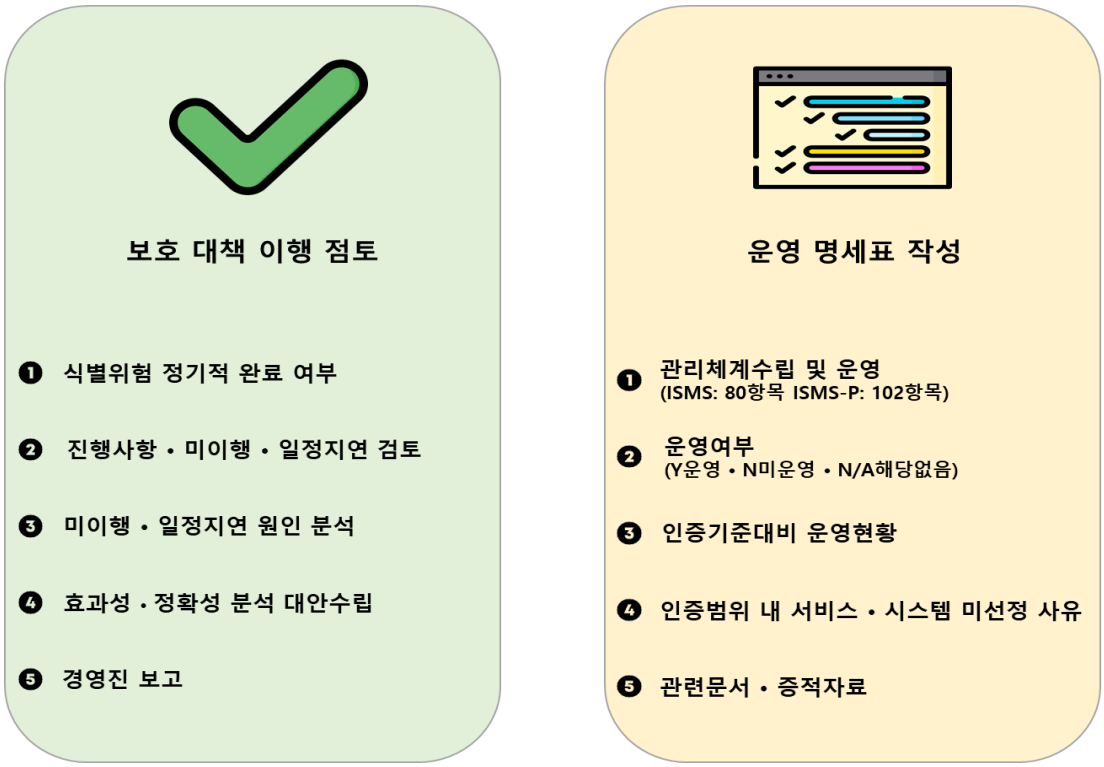
≫ 즉시 교정 가능한 취약점 제거

≫ 정책 및 절차 수립 및 변경

≫ 시스템 도입 등의 예산이 필요한 정보보안 세부 업무 계획 수립

1.3 관리체계 운영

1.3.1 보호대책 구현

<table>
<tr><th>세부분야</th><th>1.3.1 보호대책 구현</th></tr>
<tr><td>인증
기준</td><td>선정한 보호대책은 이행계획에 따라 효과적으로 구현하고, 경영진은 이행결과의 정확성과 효과성 여부를 확인하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 이행계획에 따라 보호대책을 효과적으로 구현하고 이행결과의 정확성 및 효과성 여부를 경영진이 확인할 수 있도록 보고하고 있는가?
• 관리체계 인증기준별로 보호대책 구현 및 운영 현황을 기록한 운영명세서를 구체적으로 작성하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 이행계획에 따라 보호대책을 효과적으로 구현하고 이행결과의 정확성 및 효과성 여부를 경영진이 확인할 수 있도록 보고하고 있는가?

→ 보호대책 이행 계획 수립 및 경영진 보고
① 보호대책 구현이행 성과 보고 경영진 보고</td></tr>
</table>

정보보호 및 개인정보보호 이행계획 성과보고 (예시)

과제명	추진계획	추진실적	증빙자료	비고
· 외부자 보안이행관리	· 위탁사 보안실태점검	· IT 위탁사 0건 정보보호 관리 점검 실시	· '00년 위탁사 점검결과보고서	
....	....	...	...	...

정보보호 및 개인정보 부진과제 및 향후추진계획 (예시)

부진 과제명	원인 및 상세 사유	차년도 추진계획
....	....	....

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: 이행 성과보고(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) 초과 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 보호대책수립(이해를 돕기 위한 예시)

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

→ 보호대책 및 운영 현황 운영명세서 기록 작성

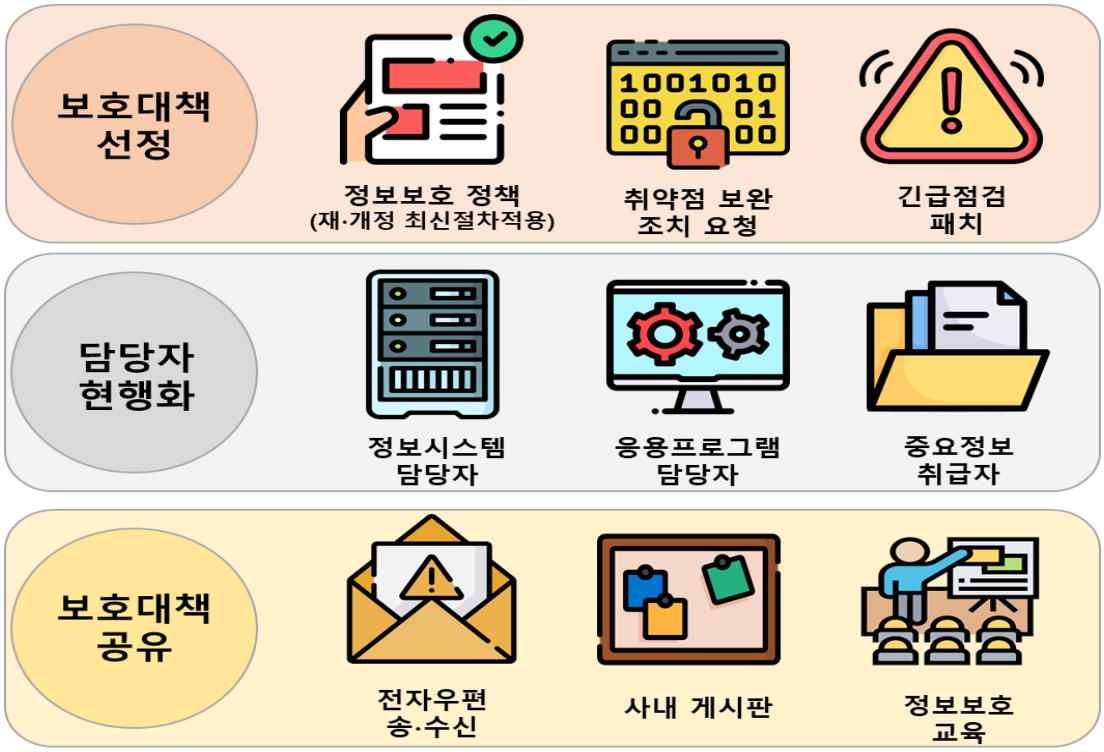
① 보호 대책 구현 현황 운영명세서 작성

ISMS&ISMS-P 운영명세서(기업명: (예명) Min'S컴퍼니)

분야		항목		상세내용	①운영 여부	②인증구분	③운영현황 (또는 미선택사유)	④관련문서 (정책, 지침 등 세부조항번호까지)	⑤기록 (증적자료)
1.관리체계 수립 및 운영									
1.1.	관리체계 기반 마련	1.1.5	정책 수립	정보보호와 개인정보보호 정책 및 시행문서를 수립·작성하며, 이때 조직의 정보보호와 개인정보보호 방침 및 방향을 명확하게 제시하여야 한다. 또한 정책과 시행문서는 경영진 승인을 받고, 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.	Y	ISMS-P	....	....	....
1.2.	위험 관리	1.2.1	정보자산 식별	조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.	Y	ISMS-P	....	....	....
2.3.	외부자보안	2.3.3	외부자 보안 이행 관리	계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보보호 요구사항에 따라 외부자의 보호대책 이행 여부를 주기적인 점검 또는 감사 등 관리·감독하여야 한다.	Y	ISMS-P	• IT 위탁사 보안관리체계 수립 및 위탁사 상반기(정기) 하반기(이행) 점검을 실시 하고 있음.	**인적 보안관리지침** 제 0조 (위탁보안 관리)	① IT 위탁사 점검 계획서 ② 위탁사 상세점검 결과보고서 ③ IT위탁사 점검 결과보고서
		2.3.4	외부자 계약 변경 및 만료 시 보안	외부자 계약만료, 업무종료, 담당자 변경 시에는 제공한 정보자산 반납, 정보시스템 접근계정 삭제, 중요정보 파기, 업무 수행 중 취득정보의 비밀유지 확약서 징구 등의 보호대책을 이행하여야 한다.	Y	ISMS-P	....	....	

※ 정보보호 운영명세서(이해를 돕기 위한 예시)

1.3.2 보호대책 공유

세부분야	1.3.2 보호대책 공유
인증 기준	보호대책의 실제 운영 또는 시행할 부서 및 담당자를 파악하여 관련 내용을 공유하고 교육하여 지속적으로 운영되도록 하여야 한다.
주요 확인사항	• 구현된 보호대책을 운영 또는 시행할 부서 및 담당자를 명확하게 파악하고 있는가? • 구현된 보호대책을 운영 또는 시행할 부서 및 담당자에게 관련 내용을 공유 또는 교육하고 있는가?
기준 요약도	
운영 방안	**◇ 구현된 보호대책을 운영 또는 시행할 부서 및 담당자를 명확하게 파악하고 있는가?** **→ 부서 및 담당자 현황 관리** **「정보보호 관리체계 운영지침」** 제 ○○조 (정보자산 등록) ① 신규 자산 등록은 정보 소유자가 필요 시 부서 정보보호책임자에 허가를 득하고 부서 자산목록에 직접등록 해야한다. ② 부서 정보보호책임자는 등록자산에 보안등급에 따라 자산코드를 부여하여야 한다. ③ 정보보호담당자는 매월 각 부서의 자산목록을 검토 현행화 한다. ④ 정보보호담당자는 년 1회 자산 실사하여야 하며, 그 결과를 정보보호위원회에

보고해야 한다.

정보자산 관리대장

정보보호담당자	정보보호최고책임자

부서 및 담당자 현황 관리

구분			호스트명	자산명	IP주소	자산위치	장비 성능 상세 CPU	메모리	HDD	OS			관리부서	담당자	자산 가치평가 기밀성	무결성	가용성
무형자산	정보																
	응용프로그램																
유형자산	서버	DNS															
		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 성능 상세내역	관리번호	관리부서	관리자	자산 가치평가 기밀성	무결성	가용성
발전기									
항온항습기									
소방시설									
UPS									

※ 정보자산관리대장(이해를 돕기위한 예시)

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

→ 담당자 보안지침 공유(예시)

① 담당자에게 사내 메일을 통한 보호대책 구현 요청

※ 담당자 전자메일을 통한 보호 대책 구현 (이해를 돕기 위한 예시)

1.3.3 운영현황 관리

<table>
<tr><th>세부분야</th><th>1.3.3 운영현황 관리</th></tr>
<tr><td>인증
기준</td><td>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.</td></tr>
<tr><td>주요
확인사항</td><td>• 관리체계 운영을 위하여 주기적 또는 상시적으로 수행하여야 하는 정보보호 및 개인정보보호 활동을 문서화하여 관리하고 있는가?
• 경영진은 주기적으로 관리체계 운영활동의 효과성을 확인하고 이를 관리하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 관리체계 운영을 위하여 주기적 또는 상시적으로 수행하여야 하는 정보보호 및 개인정보보호 활동을 문서화하여 관리하고 있는가?

→ 정보보호 및 개인정보보호 활동 작성

「정보보호 관리체계 운영지침」 제 ○○조 (정보보호 계획수립)
① 연간 정보보호 업무계획을 수립하고 '정보보호관리체계 운영현황표'를 작성 및 주기적 검토를 통해 최신상태를 유지한다</td></tr>
</table>

정보보호 관리체계 운영현황표

구분	정보보호관리체계 기준	산출물	담당자	결재자	수행주기	12월	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	진행률	비고
정보보호 정책	1.1.1 정보보호정책승인	정책 승인 증적 - 정책·지침·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	-	년 2회 이상			1										50%	
업무 연속성관리	2.11.4 사고대응훈련	모의훈련 결과보고서	· 정보보호관리자	· 정보보호관리자 · 정보보호책임자	년 1회 이상													0%	
.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	
.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	.....	

※ 정보보호 관리체계 운영현황표(이해를 돕기 위한 예시)

→ 정보보호 및 개인정보보호 활동 참고 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
...	...	...	...	...

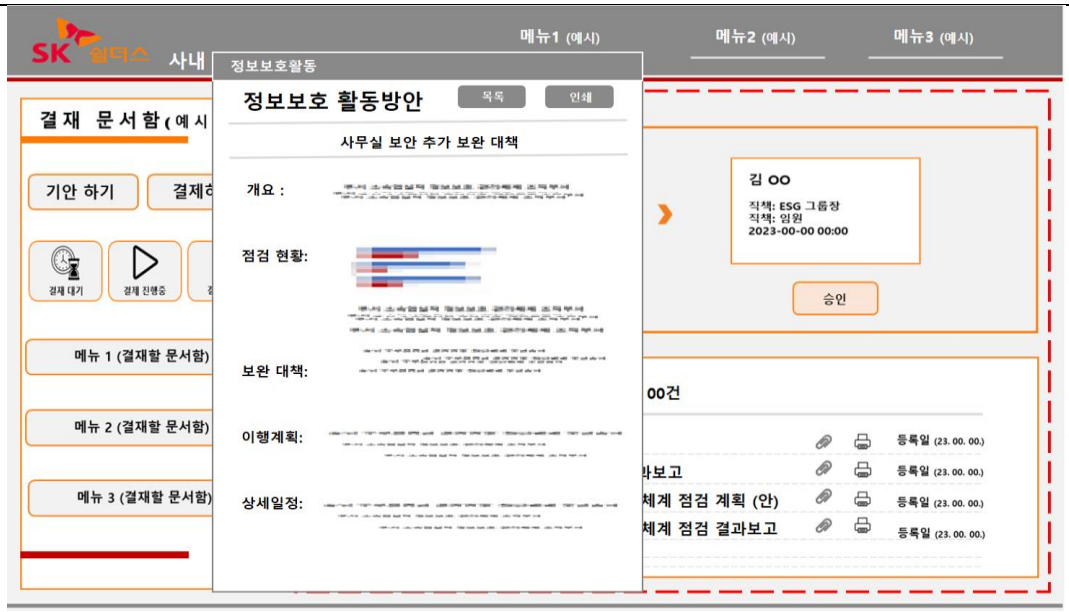
※ 정보보호 관리체계 주기적 활동 문서화(이해를 돕기 위한 예시작성)

◇ 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 효과성검토(이해를 돕기 위한 예시)

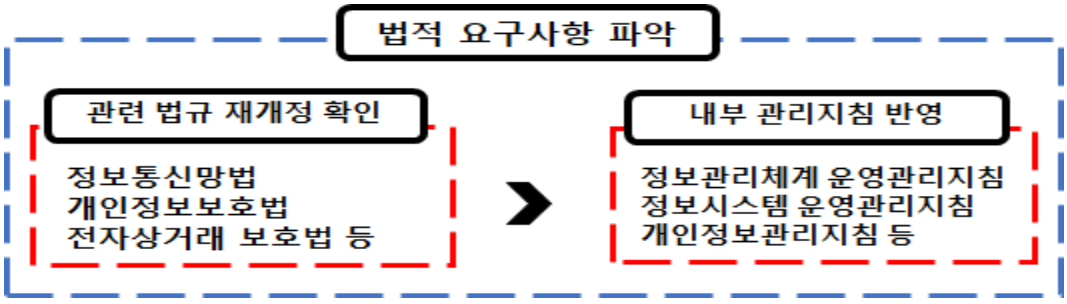
1.4 관리체계 점검 및 개선

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?** **→ 법적 요구사항을 파악하여 최신성을 유지** **「정보보호 관리체계 운영지침」** 제 ○○조 (정보보호정책 검토) ① 정보보호 정책의 타당성 및 효과성을 연 1회 이상 검토하고, 관련 법규 변경 및 내외부의 중대한 보안사고 발생 시 추가 검토하여 상시 반영해야한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 [시행 2020. 6. 11] [법률 제16825호, 2019. 12. 10, 일부개정]	정보통신망 이용촉진 및 정보보호 등에 관한 법률 [시행 2020. 8. 5] [법률 제16955호, 2020. 2. 4, 일부개정]
제1조(목적) 이 법은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다.	제1조(목적) 이 법은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다.
제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.	제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.
1. ~ 5. (생 략)	1. ~ 5. (현행과 같음)
6. "개인정보"란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.	<삭 제>

※ 출처: 정보통신망법 신구대조표(법제처)



※ 법적요구사항 파악(이해를 돕기 위한 예시)

→ 법적 요구사항(개인정보 손해배상 책임 보장제도)

「**개인정보보호법 시행령**」제48조의 7 (손해배상책임의 이행을 위한 보험 등 가입 대상자의 범위 및 기준 등)

≫ 전년도(법인의 경우 전 사업연도를 말한다)의 매출액이 5천만원 이상일 것

≫ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자수가 일일평균 1천명 이상일 것

가입 대상 개인정보처리자의 가입금액 산정요소		최저가입금액 (최소적립금액)
매출액	이용자수	
800억원 초과	100만명 이상	10억원
50억원 초과 800억원 이하		5억원
5천만원 이상 50억원 이하		2억원
800억원 초과	10만명 이상 100만명 미만	5억원
50억원 초과 800억원 이하		2억원
5천만원 이상 50억원 이하		1억원
800억원 초과	1천명 이상 10만명 미만	2억원
50억원 초과 800억원 이하		1억원
5천만원 이상 50억원 이하		5천만원

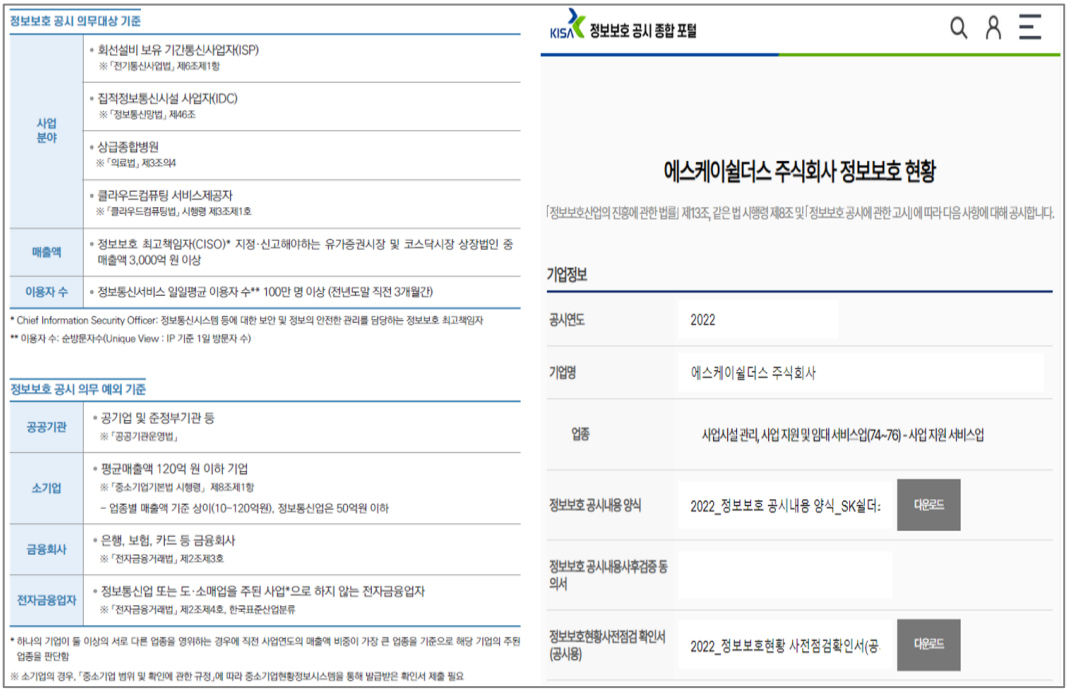
◆ 보험가입금액 : 계약상 보상 최고한도액으로, 보험계약자가 보험계약을 체결 시 약정한 금액
◆ 보험료 : 보험계약에 의하여 보험계약자가 보험회사에 납입한 금액
◆ 이용자수 : 보험(공제)에 가입하거나 준비금을 적립해야 할 연도의 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 일일 이용자수 평균
◆ 매출액 : 전년도(법인의 경우 전 사업연도)의 매출액

※ 출처: 개인정보 손해배상책임 보장제도안내서(개인정보보호 위원회)

→ 법적 요구사항(정보보호 공시)

「정보보호산업의 진흥에 관한 법률」제13조 (정보보호 공시)

① 정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자는「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조 1항 2호에 따른 정보통신서비스를 이용하는 자의 안전한 인터넷이용을 위하여 정보보호 투자 및 인력 현황, 정보보호 관련 인증 등 정보보호 현황을 대통령령으로 정하는 바에 따라 공개할 수 있다. 이 경우「자본시장과 금융투자업에 관한 법률」제159조에 따른 사업보고서 제출대상 법인은 같은 법 제391조에 따라 정보보호 준비도 평가 결과 등 정보보호 관련 인증 현황을 포함하여 공시할 수 있다.



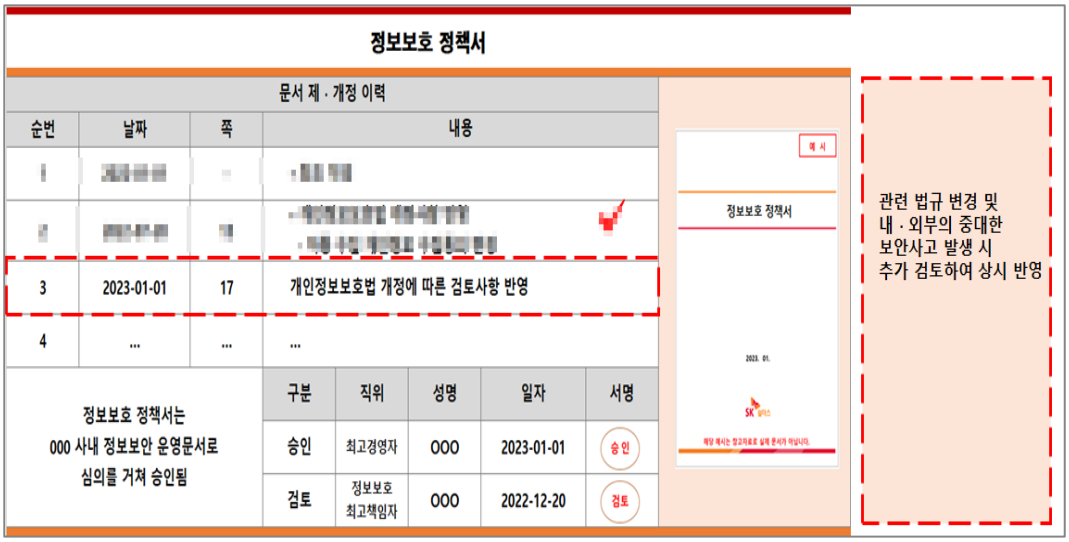
※ 출처: 정보보호 공시가이드라인 (과학기술정보통신부·KISA)

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

→ 정보보호 정책서 법적 변경 사항 타당성 검토

「**정보보호 관리체계 운영지침**」 제 ○○조 (정보보호정책 검토)

① 정보보호 정책의 타당성 및 효과성을 연 1회 이상 검토하고, 관련 법규 변경 및 내외부의 중대한 보안사고 발생 시 추가 검토하여 상시 반영해야한다



정보보호 정책서

문서 제·개정 이력

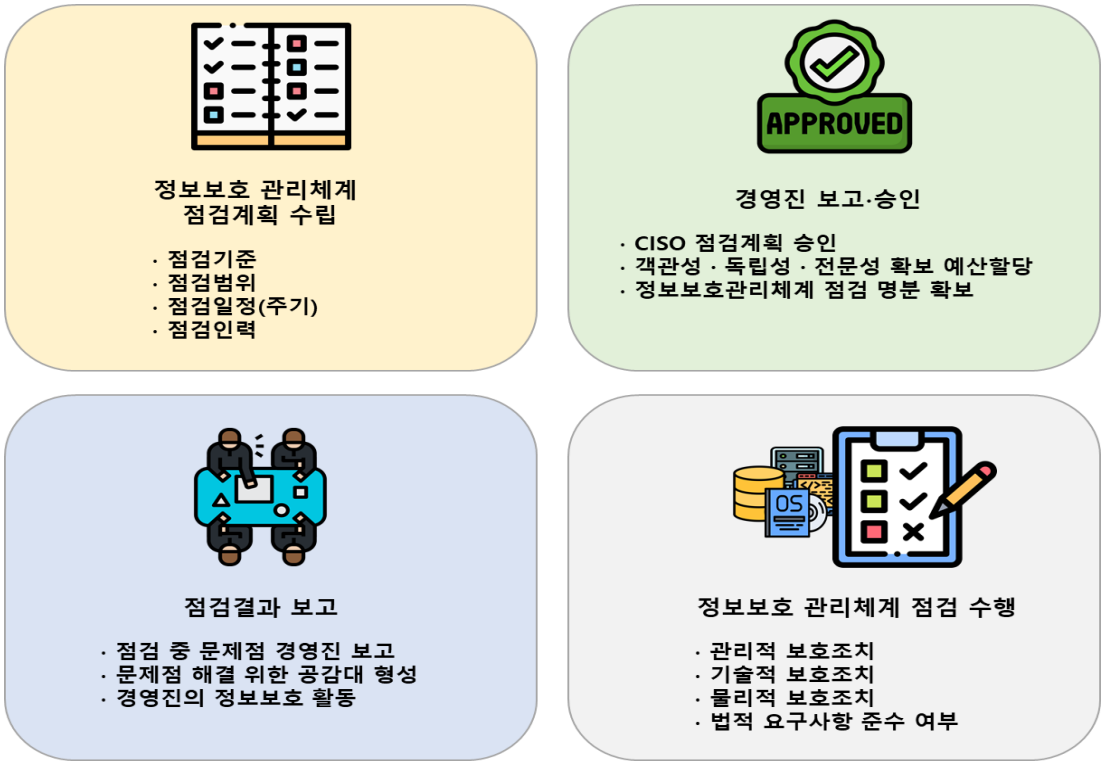
순번	날짜	쪽	내용
1	[redacted]	[redacted]	[redacted]
2	[redacted]	[redacted]	[redacted]
3	2023-01-01	17	개인정보보호법 개정에 따른 검토사항 반영
4	...	...	...

정보보호 정책서는
000 사내 정보보안 운영문서로
심의를 거쳐 승인됨

구분	직위	성명	일자	서명
승인	최고경영자	000	2023-01-01	승인
검토	정보보호 최고책임자	000	2022-12-20	검토

※ 년 1회 검도 문서 재·개정 사항 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 점검계획 수립** **「정보보호 관리체계 운영관리 지침」** 제 ○○조 (보안관리실태점검) ① 정보보호 책임자는 자체 보안관리실태점검을 연 1회 이상 실시하여야 하며, 각 분야의 점검항목은 '정보보호 관리실태 점검항목'을 기준으로 한다.

≫ 점검기준: 정보보호 및 개인정보보호 관리체계 인증기준 포함

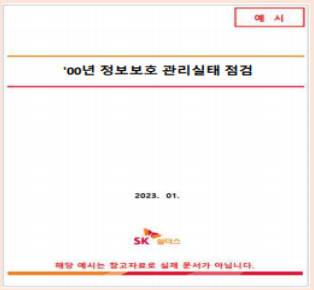
≫ 점검범위: 전사 또는 인증범위 포함

≫ 점검주기: 최소 연 1회 이상 수행 필요

≫ 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	승 인
상신	정보보호 담당자	OOO	2022-12-20	-



※ 정보보호 관리실태 점검 계획(참고예시)

◇ 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

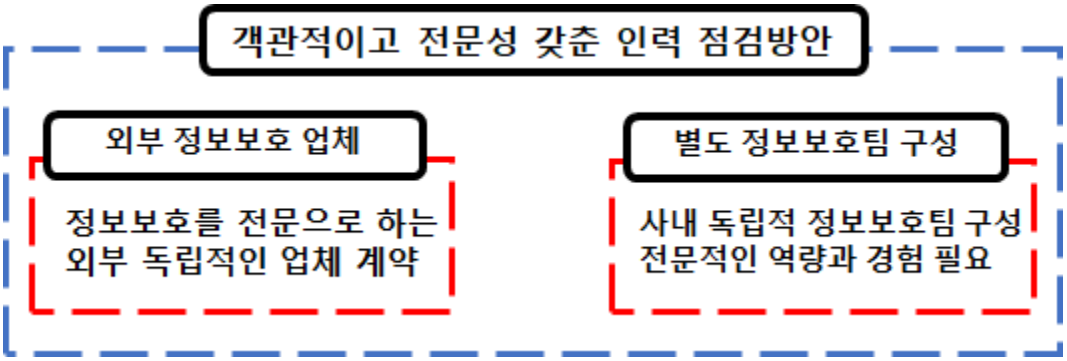
① 정보보호최고책임자(CISO) 역할

≫ 점검의 객관성, 독립성 및 전문성을 확보할 수 있도록 점검조직 구성

≫ 점검 계획에 따라 연 1회 이상 점검 수행

≫ 점검 결과 발견된 문제점에 대해서는 조치계획을 수립·이행하고, 조치 완료 여부에 대하여 추가 확인

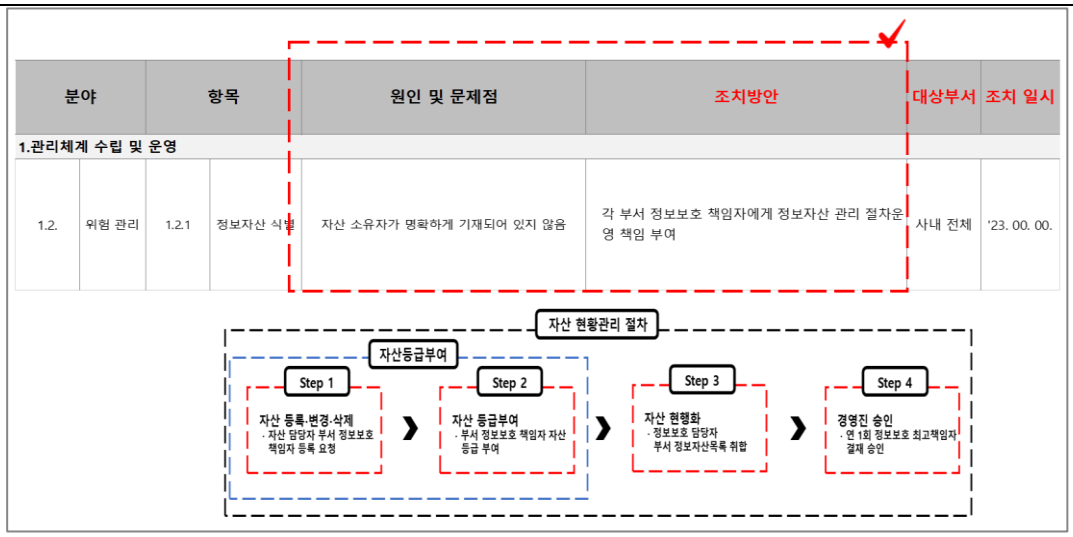
≫ 점검 결과보고서를 작성하여 정보보호 최고책임자 및 개인정보 보호책임자 등 경영진에게 보고



※ 객관적 전문성 갖춘 인력확보 (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 준수검토 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	**◇ 재발방지 및 개선 결과의 정확성 및 효과성 여부를 확인하기 위한 기준과 절차를 마련하고 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

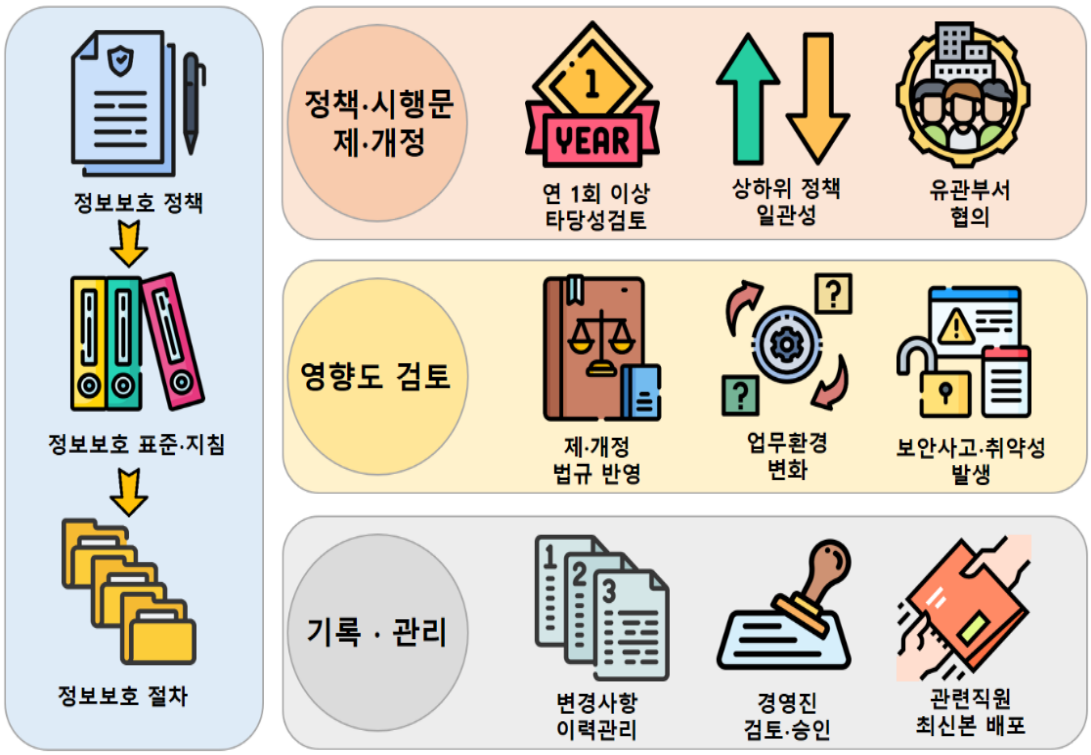
① 재발방지 및 개선조치의 정확성 및 효과성을 측정하기 위하여 관리체계 측면에서의 핵심성과지표

※ 재발방지 효과성 검토(이해를 돕기 위한 예시)

2. 보호대책 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 이력관리하여야 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 이해 관계자의 검토를 받고 있는가? • 정보보호 및 개인정보보호 관련 정책 및 시행문서의 제·개정 내역에 대하여 이력관리를 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

「**정보보호 관리체계 운영지침**」 제 ○○조 (정책 유지관리)

① 정보보호최고책임자는 다음과 같은 상황이 발생한 경우를 제·개정을 통해 관련 규정 및 지침에 반영해야 한다.

≫ 중대한 보안사고 발생

≫ 정보보안 및 개인정보보호 등 관련 법률 제·개정

≫ 새로운 위협 또는 취약성의 발견

≫ 정보보안 및 IT 환경의 중대한 변화 등

② 연 1회 이상 주기적으로 정보보안규정 및 관련 규칙의 타당성을 검토하고 필요시 제·개정을 통해 관련 규정 및 규칙에 반영해야 한다.

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

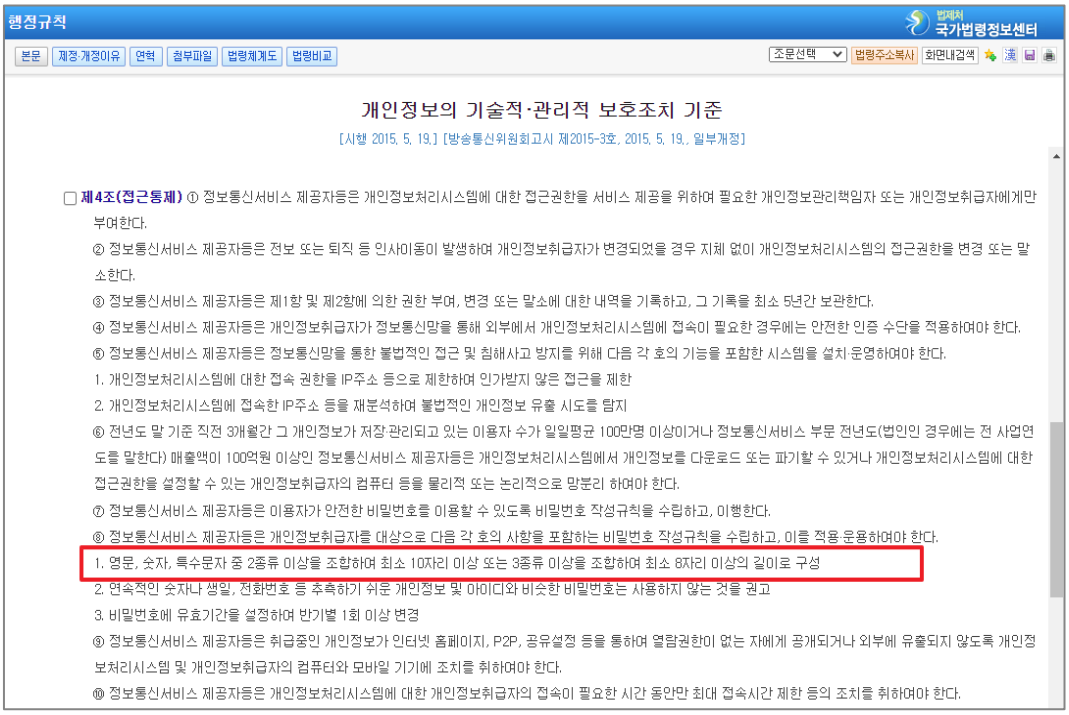
→ 대내외 환경 변화에 따라 지침 재·개정 필요

① 정보보호 및 개인정보보호 관련 법규 제·개정

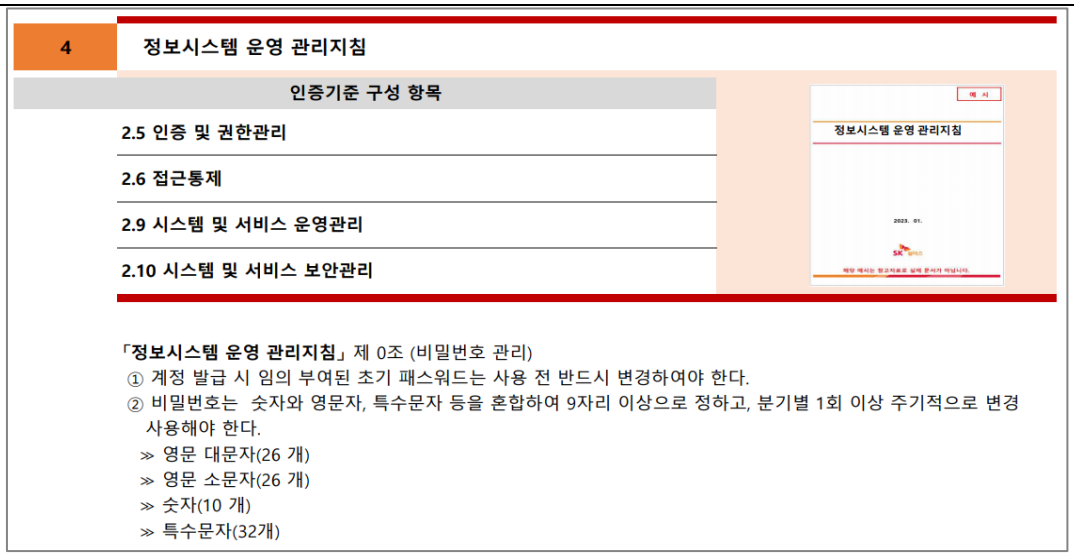
② 비즈니스 환경의 변화(신규 사업 영역 진출, 대규모 조직개편 등)정보보호, 개인정보보호 및 IT 환경의 중대한 변화(신규 보안시스템 또는 IT 시스템 도입 등)

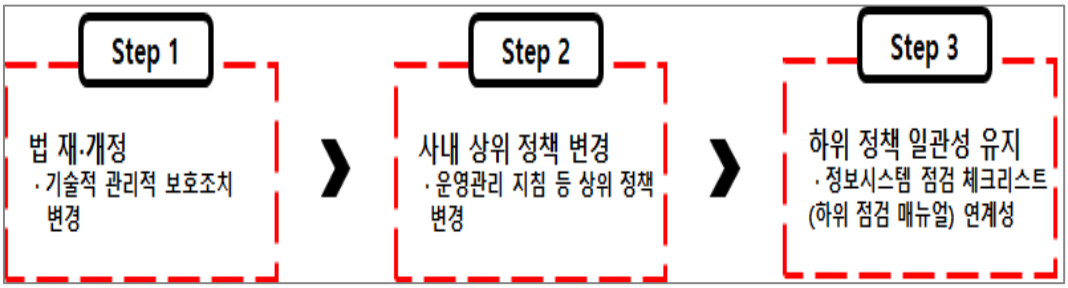
③ 내·외부의 중대한 보안사고 발생

④ 새로운 위협 또는 취약성 발견 등



※ 출처: 개인정보 기술적·관리적 보호조치기준(법제처)





※ 정책 타당성 검토(이해를 돕기 위한 예시)

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

→ 부서 이해관계자 회의 및 의견 취합

① 정보보호 최고책임자 및 개인정보 보호책임자, 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

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

→ 사내 규정 최신성 유지를 통한 변경 사항 적용

① 문서 내에 문서버전, 일자, 개정 사유, 작성자, 승인자 등 개정이력을 기록 관리

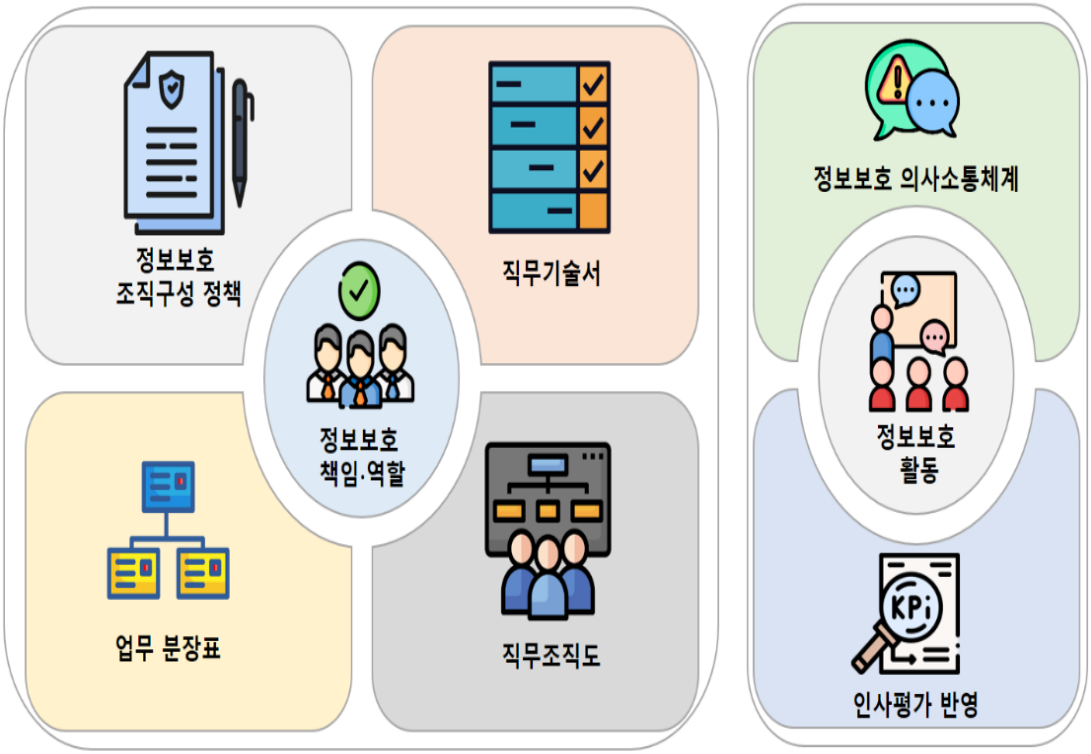
제·개정 이력

개정	제·개정 페이지 및 내용	제·개정 일자	시행 일자
1.0	정보시스템 운영관리지침	2022-01-31	2022-01-31
2.0	정보시스템 운영관리지침 개정	2023-01-31	2023-01-31

담당부서: 정보보호팀 (관리체계운영), 02-000-0000

※ 사내 정책 및 지침 재·개정 기록(이해를 돕기위한 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 의사소통할 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 의사소통할 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 책임자 및 담당자 책임 및 역할** **「정보보호 관리체계 운영지침」** 제 ○○조 (정보보호 조직) ① 정보보호 업무를 효율적으로 수행하기 위해 전담 조직을 구성한다 ≫ 정보보호 최고 책임자: 정보보호 업무 지휘 감독

≫ 정보보호 관리자: 정보보호조직 운영 및 업무 지휘 감독

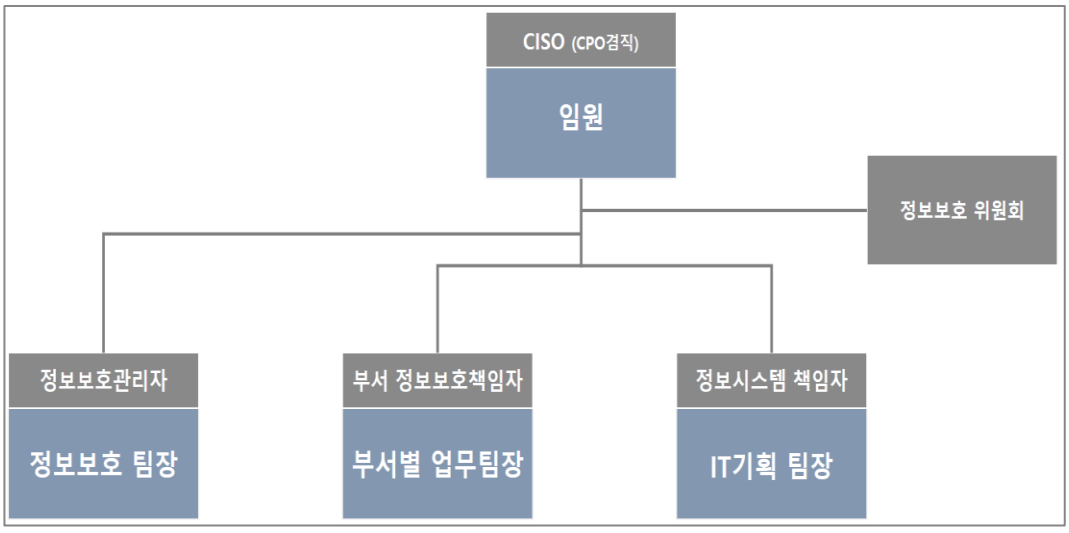
≫ 부서정보보호책임자: 소관업무별 정보보호대책 강구 및 시행

「**정보보호 관리체계 운영지침**」 제 ○○조 (개인정보보호 조직)

① 정보보호최고책임자가 개인정보보호책임자를 겸임한다.

≫ 개인정보보호 책임자는 다음 각 호의 업무를 수행한다.

- 개인정보 보호 계획의 수립 및 시행
- 개인정보 처리 실태에 대한 정기적인 조사 및 개선
- 개인정보 처리와 관련한 불만의 처리 및 피해 구제
- 개인정보 유출 및 오·남용 방지를 위한 내부통제시스템의 구축
- 개인정보 보호 교육 계획의 수립 및 시행
- 개인정보파일의 보호 및 관리 감독
- 개인정보보호법에 따른 개인정보 처리방침의 수립 및 시행
- 개인정보 보호 관련 자료의 관리
- 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기
- 그 밖에 개인정보보호를 위해 필요한 사항



※ 출처: 정보보호조직 구성도(이해를 돕기 위한 예시)

정보보호 조직 업무분장

구분	주요 업무 및 역할
정보보호최고책임자	• 정보보호 정책 및 기본계획 수립·시행 • 정보보호 관련 규정·지침 등 제·개정 • 정보보호심사위원회에 정보보호 분야 안건 심의 주관 • 정보보호 업무 지도·감독, 정보보호 감사 및 심사분석 • 정보통신실, 정보통신망 및 정보자료 등의 보안관리 • 정보보호 수준진단 • 사이버공격 초동조치 및 대응 • 사이버위협정보 수집·분석 및 보안관제 • 정보보호 예산 및 전문인력 확보 • 정보보호 사고조사 결과 처리 • 정보보호 교육 및 정보협력 • 주요정보통신기반시설 보호활동 • 정보통신망 보안대책의 수립·시행 • 그 밖에 정보보호 관련 사항
정보보호관리자	• 정보보호최고책임자의 업무를 보좌 • 정보시스템책임자 및 부서정보보호책임자들의 업무를 관리감독 • 정보보호 관리규정, 시행규칙 제·개정 총괄 • 정보보호 내·외부 감사 및 보안점검 총괄 • 그 밖에 정보보호업무 전반에 관한 지도, 조정 및 그 밖의 감독에 관한 사항
정보시스템책임자	• 정보보호규정 및 관련 규칙에 따른 관리적 및 기술적 보안의 실무활동 수행
부서정보보호책임자	• 부서 내 정보보호 활동 총괄 수행

정보보호 조직 업무분장

구분	주요 업무 및 역할
개인정보보호책임자	• 개인정보 보호 계획의 수립 및 시행 • 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 • 개인정보 처리와 관련한 불만의 처리 및 피해 구제 • 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축 • 개인정보 보호 교육 계획의 수립 및 시행 • 개인정보파일의 보호 및 관리 감독 • 개인정보보호법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행 • 개인정보 보호 관련 자료의 관리 • 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 • 개인정보파일의 보유기간 산정
개인정보보호담당자	• 개인정보 처리 실태의 정기적인 조사 및 개선 • 개인정보 처리와 관련한 불만의 처리 및 피해 구제 • 개인정보파일의 보호 및 관리·감독 • 개인정보 처리방침의 수립·변경 및 시행 • 개인정보 보호 관련 자료의 관리 • 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 • 그 밖에 해당부서의 개인정보 보호를 위해 필요한 사항 등
정보보호위원회	• 정보보호규정 및 관련 규칙, 정보보호계획, 내부감사 등 정보보호 관련 활동의 검토 및 승인 • 위험분석 및 평가로 도출된 위험 대상, 방법 및 통제의 검토 및 승인 • 보안 사고에 대한 검토 • 정보보호를 향상시키기 위한 주요 통제의 승인 • 정보보호담당부서에서 상정한 안건의 검토 및 승인

※ 정보보호조직 업무분장(이해를 돕기 위한 예시)

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

→ 정보보호 및 개인정보보호 관련 담당자와 책임자 활동을 평가

「**정보보호 관리체계 운영지침**」 제 ○○조 (정보보호 직무 수행)

① 정보보호 및 개인정보보호 업무를 수행하는 구성원의 경우 인사평가 지표 중 정보보호 직무수행에 대한 핵심성과지표 10% 이상을 적용한다.

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

→ 조직 구성원간의 의사소통 체계 마련

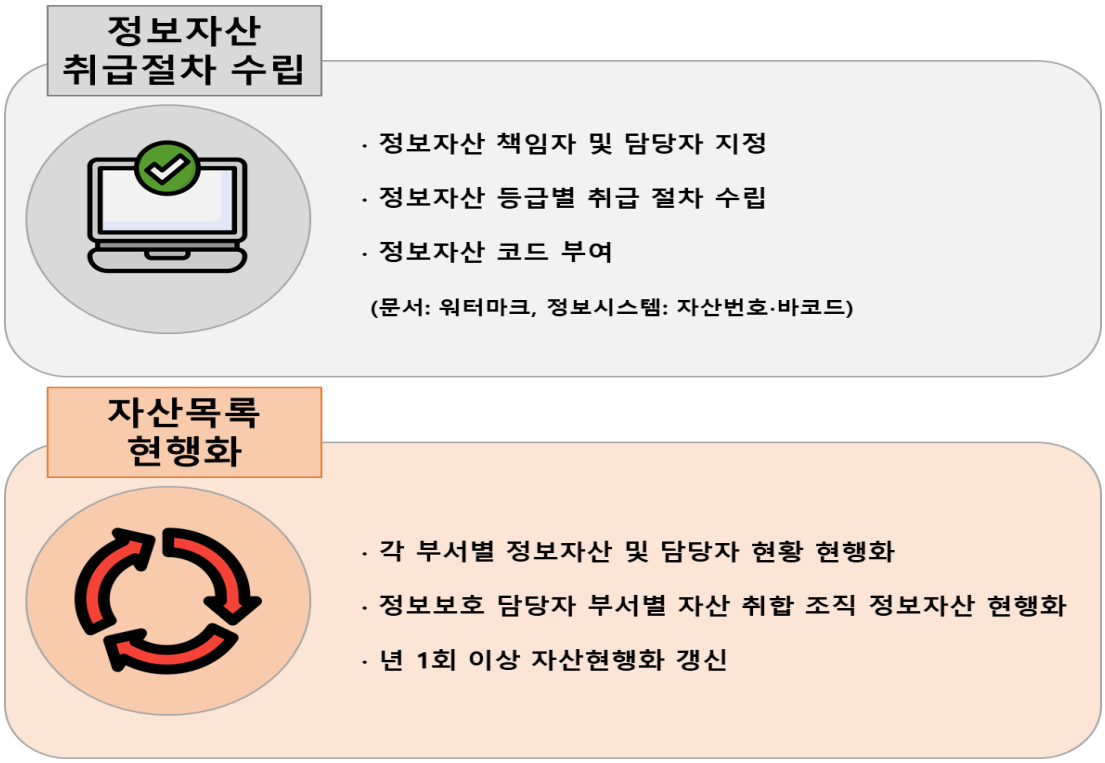
① 의사소통 관리 계획 개요: 목적 및 범위

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

세부분야	2.1.3 정보자산 관리
인증 기준	정보자산의 용도와 중요도에 따른 취급 절차 및 보호대책을 수립·이행하고, 자산별 책임소재를 명확히 정의하여 관리하여야 한다.
주요 확인사항	• 정보자산의 보안등급에 따른 취급절차(생성·도입, 저장, 이용, 파기) 및 보호대책을 정의하고 이행하고 있는가? • 식별된 정보자산에 대하여 책임자 및 관리자를 지정하고 있는가?
기준 요약도	
운영 방안	**◇ 정보자산의 보안등급에 따른 취급절차(생성·도입, 저장, 이용, 파기) 및 보호대책을 정의하고 이행하고 있는가?** **→ 보안등급에 따라 취급절차(예시)** **「정보보호 관리체계 운영지침」** 제 ○○조 (정보자산 처리) ① 1등급·2등급 정보자산의 경우 부서 보안책임자의 승인없이 외부로 유출 또는 공개해선 안 된다. ② 1등급·2등급 정보자산은 공개 결정시 보안성 검토를 거쳐야 한다 **→ 자산등록 절차(예시)**

「**정보보호 관리체계 운영지침**」 제 ○○조 (정보자산 등록)

① 신규 자산 등록은 정보 소유자가 필요 시 부서 정보보호책임자에 허가를 득하고 부서 자산목록에 직접등록한다.

② 부서 정보보호책임자는 등록자산에 보안등급에 따라 자산코드를 부여하여야 한다.

③ 정보보호담당자는 매월 각 부서의 자산목록을 검토 현행화 한다.

④ 정보보호담당자는 년 1회 자산 실사하여야 하며, 그 결과를 정보보호위원회에 보고해야 한다.

◇ 식별된 정보자산에 대하여 책임자 및 관리자를 지정하고 있는가?

→ 책임자 및 관리자 지정 절차(예시)

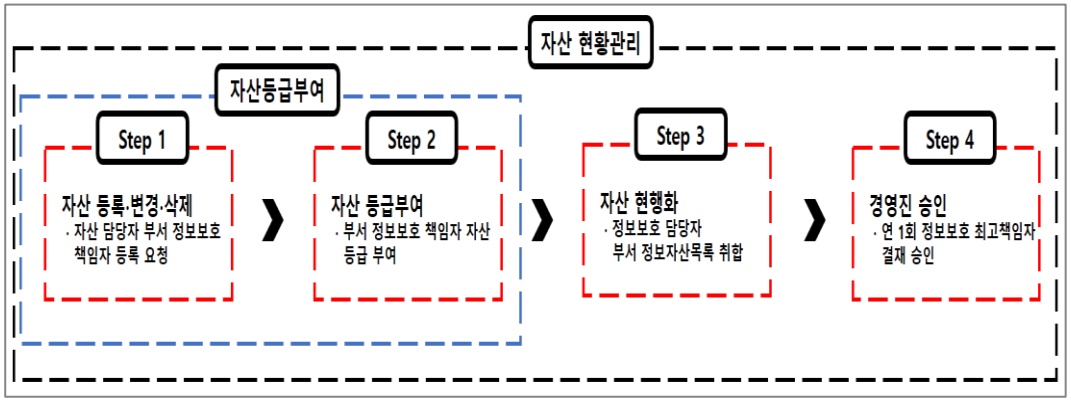
「**정보보호 관리체계 운영지침**」 제 ○○조 (정보자산 등록)

① 자산 등록·변경·삭제 은 정보 소유자가 필요 시 부서 정보보호책임자에 허가를 득하고 부서 자산목록에 직접등록한다.

② 부서 정보보호책임자는 등록자산에 보안등급에 따라 자산코드를 부여하여야 한다.

③ 정보보호담당자는 분기별 각 부서의 자산목록을 검토 취합 현행화 한다.

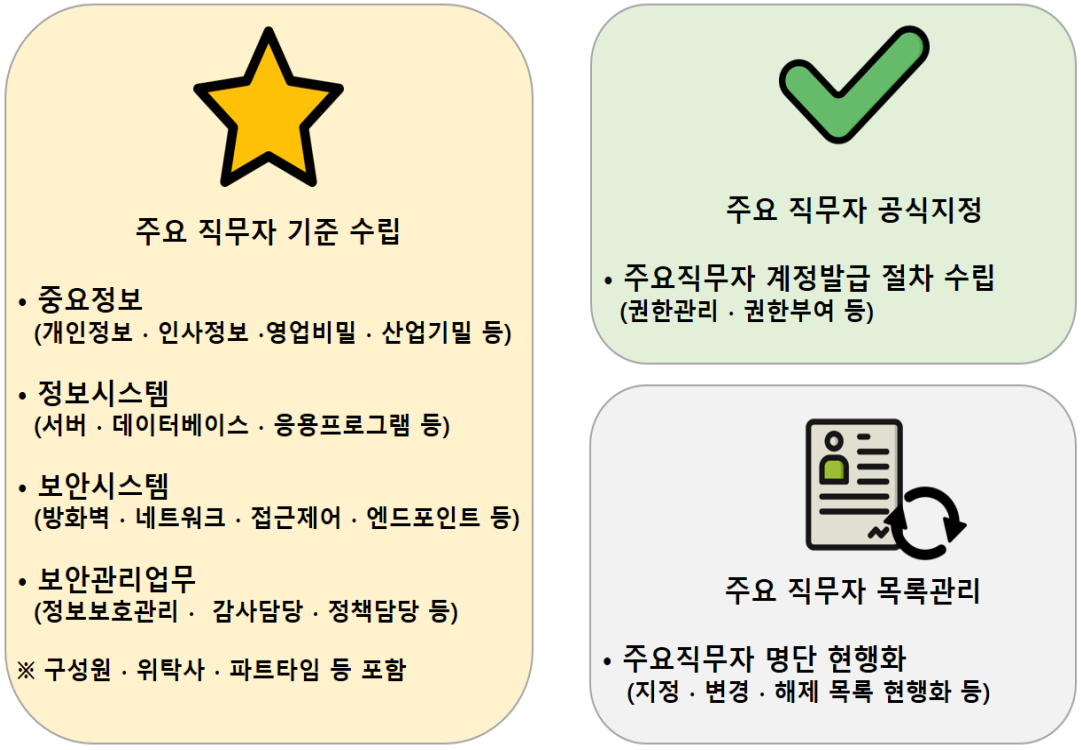
④ 정보보호담당자는 년 1회 자산 실사하여야 하며, 그 결과를 정보보호최고책임자에 보고해야 한다.



※ 식별자산 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?

→ 주요 직무자 지정 문서화(예시)

「인적보안 관리지침」 제 ○○조 (주요 직무자 지정)</td></tr>
</table>

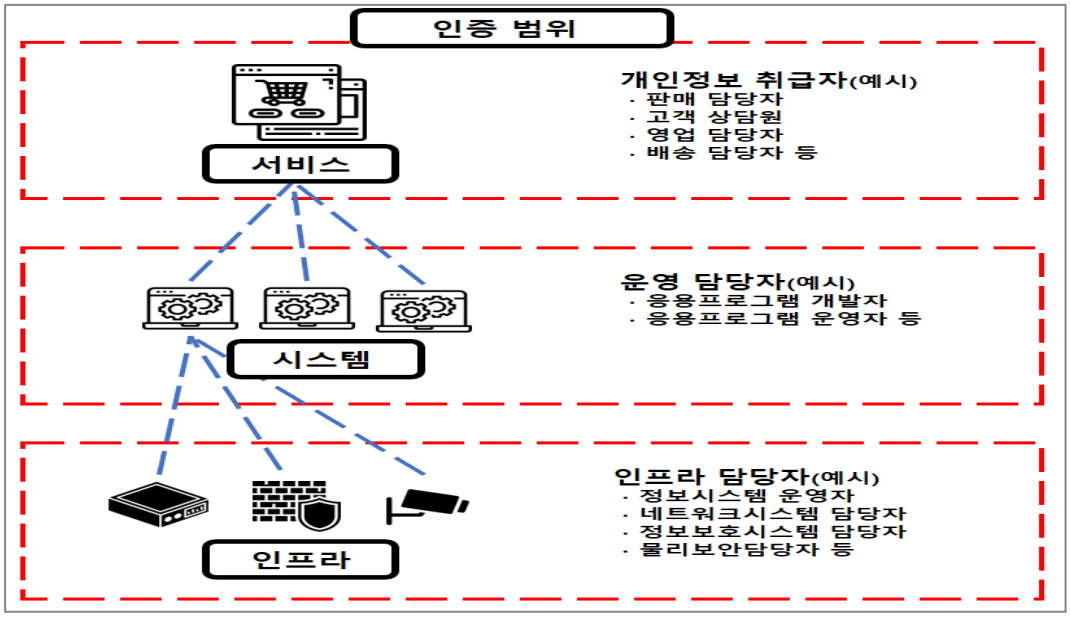
① 부서별 보안담당자는 다음 각 호의 업무를 수행에 필요한 최소한으로 제한하며 주요 직무자로 지정하여야 한다.

≫ 중요정보(개인정보, 인사정보, 영업비밀, 산업기밀, 재무정보 등) 취급

≫ 중요 정보시스템(서버, 데이터베이스, 응용 프로그램 등) 및 개인정보처리시스템 운영·관리자

≫ 정보보안 시스템 운영 관리자

≫ 정보보안관리 업무를 수행하는자



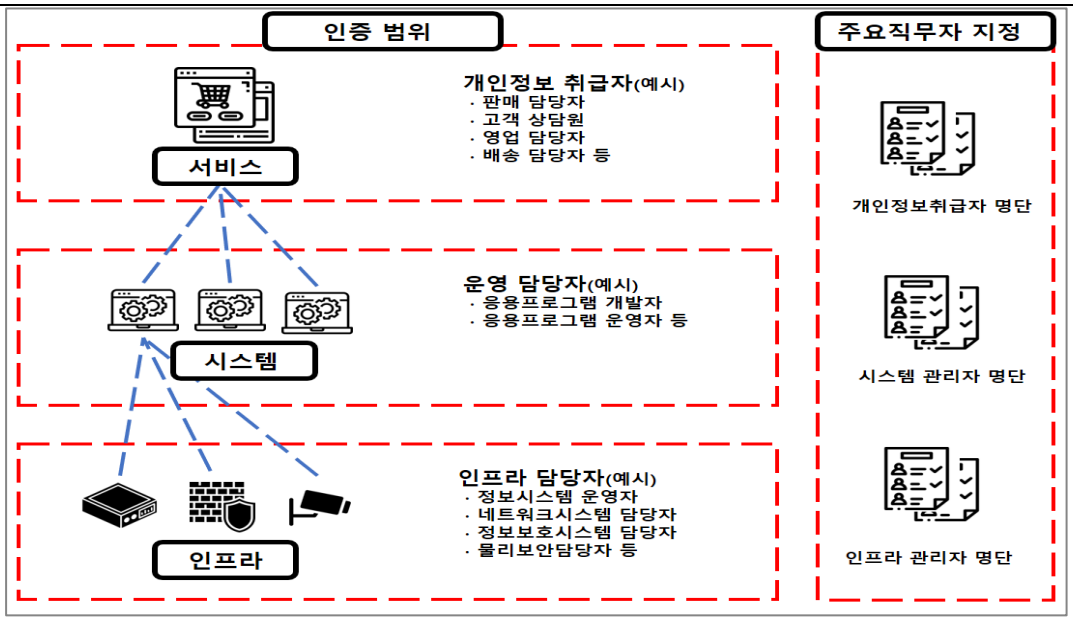
※ 주요취급자 지정범위 산정 (이해를 돕기 위한 예시))

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

→ 주요정보 취급자 현황관리

「**인적보안 관리지침**」 제 ○○조 (주요 직무자 지정)

① 부서별 보안담당자는 부서별 주요직무자 및 개인정보취급자의 명단을 관리해야 하며 반기 1회 이상 주요 직무자 및 개인정보취급자의 명단을 검토 관리 현행화 해야한다.



정보시스템 사용자계정(ID) 관리대장

검토 일자:

순번	시스템명	ID	IP 주소	위치	권한	사용자	사용기간
1							
2							

※ 주요취급자 현황관리 (이해를 돕기 위한 예시)

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

→ 개인정보 취급자 목록 최신화

① 임직원, 파견근로자, 시간제근로자 등 개인정보취급자의 지휘·감독을 받아 개인정보를 처리하는 자

"000 개인정보처리시스템" 접근권한 관리대장

검토 일자:

순번	사용자	ID	권한 상세 내역			담당자 (서명)	개인정보 보호책임자 (서명)
			종류	부여일시	말소일시		
1							
2							

※ 개인정보취급자 현황대장(이해를 돕기 위한 예시)

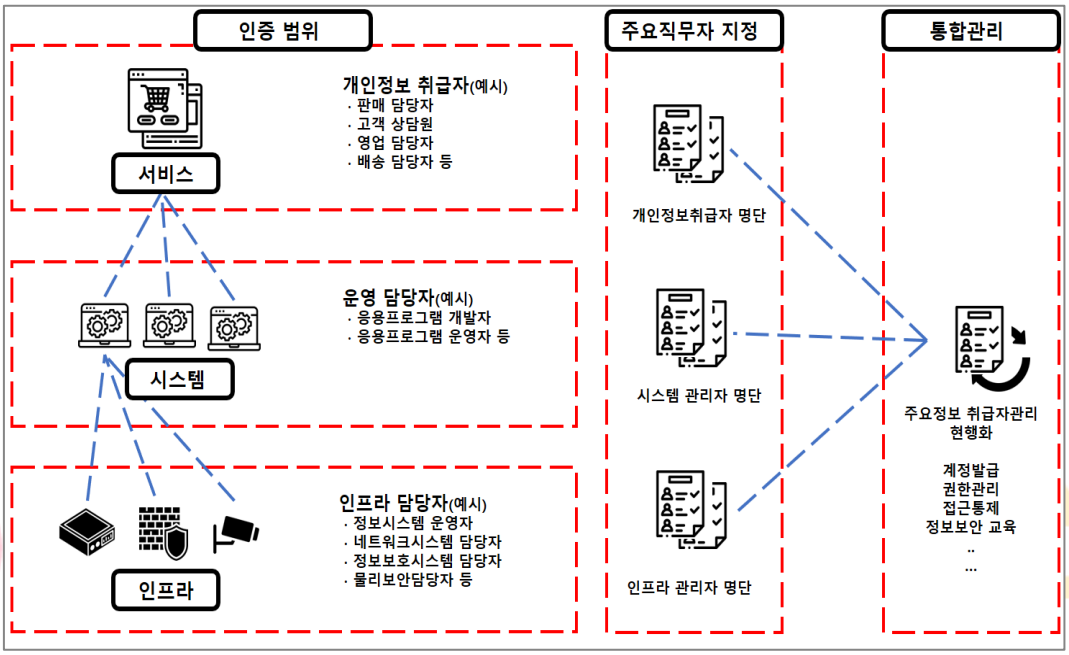
◇ 업무 필요성에 따라 주요 직무자 및 개인정보취급자 지정을 최소화하는 등 관리방안을 수립·이행하고 있는가?

→ 업무상 필요한 주요 직무자 및 개인정보 취급자 관리방안 수립

① 업무상 반드시 필요한 경우에 한하여 주요 직무자 및 개인정보취급자로 지정

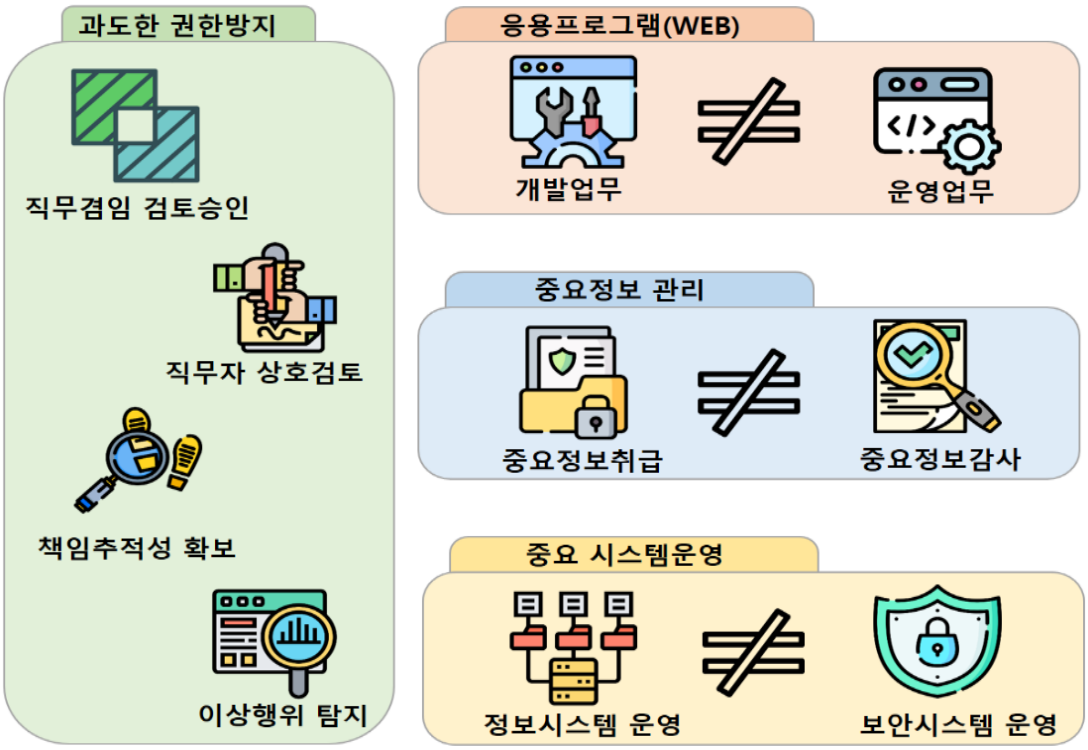
② 주요 직무자 및 개인정보취급자 권한 신청 및 부여에 대한 승인 절차 마련

③ 주요 직무자 및 개인정보취급자에 대한 관리 및 통제방안 수립·이행



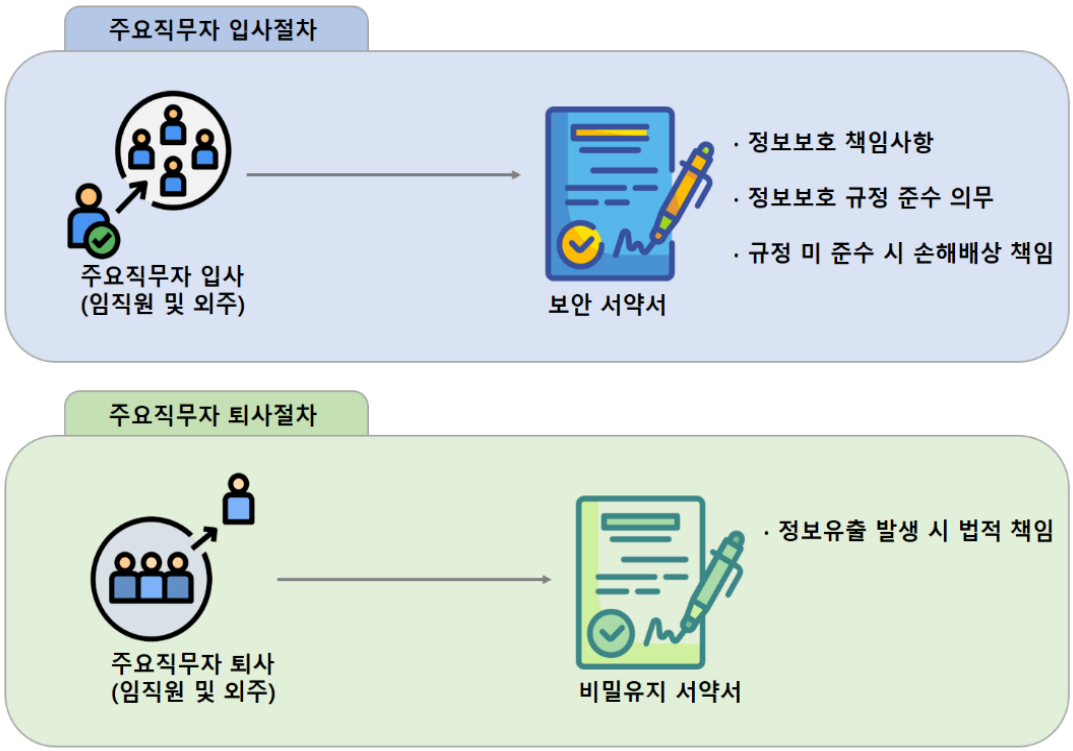
※ 주요 직무자 및 취급자 관리방안 수립(이해를 돕기 위한 예시)

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 변경사항 승인, 책임추적성 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?** **→ 전자금융감독 규정 (예시)** 「**전자금융감독규정**」 제26조 (직무분리) ① 다음 각 호의 업무에 대하여 직무를 분리·운영하여야 한다. ≫ 프로그래머와 오퍼레이터 ≫ 응용프로그래머와 시스템프로그래머 ≫ 시스템보안관리자와 시스템프로그래머 ≫ 전산자료관리자(librarian)와 그 밖의 업무 담당자

	≫ 업무운영자와 내부감사자 ≫ 내부인력과 전자금융보조업자 및 유지보수업자 등을 포함한 외부인력 ≫ 정보기술부문인력과 정보보호인력 ≫ 그 밖에 내부통제와 관련하여 직무의 분리가 요구되는 경우 **◇ 직무 분리가 어려운 경우 직무자 간 상호 검토, 상위관리자 정기 모니터링 및 변경사항 승인, 책임추적성 확보 방안 등의 보완통제를 마련하고 있는가?** **→ 직무분리가 어려운 경우 직무자 보완통제 절차 마련 (예시)** ① 상호 검토 절차 마련 (방안 예시) ≫ "상호검토 작업관리대장" 관리작성 ≫ 공통계정 작업 시 작업자 외 공통계정 사용자 상호 검토서명 ≫ 시스템 "접속 및 작업 기록" 과 "상호검토 작업관리대장" 주 1회 이상 상호검토 ≫ 특이사항 발생 시 상위관리자 즉시 보고 ≫ 별다른 특이사항 없을 시 월별 운영관리 현황 보고에 첨부 작성

2.2.3 보안 서약

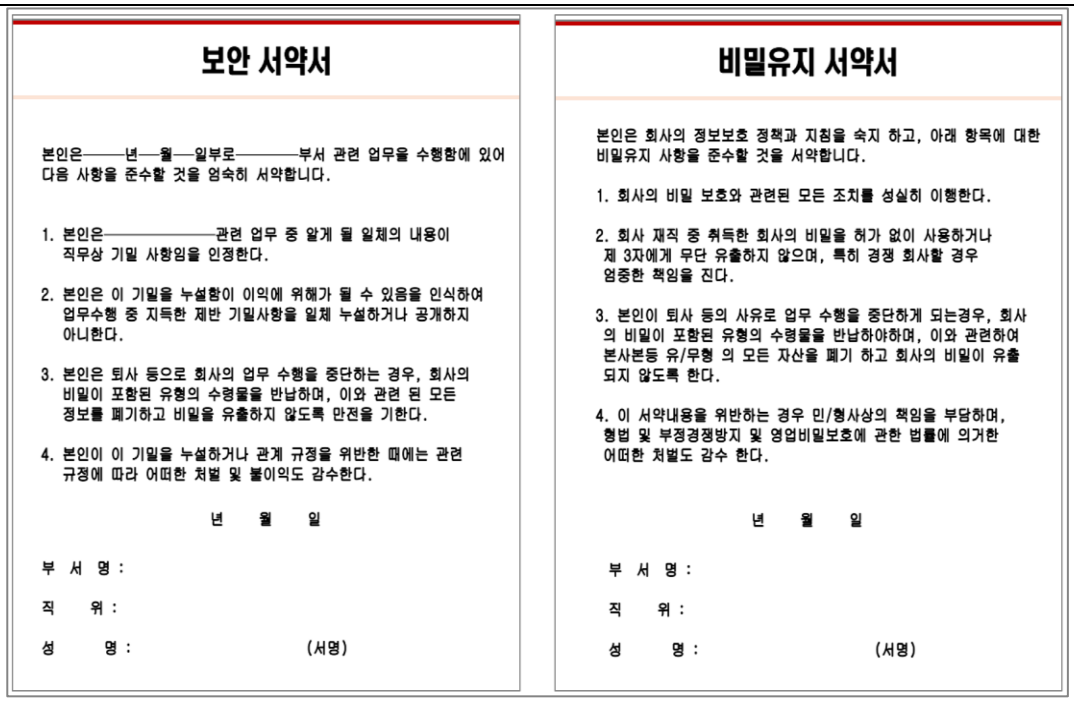
세부분야	2.2.3 보안 서약
인증 기준	정보자산을 취급하거나 접근권한이 부여된 임직원·임시직원·외부자 등이 내부 정책 및 관련 법규, 비밀유지 의무 등 준수사항을 명확히 인지할 수 있도록 업무 특성에 따른 정보보호 서약을 받아야 한다.
주요 확인사항	• 신규 인력 채용 시 정보보호 및 개인정보보호 책임이 명시된 정보보호 및 개인정보보호 서약서를 받고 있는가? • 임시직원, 외주용역직원 등 외부자에게 정보자산에 대한 접근권한을 부여할 경우 정보보호 및 개인정보보호에 대한 책임, 비밀유지 의무 등이 명시된 서약서를 받고 있는가? • 임직원 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 퇴직시 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 내용 포함 서약서 작성



보안 서약서

본인은 ____년 ____월 ____일부로 ____부서 관련 업무을 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 퇴사 등으로 회사의 업무 수행을 중단하는 경우, 회사의 비밀이 포함된 유형의 수령물을 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 퇴사 등의 사유로 업무 수행을 중단하게 되는경우, 회사의 비밀이 포함된 유형의 수령물을 반납하여야하며, 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 :

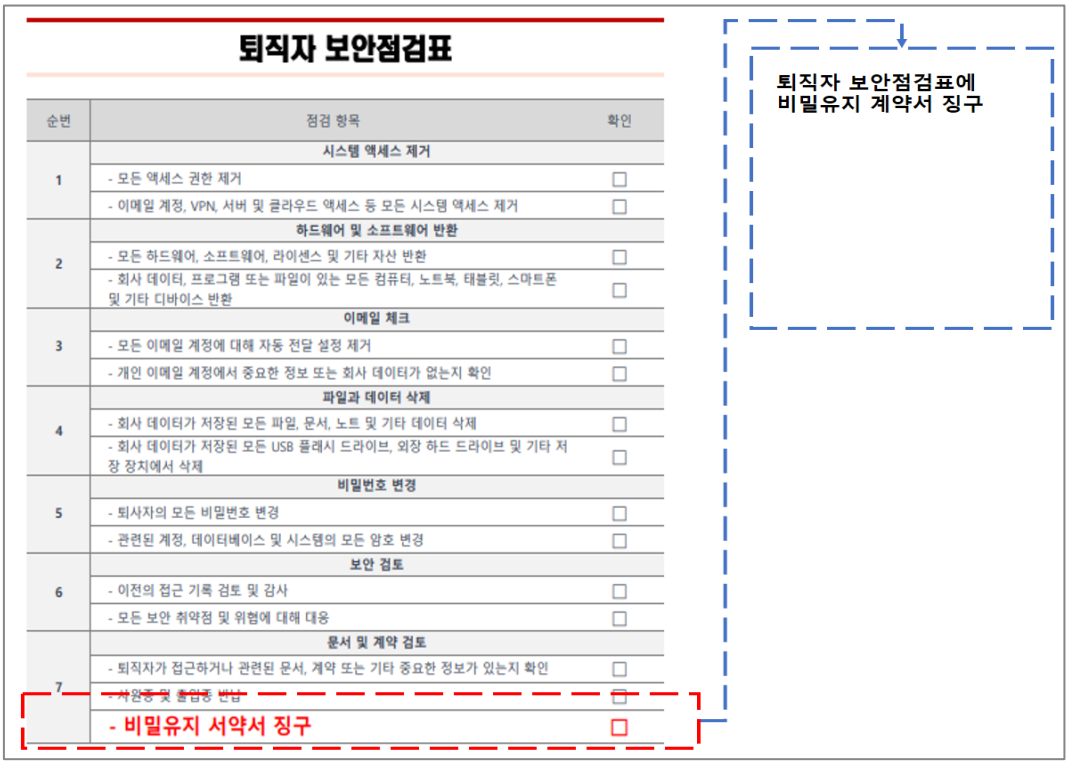
성 명 : (서명)

※ 보안서약서 작성(이해를 돕기 위한 예시)

◇ 임직원 퇴직 시 별도의 비밀유지에 관련한 서약서를 받고 있는가?

→ 퇴직 시 보안 체크리스트 작성 적용

① 퇴직자에게 정보유출 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	☐
	- 서명 및 출입증 반납	☐
	- 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? • 교육시행에 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

「**인적보안 지침**」 제 ○○조 (교육 및 훈련)

① 정보보호 관리자는 매년 각 호를 포함한 정보보안 교육 및 훈련 계획을 수립하고 정보보호 관리책임자(CISO)에 승인을 받아야한다.

≫ 교육 유형: 임직원 인식제고 교육, 주요직무자, 개인정보취급자 교육, 수탁자 교육, 전문 교육

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

≫ 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	-

※ 정보보호교육계획 (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?

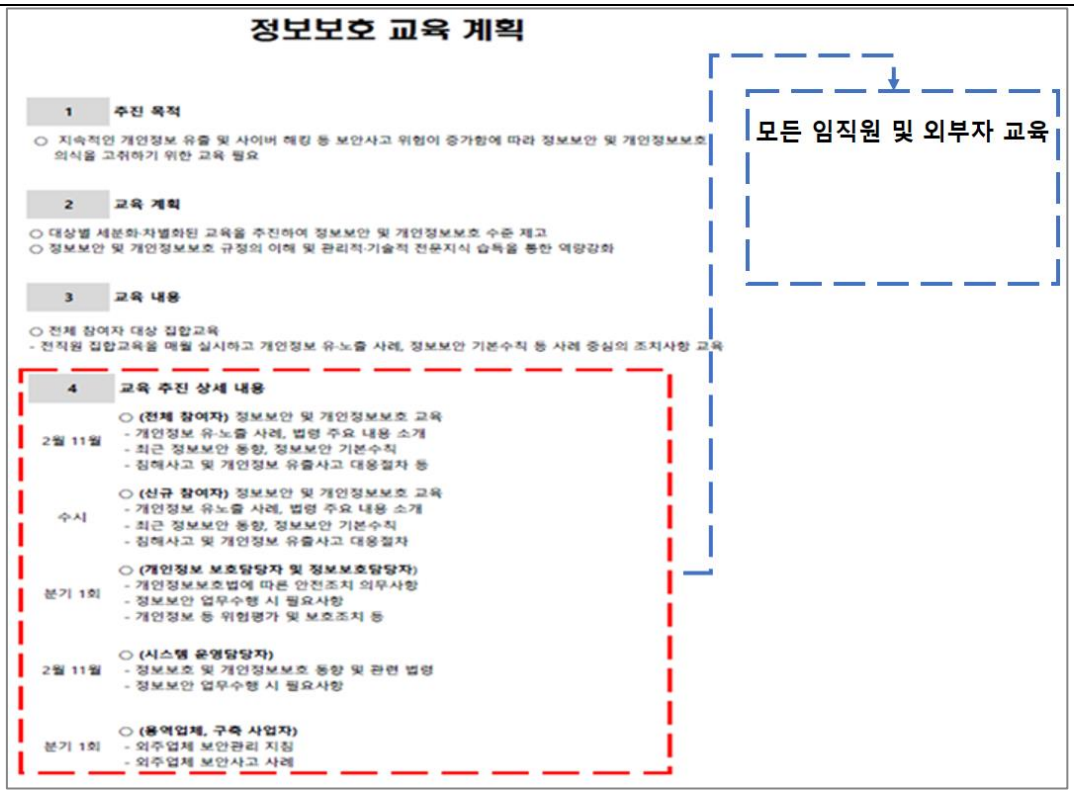
→ 내 모든 임직원과 외부자를 대상으로 연간 교육 계획

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

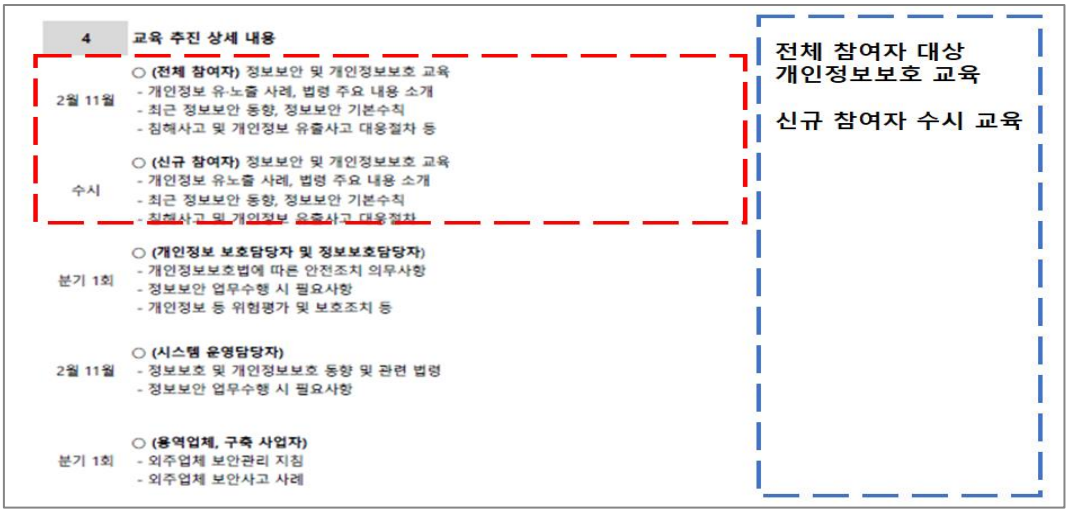


※ 정보보호 교육 계획(이해를 돕기 위한 예시)

◇ 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



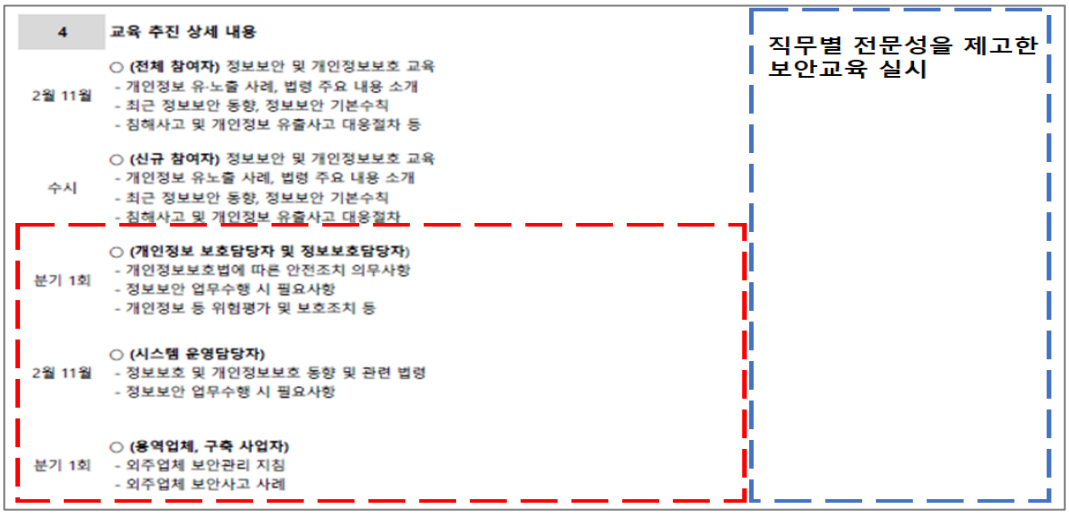
※ 정보보호 교육 상세 일정 (이해를 돕기 위한 예시)

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

→ 직무별 전문교육 실시

① 관련 직무자: IT 직무자, 정보보호 최고책임자, 개인정보 보호책임자, 개인정보취급자, 정보보호 직무자 등

② 교육과정: 정보보호 및 개인정보보호 관련 콘퍼런스·세미나·워크숍 참가, 교육 전문기관 위탁 교육, 외부 전문가 초빙을 통한 내부교육 등



※ 정보보호 교육 전문적 교육 실시 (이해를 돕기 위한 예시)

◇ 교육시행에 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

1 교육 목적

○ 정보유출, 대량 개인 정보유출과 같은 공공기관, 연구기관, 기업 등 특정 표적을 대상으로 사이버 공격이 빈번히 발생하고 있음

2 교육 내용

○ 일 시 : '00. 00. 00 13:00 ~ 18:00
○ 장 소 : OOO 본사 대회의실

3 교육 결과 요약

○ 참석 00명

부서	참석인원	부서
OO 부서	24 명	OO 부서
OO 부서	3 명	OO 부서
OO 부서	8 명	OO 부서

4 교육사진

교육 사진 1	교육 사진 2	교육 사진 3
사진 1	사진 2	사진 3

보안교육 참석자 명단

- OOO 교육 - 2023. 0. 0(요일) 15:00 ~ 16:00

부 서	직 책	성명	서 명	비고

정보보호 교육 만족도 조사(예시)

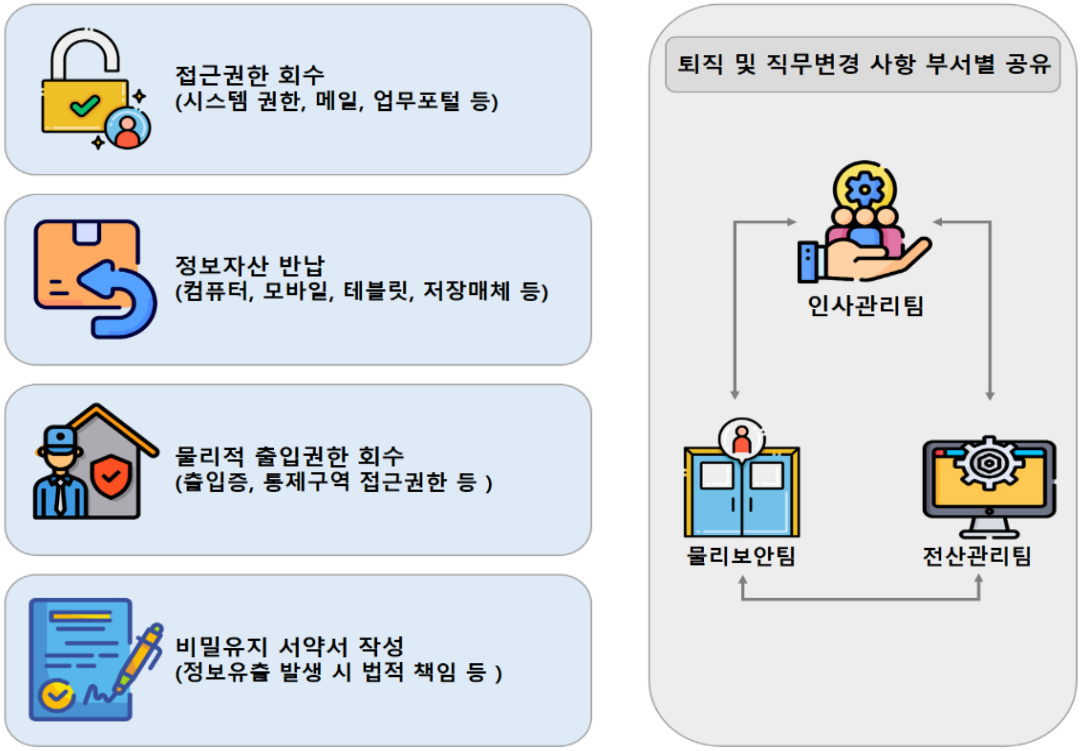
항목	만족도				
	매우만족	만족	보통	불만	매우불만
교육 프로그램의 구성	□	□	□	□	□
강사의 전달력	□	□	□	□	□
교육 자료의 질	□	□	□	□	□
교육 시간의 적절성	□	□	□	□	□
실습 시스템의 안정성	□	□	□	□	□
교육장의 시설 및 환경	□	□	□	□	□
교육 후의 질문 답변 및 피드백	□	□	□	□	□
전반적인 교육 만족도	□	□	□	□	□
...	...	...	...	...	...

00년 정보보호 교육결과보고

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

※ 정보보호교육결과보고 (이해를 돕기 위한 예시)

2.2.5 퇴직 및 직무변경 관리

<table>
<tr><th>세부분야</th><th>2.2.5 퇴직 및 직무변경 관리</th></tr>
<tr><td>인증
기준</td><td>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.</td></tr>
<tr><td>주요
확인사항</td><td>• 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?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 퇴직, 직무변경, 부서이동, 휴직 등으로 인한 인사변경 내용이 인사부서, 정보보호 및 개인정보보호 부서, 정보시스템 및 개인정보처리시스템 운영부서 간 공유되고 있는가?

→ 퇴직절자 부서 공유 절차 필요
① 인사 변경 내용에 대한 신속한 공유 절차 (예시)
≫ 정보처리시스템을 인사시스템과 연동하여 실시간 또는 일배치로 계정정보 동기화
≫ 협력업체 인원에 대한 통합 계정 등록·관리시스템을 구축하여 개별 시스템과 계정 동기화</td></tr>
</table>

≫ 퇴직 프로세스 내에 관련 부서에 퇴직자 정보를 관련 부서에 공유하는 절차 포함

◇ 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?

→ 퇴직자 확인 절차 마련

「**인적보안 관리지침**」 제 ○○조 (퇴직 및 계약해지 시)

① 퇴직자는 재직 중 보유 한 모든 정보자산 반환할 의무가 있으며, 보안담당자는 "퇴직자 보안점검표"를 이용해 처리결과를 확인해야 한다.

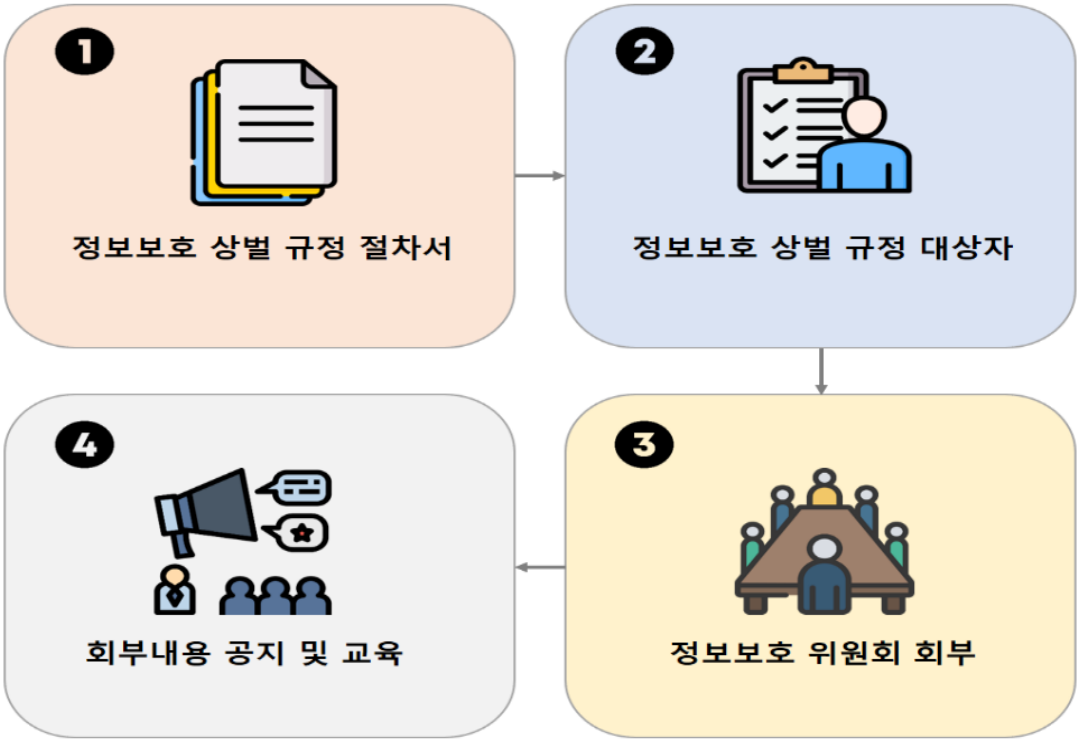
퇴직자 보안점검표

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	☐
	- 사원증 및 출입증 반납	☐
	- 비밀유지 서약서 징구	☐

퇴직자 보안점검표를 통해 퇴직 절차에 누락이 없는지 확인

※ 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 개인정보 보호 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?** **→ 처벌 규정 수립** 「**인적보안 관리지침**」 제 ○○조 (처벌 기준) ① 경미 위반사고 ≫ 1회 위반: 정보보호최고책임자에 의한 1차 구두 경고 ≫ 2회 위반: 정보보호최고책임자에 의한 2차 구두 경고

≫ 3회 위반: 정보보호위원회에 안건 상정하여 위반 시 시말서 징구

≫ 4회 위반: 정보보호위원회에 회부 및 징계수위 결정·위반사실 전사공지

② 중대 위반사고

≫ 1회 위반: 정보보호위원회에 회부 및 징계수위 결정·위반사실 전사공지

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

→ 상벌 규정 기록 및 전파

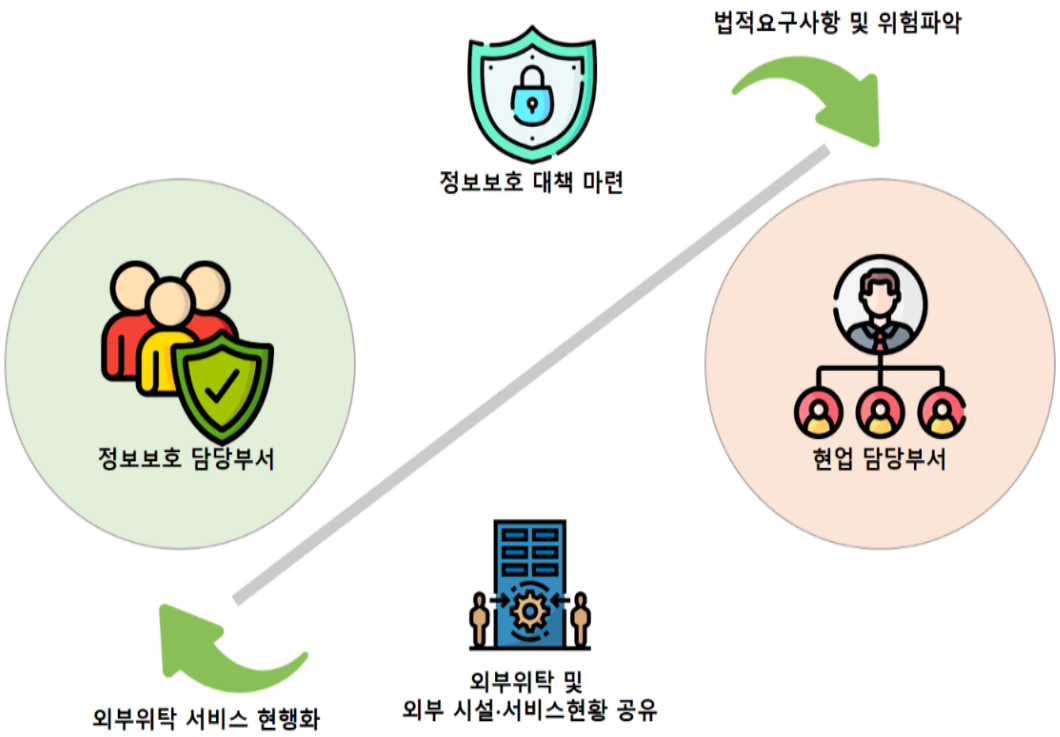
① 상벌 규정에 따른 조치를 수행하고 결과 기록

② 필요한 경우 전사 공지 또는 교육 사례로 활용 등

※ 규정위반 심의 결과 공지(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 보호대책을 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 보호대책을 마련하고 있는가?
기준 요약도	
운영 방안	**◇ 관리체계 범위 내에서 발생하고 있는 업무 위탁 및 외부 시설·서비스의 이용 현황을 식별하고 있는가?** **→ 업무위탁 유형(예시)** ① 운영 용역 ≫ 업무망 내 시스템 네트워크 및 보안 장비 운영 IT ≫ 기업 내부망에 대한 취약점점검 및 모의해킹 ② 유지보수 용역

≫ 업무망에 온라인 접속권한으로 수행된 업무에 대한 유지보수

≫ 기업 내 온라인으로 진행되는 시스템 네트워크 및 IT보안장비 유지보수

≫ IT 외주업체 내에서 운영되는 시스템 네트워크 및 보안장비 유지보수

≫ 원격시스템 네트워크 및 보안장비 유지보수

≫ 원격 유지보수 및 장애 관리

③ SI 용역

≫ IT 업무지원 시스템 개발 구축

④ 데이터처리 용역

≫ 기업 내의 헬프데스크 운영

≫ 기업 내부데이터를 활용한 대리점 운영

⑤ 오프라인 지원

≫ 오프라인으로 출력된 산출물을 관리하는 용역업체

≫ 오프라인으로 출력된 내부데이터를 활용하여 면담으로 진행되는 정보보호컨설팅

≫ 오프라인으로 출력된 내부데이터를 활용하여 진행되는 기업 회계감사 및 보안컨설팅

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	김00	010-1234-5678
쇼핑몰 고객상담	㈜ OOO 콜센터	20명	고객 상담	2022-01-01	2022-12-31	상	고객가치팀	이00	010-9874-5632
...	...	...	...	...	...		...	...	...

※ 업무위탁현황표(이해를 돕기 위한 예시)

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

→ 위탁사업 법적 요구사항 및 위험 파악

① 개인정보 처리업무 위탁에 해당되는지 확인

② 개인정보 등의 국외 이전에 해당되는지 확인

③ 개인정보 보호법, 정보통신망법 등 관련된 법적 요구사항 파악

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

⑤ 위험평가 결과를 반영하여 적절한 보호대책

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 개인정보 보호 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 개인정보 보호 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 이용시 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 인터넷접속 제한, 물리적 보호조치(장비 및 매체 반출입 등), PC 등 단말 보안(백신설치, 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 정의보안 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?

→ 업무 위탁 보안요구사항 계약 시 반영

「**외부자 보안지침**」 제 ○○조 (계약 시 보안 요구사항)

① 정보처리 업무를 외부자에게 위탁하거나 외부 서비스를 이용하는 경우 보안 요구사항을 정의하여 계약 시 반영하여야 한다.

≫ 정보보호 및 개인정보보호 관련 법적 요구사항 준수

≫ 안전한 코딩 표준 준수 등 개발보안 절차 적용

≫ 개발 완료된 정보시스템 및 개인정보처리시스템에 대한 취약점 점검 및 조치

≫ 개발 관련 산출물, 소스 프로그램, 개발용 데이터 등 개발환경에 대한 보안관리

≫ 개발 과정에서 취득한 정보에 대한 비밀유지 의무

≫ 위반 시 손해배상 등 책임에 대한 사항

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 보호대책 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 개선계획을 수립·이행하고 있는가? • 개인정보 처리업무를 위탁받은 수탁자가 관련 업무를 제3자에게 재위탁하는 경우 위탁자의 승인을 받도록 하고 있는가?
기준 요약도	
운영 방안	**◇ 외부자가 계약서, 협정서, 내부정책에 명시된 정보보호 및 개인정보보호 요구사항을 준수하고 있는지 주기적으로 점검 또는 감사를 수행하고 있는가?** **→ 외부자 정보보호 및 개인정보보호 요구사항 준수 주기적 검토** 「**외부자 보안지침**」 제 ○○조 (협력업체 인력 보안) ① 업무담당자는 아웃소싱 인력 투입 시 다음 각 호의 서류를 징구하며, 부서 정보보호관리자에게 제출하여야 한다. ≫ 보안서약서

≫ 개인정보보호 서약서

≫ 출입신청서

≫ 정보자산 반출입 신청서

② 개인정보 보호 책임자는 수탁자를 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	재 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 개선계획을 수립·이행하고 있는가?

→ 발견된 문제점에 대하여 개선계획을 수립·이행

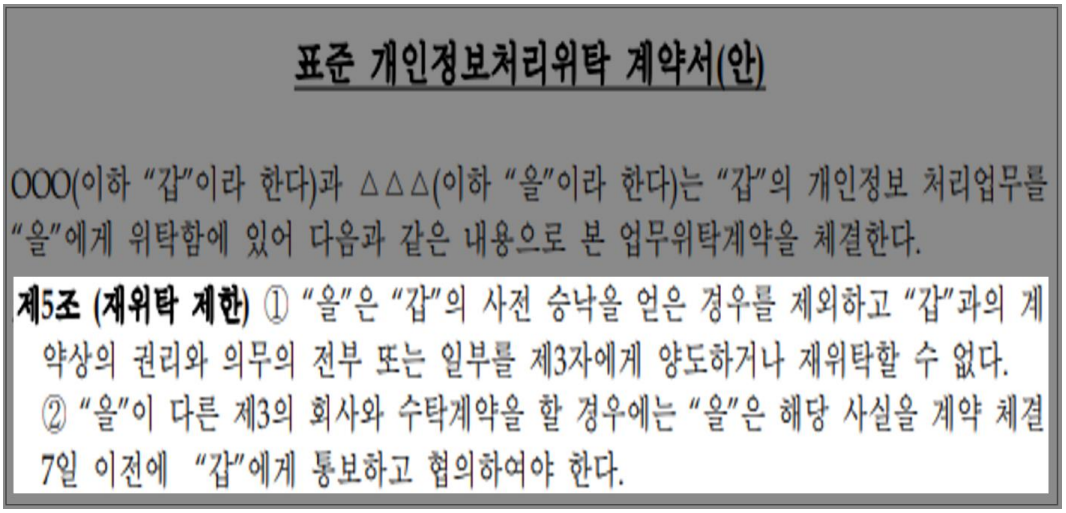
① 점검 및 감사 결과에 대하여 공유하고 발견된 문제점에 대한 개선방법 및 재발방지대책을 수립하여 이행

② 개선 조치 완료 여부에 대한 이행점검 수행

◇ 개인정보 처리업무를 위탁받은 수탁자가 관련 업무를 제3자에게 재·위탁하는 경우 위탁자의 승인을 받도록 하고 있는가?

→ 재수탁 관리감독 사항

① 개인처리방침 재위탁에 대한 위탁자 승인



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

≫ 위탁자는 법 제26조 제4항에 의하여 재수탁자를 교육하고 개인정보 처리 현황을 감독할 의무가 있음

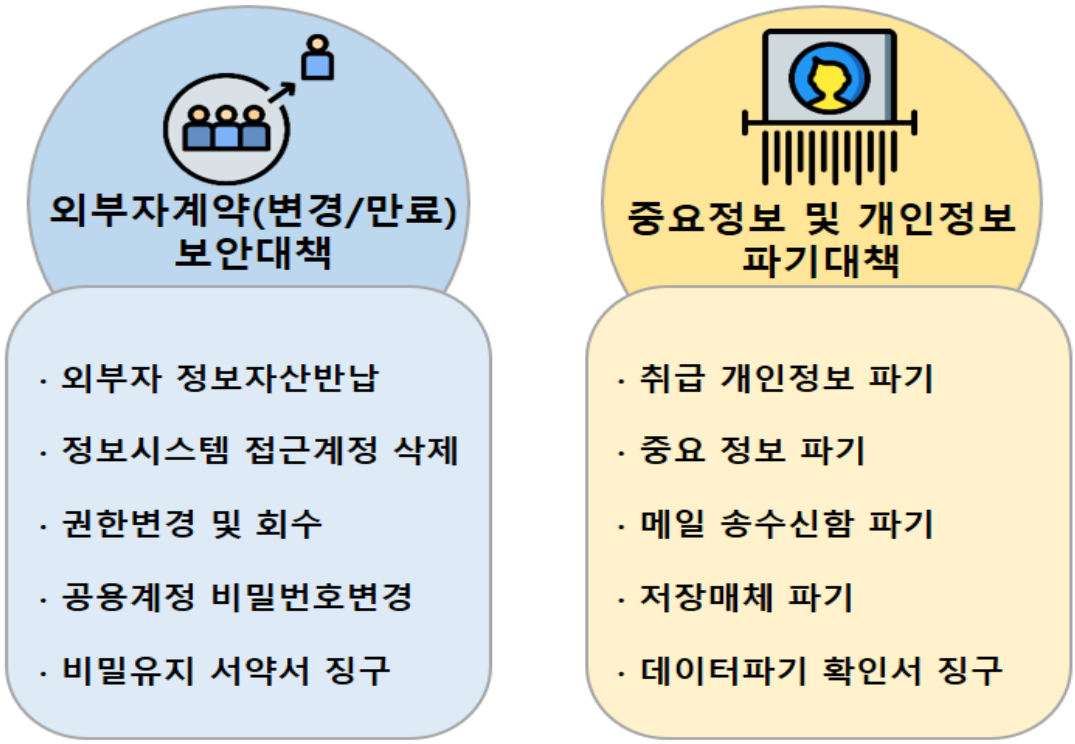
≫ 위탁자는 법 제26조 제2항에 의하여 재위탁하는 업무의 내용과 재수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 공개해야 함

「**개인정보보호법**」 제26조 (업무위탁에 따른 개인정보의 처리 제한)

① 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 "위탁자"라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 "수탁자"라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

② 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

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, 업무종료, 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?

→ 외부자 계약 변경 및 만료 시 보안대책 수립

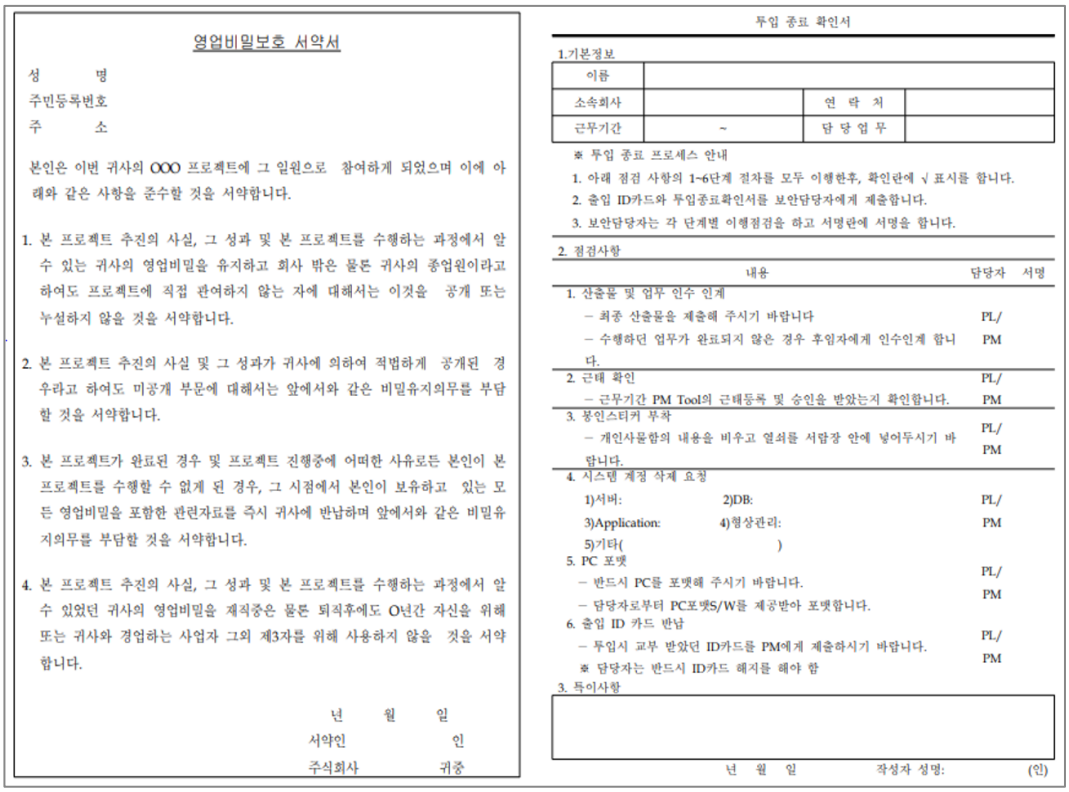
「외부자 보안지침」 제 ○○조 (사업완료시 보안관리)
① 사업완료 후 생산되는 최종 산출물 중 대외보안이 요구되는 자료는 대외비로 작성·관리하고 불필요한 자료는 삭제 및 세단 후 폐기한다.</td></tr>
</table>

≫ 정보보호 관련 법령 및 규정위반

② 아웃소싱업체에 제공한 제반자료, 장비 서류와 중간·최종 산출물 등 제반자료는 전량 회수하고 아웃소싱업체에 복사본 등을 별도 보관을 금지한다.

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

④ 아웃소싱사업 관련자료 회수 및 삭제조치 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 미공개 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 경업하는 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 1~6단계 절차를 모두 이행한후, 확인란에 √ 표시를 합니다.
2. 출입 ID카드와 투입종료확인서를 보안담당자에게 제출합니다.
3. 보안담당자는 각 단계별 이행점검을 하고 서명란에 서명을 합니다.

2. 점검사항

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

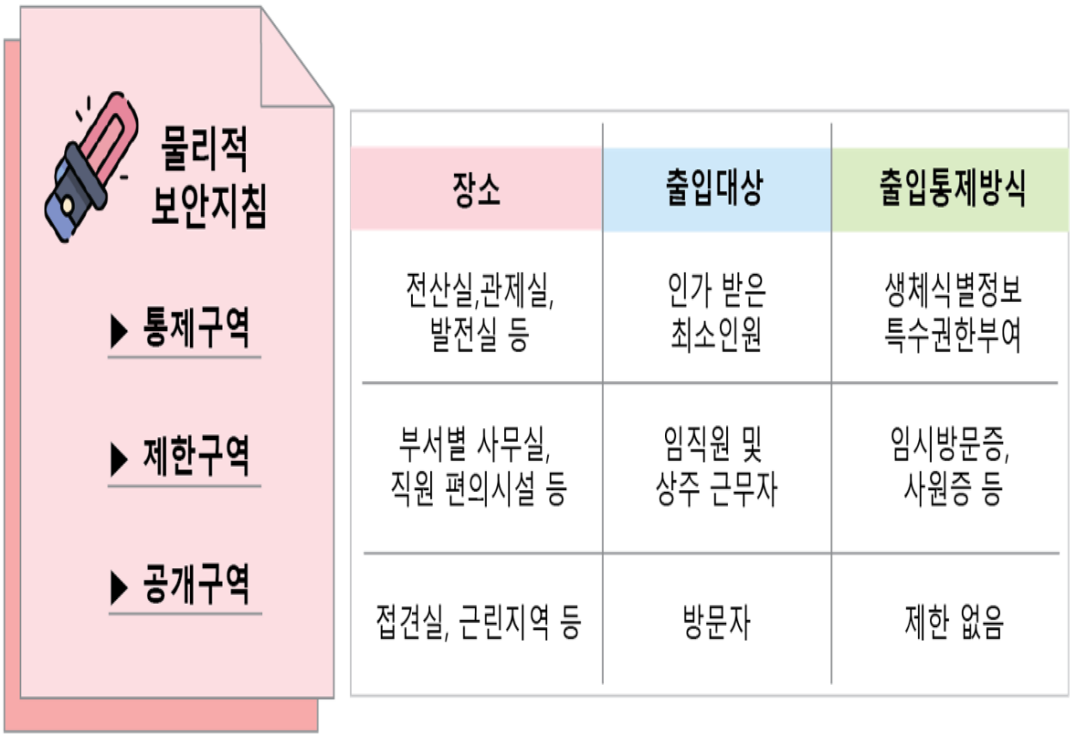
① 개인정보 등 중요정보를 회수·파기하기 위하여 수탁사 직접 방문 또는 원격으로 개인정보를 파기한 후 파기 확약서 작성

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 보호대책을 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 보호대책을 수립·이행하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</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?

→ 물리적보안 관리 지침(예시)

「물리적보안 지침」 제 ○○조 (보호구역의 지정)
① 중요 정보 및 정보처리시설을 보호하기 위한 물리적 보안 구역을 지정하고, 각 보안</td></tr>
</table>

구역에 대한 보안 대책을 마련하여야 하며, 각 구역에 대한 의미는 다음의 각 호와 같다.

≫ 공개구역: 통제구역과 제한구역을 제외한 회사 내 모든 구역

≫ 제한구역: 비 인가자의 불필요한 접근을 방지하기 위하여 출입통제가 필요한 구역

≫ 통제구역: 인가받은 자 이외의 불필요한 인원의 출입이 금지되는 구역

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

→ 물리적 보호구역별 보호대책 수립

「물리적보안 지침」 제 ○○조 (보호구역의 관리)

① 통제구역으로 지정된 장소는 다음과 같은 통제를 적용한다.

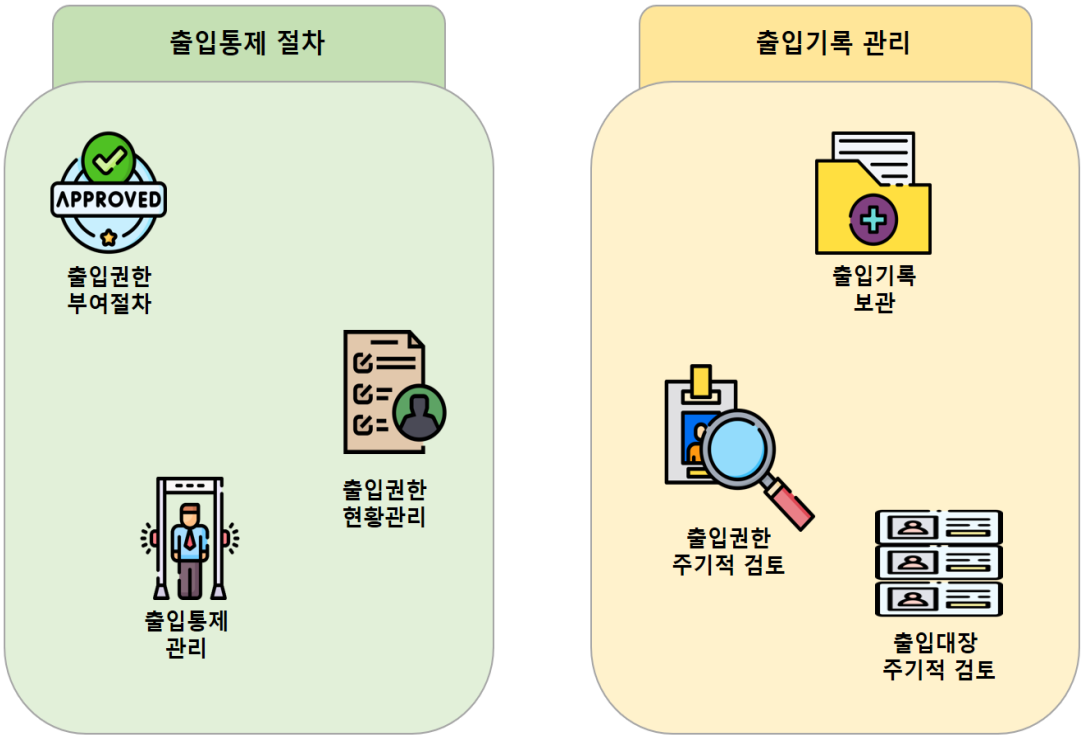
≫ 출입통제 및 감시를 위해 출입통제시스템, 감시카메라(CCTV) 등을 설치

≫ 비인가자의 출입이 제한되는 '통제구역' 표시

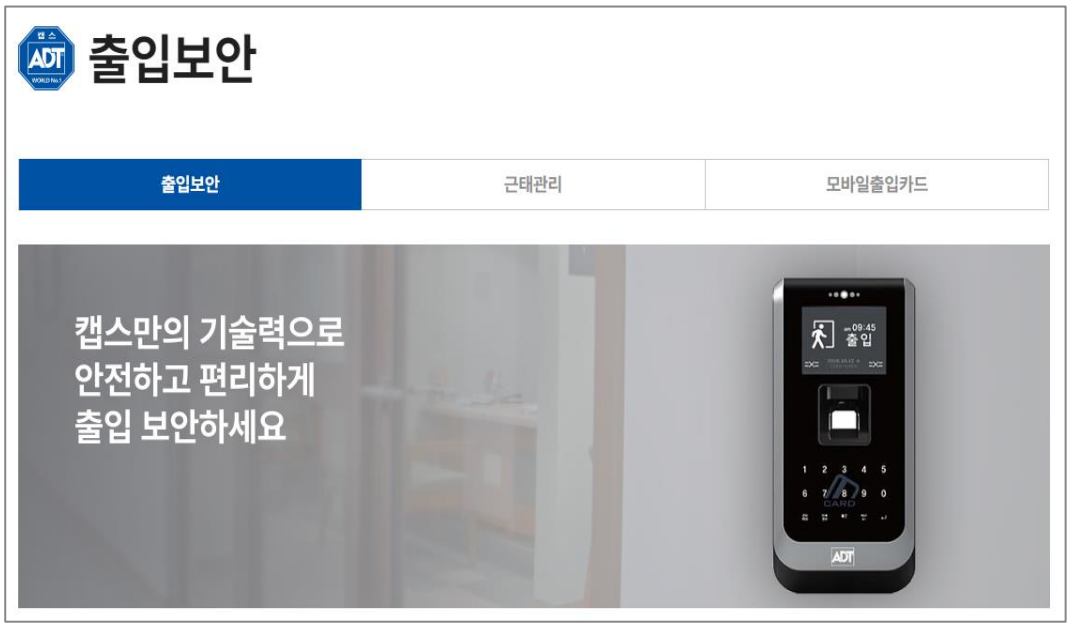
≫ 인가자 외의 인원 출입시 담당자 인솔

※ 통제구역 안내표(이해를 돕기 위한 예시)

2.4.2 출입통제

세부분야	2.4.2 출입통제
인증 기준	보호구역은 인가된 사람만이 출입하도록 통제하고 책임추적성을 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 출입기록을 일정기간 보존하고 출입기록 및 출입권한을 주기적으로 검토하고 있는가?
기준 요약도	
운영 방안	**◇ 보호구역은 출입절차에 따라 출입이 허가된 자만 출입하도록 통제하고 있는가?** **→ 내·외부자 출입통제 절차를 마련** ① 보호구역별로 출입 가능한 부서·직무·업무를 정의, 출입권한이 부여된 임직원 식별하고 그 현황을 관리 ② 통제구역의 경우 업무목적에 따라 최소한의 인원만 출입할 수 있도록 통제 ③ 출입절차: 출입신청, 책임자 승인, 출입권한 부여 및 회수, 출입내역 기록, 출입기록 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 출입기록을 일정기간 보존하고 출입기록 및 출입권한을 주기적으로 검토하고 있는가?

→ 내·외부자 출입통제 절차 수립

「물리적보안 지침」 제 ○○조 (통제구역)

① 통제구역의 출입기록은 책임추적성을 확보할 수 있도록 2년 이상 보관하고 분기별 검토한다.

≫ 출입기록: 출입자(소속·성명·연락처), 출입일시, 출입사유, 출입증번호, 승인자

≫ 출입검토: 장기 미 출입자, 비인가 출입 시도, 출입권한 과다부여 등

≫ 검토사항: 직무변경·퇴직 등에 따른 출입권한 조정·삭제, 출입증 회수 등

2.4.3 정보시스템 보호

세부분야	2.4.3 정보시스템 보호
인증 기준	정보시스템은 환경적 위협과 유해요소, 비인가 접근 가능성을 감소시킬 수 있도록 중요도와 특성을 고려하여 배치하고, 통신 및 전력 케이블이 손상을 입지 않도록 보호하여야 한다.
주요 확인사항	• 정보시스템의 중요도, 용도, 특성 등을 고려하여 배치 장소를 분리하고 있는가? • 정보시스템의 실제 물리적 위치를 손쉽게 확인할 수 있는 방안을 마련하고 있는가? • 전력 및 통신케이블을 외부로부터의 물리적 손상 및 전기적 영향으로부터 안전하게 보호하고 있는가?
기준 요약도	
운영 방안	◇ 정보시스템의 중요도, 용도, 특성 등을 고려하여 배치 장소를 분리하고 있는가? → 물리적 보호 ① 전산랙을 이용하여 시스템을 외부로부터 보호 ② 중요시스템 잠금 및 별도 물리적 안전장치 보호

※ 전산실 구조도(이해를 돕기 위한 예시)

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

→ 물리적 위치 확인방안 (배치도, 자산목록 등)을 마련

① 보안사고, 장애 발생 시 신속한 조치를 위한 물리적 배치도 (시설 단면도, 배치도 등), 자산목록 전사관리

② 자산목록 등에 물리적 위치 항목을 포함하고 현행화하여 최신본 유지

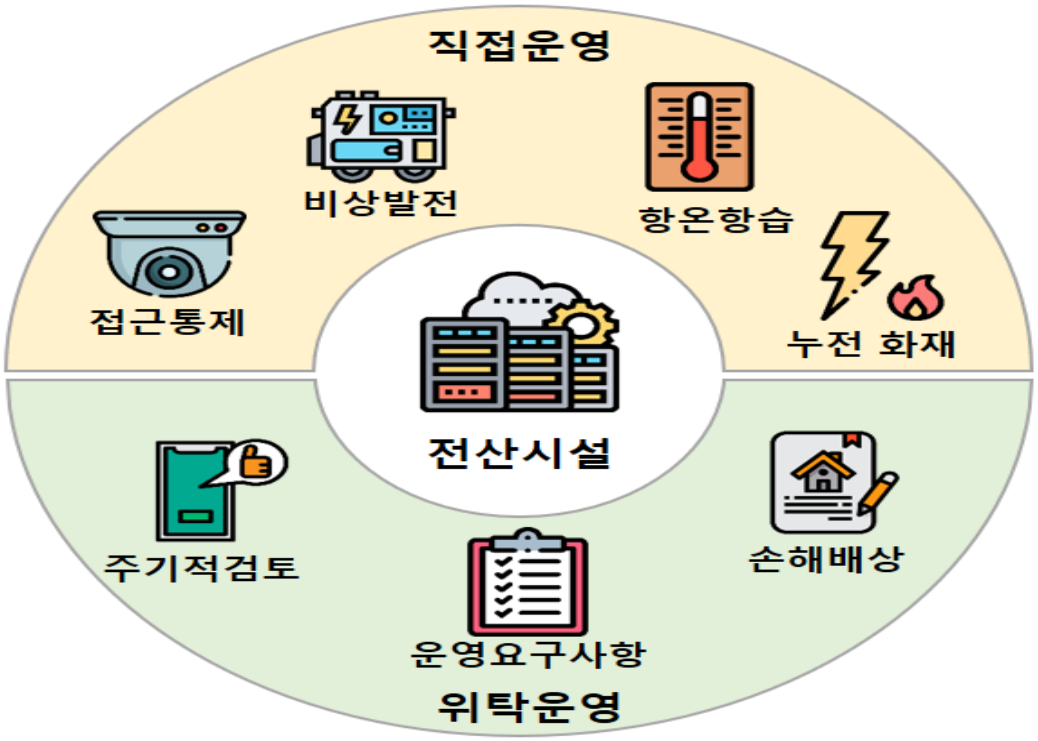
◇ 물리적 손상 및 전기적 영향으로부터 안전하게 보호

→ 물리적 손상 보호 관리

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

② 배전반, 강전실, 약전실 등에는 인가된 최소한의 인력만 접근할 수 있도록 접근통제

2.4.4 보호설비 운영

세부분야	2.4.4 보호설비 운영
인증 기준	보호구역에 위치한 정보시스템의 중요도 및 특성에 맞춰 온·습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 보호설비를 갖추고 운영절차를 수립·운영하여야 한다
주요 확인사항	• 각 보호구역의 중요도 및 특성에 따라 화재, 수해, 전력 이상 등 인재 및 자연재해 등에 대비하여 필요한 설비를 갖추고 운영절차를 수립하여 운영하고 있는가? • 외부 집적정보통신시설(IDC)에 위탁 운영하는 경우 물리적 보호에 필요한 요구사항을 계약서에 반영하고 운영상태를 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 운영절차를 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 요구사항을 계약서 반영

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

② IDC의 책임보험 가입 여부 확인

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

→ 물리적 보호 보안요구사항 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)

2.4.5 보호구역 내 작업

<table>
<tr><th>세부분야</th><th>2.4.5 보호구역 내 작업</th></tr>
<tr><td>인증
기준</td><td>보호구역 내에서의 비인가행위 및 권한 오·남용 등을 방지하기 위한 작업 절차를 수립·이행하고, 작업 기록을 주기적으로 검토하여야 한다</td></tr>
<tr><td>주요
확인사항</td><td>• 정보시스템 도입, 유지보수 등으로 보호구역 내 작업이 필요한 경우에 대한 공식적인 작업신청 및 수행 절차를 수립·이행하고 있는가?
• 보호구역 내 작업이 통제 절차에 따라 적절히 수행되었는지 여부를 확인하기 위하여 작업 기록을 주기적으로 검토하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td>
① 작업신청서 — 작업 계획서 작성
② 승인·작업기록 — 작업 계획 승인 및 기록 저장 보관
③ 담당자 입회 관리 감독 — 책임 추적성 확보 및 모니터링
④ 작업내역 정기적 검토 — 승인내역, 출입기록, 로그 등 이상징후 탐지
</td></tr>
<tr><td>운영
방안</td><td>
◇ 정보시스템 도입, 유지보수 등으로 보호구역 내 작업이 필요한 경우에 대한 공식적인 작업신청 및 수행 절차를 수립·이행하고 있는가?

→ 공식적인 작업 신청 및 수행

「물리적보안 지침」 제 ○○조 (보호구역 작업통제)
① 보호구역 에서의 작업은 비인가 행위 및 권한 오·남용 등을 방지하기 ‘보호구역 출입 신청서’를 통해 관리되어야 한다.
② 부서 정보보호책임자는 물리보안책임자에게 출입 허가를 득 해야한다.
</td></tr>
</table>

보호구역 출입 신청서

부서 정보보호책임자	물리보안 책임자

신청자		소 속	
방문 업체		연락처	
관련 부서		부서 담당자	
출입 일자		작업 시간	00시 00분 ~ 00시 00분
출입목적	□ 작업 □ 장애처리 □ 점검 □ 기타( )		
작업 내용			
특이사항			
비고			

본인은 업무 수행을 위하여 다음과 같이 출입을 신청하오니 허락하여 주시기 바랍니다

00년 00월 00일

서 명 : (인)

사내 규정을 통한 출입절차 마련

물리적보안 관리지침

① 보호구역 에서의 작업은 비인가 행위 및 권한 오·남용 등을 방지하기 '보호구역 출입 신청서'를 통해 관리되어야 한다.

② 부서 정보보호책임자는 물리보안책임자에게 출입 허가를 득 해야한다

※ 전산실 출입신청(이해를 돕기 위한 예시)

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

→ 주기적 검토 실시

「**물리적보안 지침**」 제 ○○조 (보호구역 작업통제)

③ 물리보안 책임자는 "보호구역 출입기록 관리대장'을 작성하고 분기별 1회 각 호에 따라 작업기록을 검토해야 한다.

≫ 작업검토: 사전 승인 내역, 출입기록, 작업기록 등에 대한 정기적 검토 수행 등

≫ 검토방법: 출입 신청서와 출입 내역(관리대장, 시스템 로그 등) 일치성 등

보호구역 출입기록 관리대장

점검 일자 :

일시	출입시간	퇴소시간	작업내용	출 입 자			입 회 자			비고
				소속	이름	연락처	소속	이름	서명(인)	

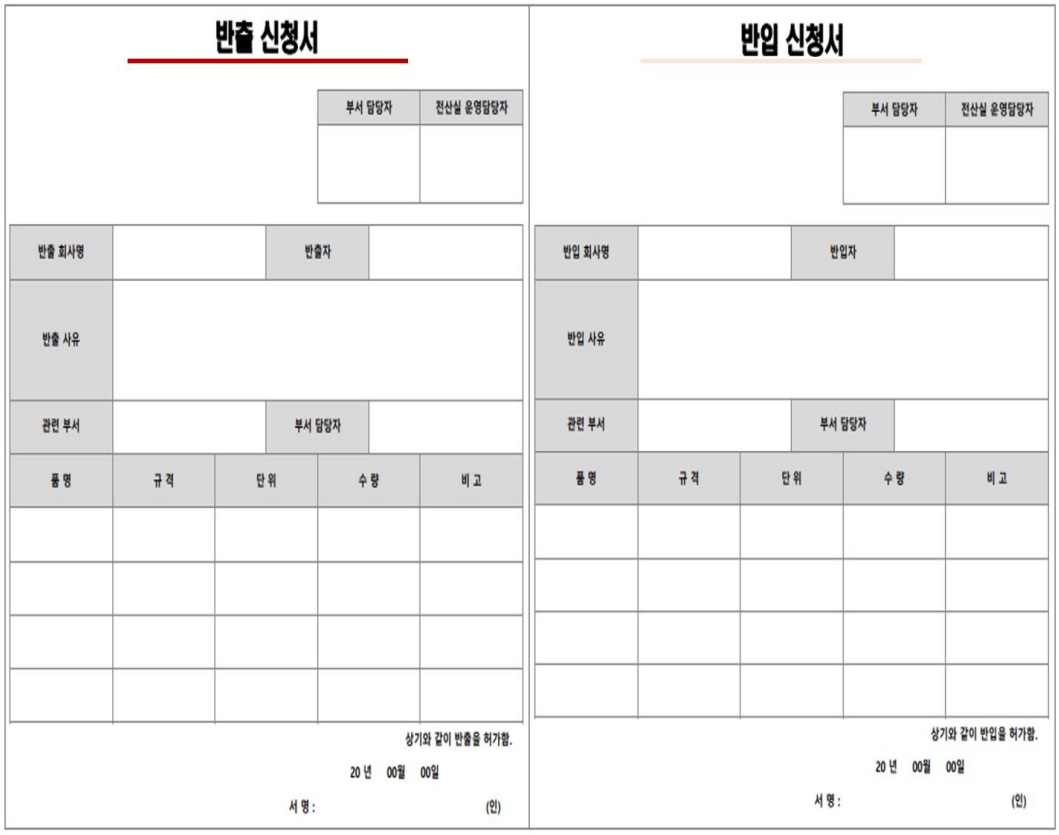
※ 통제구역 출입대장(이해를 돕기 위한 예시)

2.4.6 반출입 기기 통제

세부분야	2.4.6 반출입 기기 통제
인증 기준	보호구역 내 정보시스템, 모바일 기기, 저장매체 등에 대한 반출입 통제절차를 수립·이행하고 주기적으로 검토하여야 한다.
주요 확인사항	• 정보시스템, 모바일 기기, 저장매체 등을 보호구역에 반입하거나 반출하는 경우 정보유출, 악성코드 감염 등 보안사고 예방을 위한 통제 절차를 수립·이행하고 있는가? • 반출입 통제절차에 따른 기록을 유지·관리하고, 절차 준수 여부를 확인할 수 있도록 반출입 이력을 주기적으로 점검하고 있는가?
기준 요약도	
운영 방안	**◇ 정보시스템, 모바일 기기, 저장매체 등을 보호구역에 반입하거나 반출하는 경우 정보유출, 악성코드 감염 등 보안사고 예방을 위한 통제 절차를 수립·이행하고 있는가?** **→ 반출입 기기 통제절차 수립** 「**물리적보안 지침**」 제 ○○조 (기기 반출입 통제) ① 통제구역에서의 정보유출, 악성코드 감염 등 보안사고를 예방하기 위해 다음과 같이 기기 반출입을 통제하여야 한다. ≫ 반출입 통제 대상: 정보시스템(서버, 네트워크 장비 등), 모바일 기기(노트북, 스마트패드, 스마트폰 등), 저장매체(HDD, SSD, USB메모리, 외장하드디스크,

CD/DVD, 테이프 등) 등

≫ 정보시스템 관리자는 반출입 통제 대상 기기에 대해 보안점검(백신설치, 악성코드검사, 보안업데이트, 매체봉인, 자료유출 여부 등)을 실시한 후 기기 반출입 허용



반출 신청서

부서 담당자	전산실 운영담당자

반출 회사명		반출자	
반출 사유			
관련 부서		부서 담당자	

품 명	규 격	단 위	수 량	비 고

상기와 같이 반출을 허가함.

20 년 00월 00일

서 명 : (인)

반입 신청서

부서 담당자	전산실 운영담당자

반입 회사명		반입자	
반입 사유			
관련 부서		부서 담당자	

품 명	규 격	단 위	수 량	비 고

상기와 같이 반입을 허가함.

20 년 00월 00일

서 명 : (인)

※ 반출입 신청서(이해를 돕기위한 예시)

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

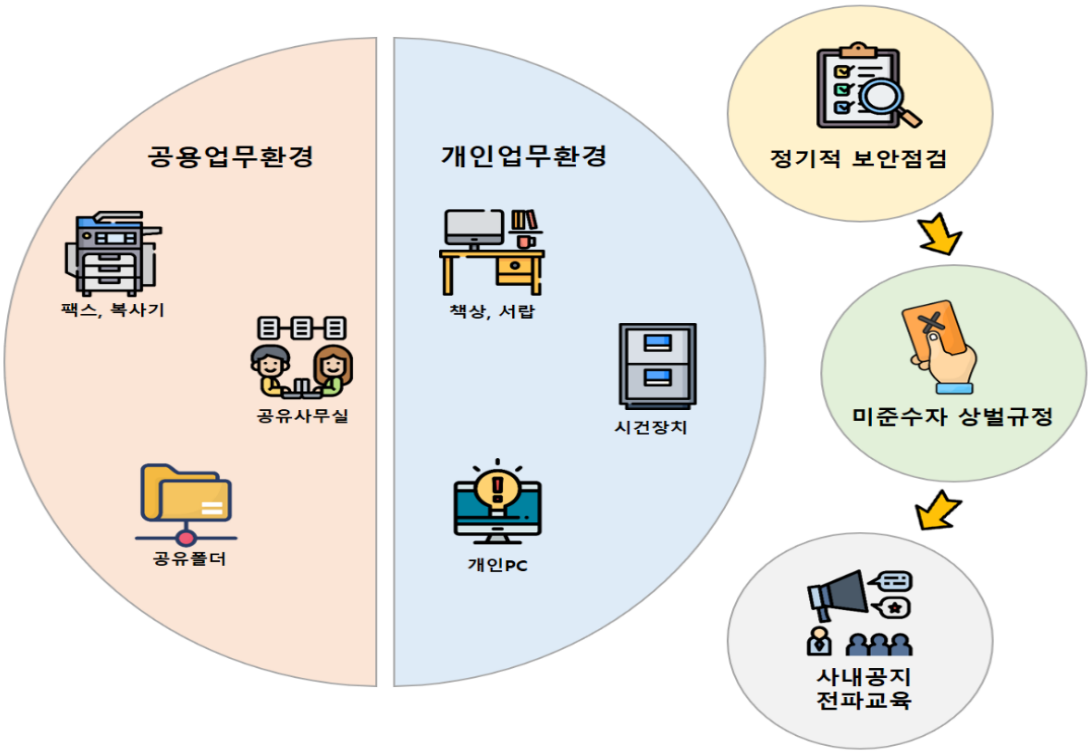
→ 반출입 기기 이력 주기적 관리 검토

① 반출입 통제절차에 따른 기록을 유지·관리하고, 절차 준수 여부를 확인할 수 있도록 반출입 이력을 주기적으로 점검하여야 한다.

≫ 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 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 문서고, 공용 PC, 복합기, 파일서버 등 공용으로 사용하는 시설 및 사무용 기기에 대한 보호대책을 수립·이행하고 있는가? • 업무용 PC, 책상, 서랍 등 개인업무 환경을 통한 개인정보 및 중요정보의 유·노출을 방지하기 위한 보호대책을 수립·이행하고 있는가? • 개인 및 공용업무 환경에서의 정보보호 준수 여부를 주기적으로 검토하고 있는가?
기준 요약도	
운영 방안	**◇ 문서고, 공용 PC, 복합기, 파일서버 등 공용으로 사용하는 시설 및 사무용 기기에 대한 보호대책을 수립·이행하고 있는가?** **→ 공용환경 보호대책 수립** ① 문서고: 출입인원 최소화, 부서·업무별 출입 접근권한 부여, 출입 이력관리 ② 공용PC: 담당자 지정, 화면보호기 설정, 로그인 암호설정, 주기적 패스워드 변경, 중요정보 저장 제한, 백신 설치, 보안업데이트 등 ③ 공용사무기기: 팩스, 복사기, 프린트 등의 공용사무기기 주변에 중요 문서 방치 금지 ④ 파일서버: 부서·업무 접근권한 부여, 불필요한 정보공개 최소화, 사용자별 계정 발급

⑤ 공용 사무실: 회의실, 프로젝트룸 등 공용사무실 내 중요정보 문서 방치 금지

⑥ 기타 공용업무환경에 대한 보호대책 수립

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

→ 업무환경 보안 보호대책 수립

「물리적보안 지침」 제 ○○조 (업무환경 보안점검)

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

② 업무환경 보안점검 결과 중대한 위반사실이 지적되었거나 평가결과가 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 환경 보안 점검표 (이해를 돕기 위한 예시)

◇ 개인 및 공용업무 환경에서의 정보보호 준수 여부를 주기적으로 검토하고 있는가?

→ 개인 및 공용업무 환경에서의 정보보호 준수 여부를 주기적으로 검토

① 개인 및 공용업무 환경에서의 정보보호 준수 여부를 주기적으로 검토하여야 한다.

≫ 개인 및 공용업무 환경 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 보안점검결과보고 (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 권한부여 시 사용자에게 보안책임이 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 접근권한생성·등록·변경 시 직무별 접근권한 분류 체계에 따라 업무상 필요한 최소한의 권한만을 부여하고 있는가? • 사용자에게 계정 및 접근권한을 부여하는 경우 해당 계정에 대한 보안책임이 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? → 계정관리 절차 수립(예시)

「**정보시스템 운영관리 지침**」 제 ○○조 (사용자 계정발급)

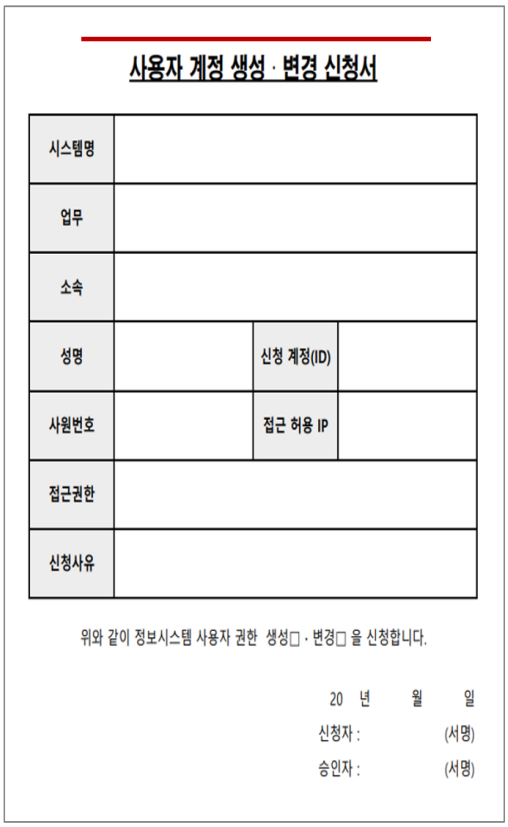
① 사용자에게 계정을 발급·변경·해지하거나 접근권한을 부여할때 각 호의 절차를 따른다.

≫ 사용자 계정 생성·변경 신청서 작성 신청

≫ 정보시스템 관리자 검토·승인·계정발급

≫ 계정발급 내용 기록 보관

② 사용자에게 계정 및 접근권한을 부여하는 경우 해당 계정에 대한 보안책임이 본인에게 있음을 명확히 인식할 수 있도록 보안서약서의 내용을 상기 하도록하고 서명징구한다.



사용자 계정 생성 · 변경 신청서

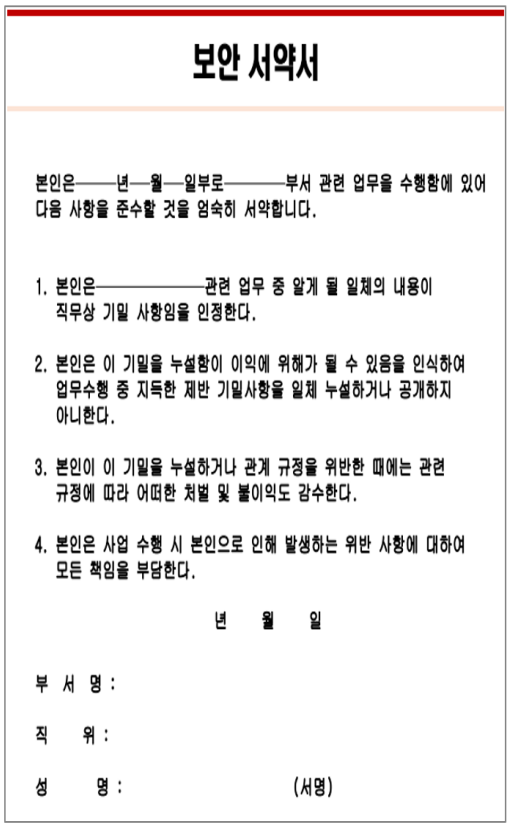
시스템명			
업무			
소속			
성명		신청 계정(ID)	
사원번호		접근 허용 IP	
접근권한			
신청사유			

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 업무을 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)

※ 계정발급 신청서 (이해를 돕기 위한 예시)

◇ 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?

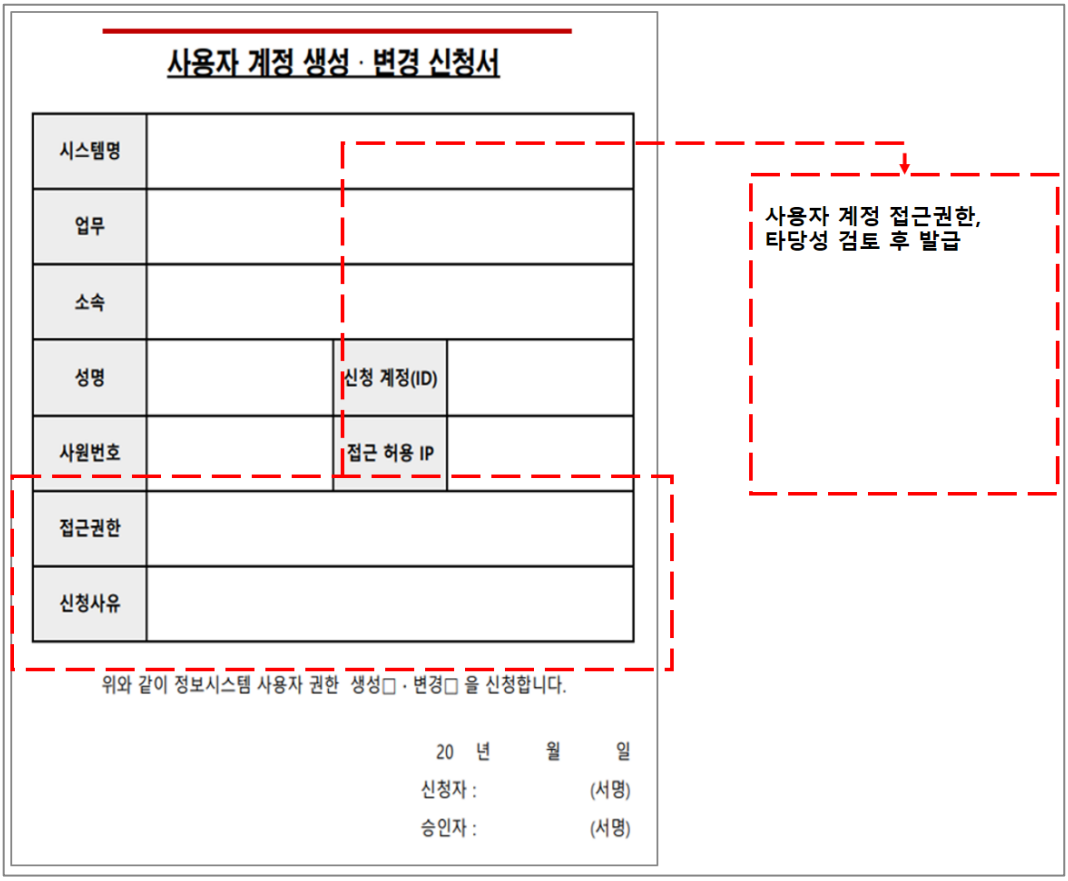
→ 직무별 접근권한 업무에 필요한 최소한으로만 부여

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

② 중요 정보 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 중요 정보 또는 개인정보에 접근하지 못하도록 권한 세분화

④ 권한 부여 또는 변경 시 승인절차 등을 통하여 적절성 검토 등



※ 계정발급 권한 점검 (이해를 돕기 위한 예시)

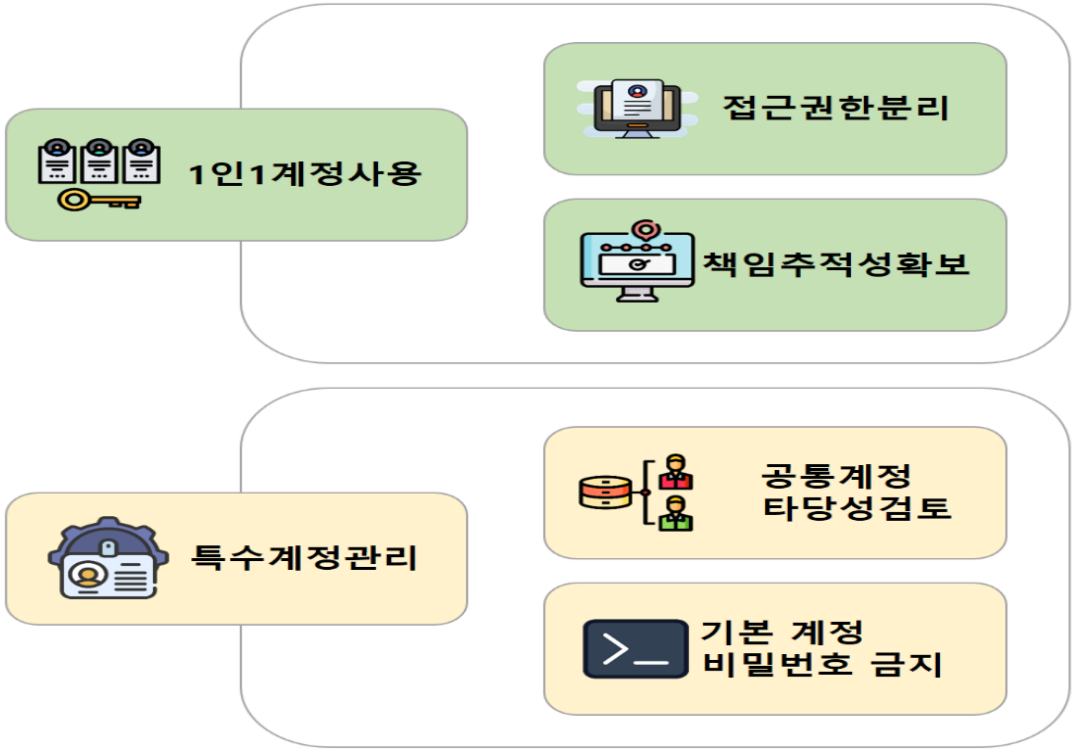
◇ 사용자에게 계정 및 접근권한을 부여하는 경우 해당 계정에 대한 보안책임이 본인에게 있음을 명확히 인식시키고 있는가?

→ 보안책임이 본인에게 있음을 보안 인식 절차 필요

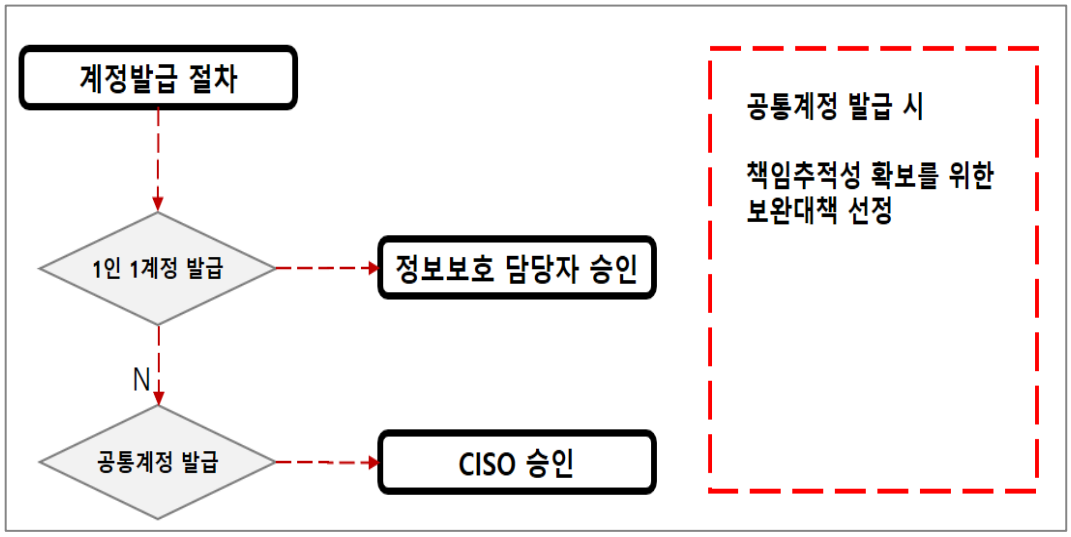
① 정보보호 및 개인정보보호 정책, 서약서 등에 계정에 대한 책임과 의무를 명기(타인에게 본인 계정 및 비밀번호 공유 대여 금지, 공공장소에서 로그인 시 주의사항 등)

② 서약서, 이메일, 시스템 공지, 교육 등 다양한 방법 활용

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 책임추적성 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** **「정보시스템 운영관리지침 」** 제 ○○조 (사용자 계정관리) ① 정보시스템 및 개인정보처리시스템은 사용자의 책임추적성 확보를 하기 위해 1인 1계정 발급을 원칙으로한다.

② 정보시스템 계정은 추측 가능한 식별자 (root·admin·administrator등) 사용을 제한한다.



※ 계정 발급 절차 (이해를 돕기 위한 예시)

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

→ 불가피한 공용계정 사용 시 보완대책 필요

「정보시스템 운영관리지침」 제 ○○조 (사용자 계정관리)

③ 업무상 불가피하게 공용계정을 사용하는 경우 그 사유와 타당성을 검토하고 책임추적성 확보 등 추가 보완대책을 마련하여 정보시스템 책임자의 승인을 받아야 한다

≫ 업무 분장상 정·부의 역할이 구분되어 관리자 계정을 공유하는 경우에도 사용자 계정을 별도로 부여하고 사용자 계정으로 로그인 후 관리자 계정으로 변경

≫ 유지보수 업무 등을 위하여 임시적으로 계정을 공유한 경우 업무 종료 후 즉시 해당 계정의 비밀번호 변경

≫ 업무상 불가피하게 공용계정 사용이 필요한 경우 그 사유와 타당성을 검토하여 책임자의 승인을 받고 책임추적성을 보장할 추가 통제방안 적용

2.5.3 사용자 인증

세부분야	2.5.3 사용자 인증
인증 기준	정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용하여야 한다. 또한 로그인 횟수 제한, 불법 로그인 시도 경고 등 비인가자 접근 통제방안을 수립·이행하여야 한다.
주요 확인사항	• 정보시스템 및 개인정보처리시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법로그인 시도 경고 등 안전한 사용자 인증 절차에 따라 통제하고 있는가? • 정보통신망을 통하여 외부에서 개인정보처리시스템에 접속하려는 경우에는 법적요구사항에 따라 안전한 인증수단 또는 안전한 접속수단을 적용하고 있는가?
기준 요약도	
운영 방안	**◇ 정보시스템 및 개인정보처리시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 따라 통제하고 있는가?** **→ 계정 도용 방지** **「정보시스템 권한관리 지침」** 제 ○○조 (사용자 인증) ① 정보시스템 인증방식을 다음 각 호에 중 하나로 선택 구현해야한다. ≫ 비밀번호 ≫ OTP, 모바일 OTP, 일회성 비밀번호

≫ 전자 서명(인증서)

≫ 생체인증

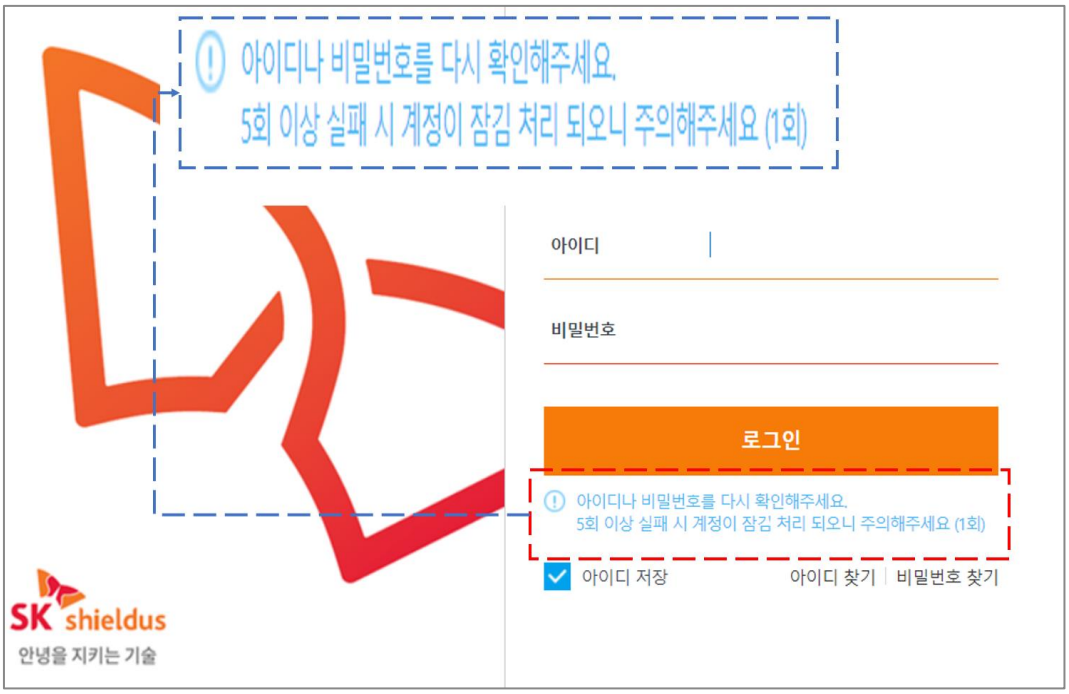
② 정보시스템의 비인가자의 접근을 통제를 위해 각호의 사항을 적용해야 한다.

≫ 로그인 실패횟수 5회 이상 제한

≫ 접속 유지시간 최소 10분 이상 제한

≫ 동일 계정의 동시 접속 세션 수 제한

≫ 불법 로그인 시도 등 경고



※ 출처: 임계값 설정 예시 (SK쉴더스)

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

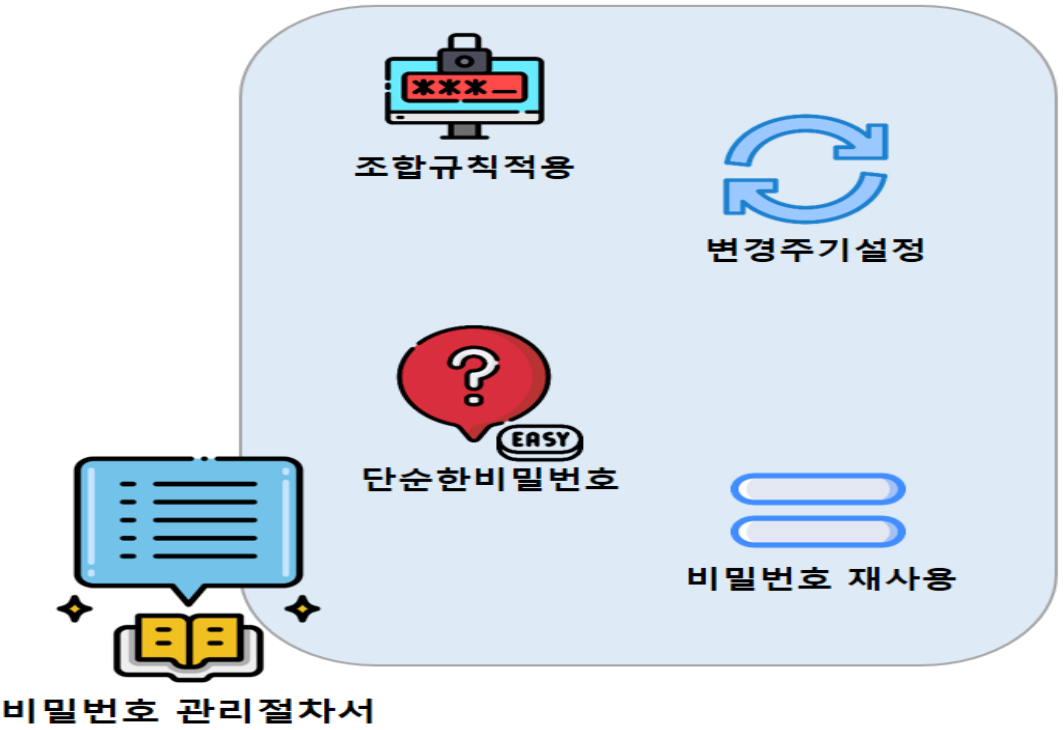
→ 외부에서 개인정보처리시스템 접근

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

② 안전한 접속수단: 가상사설망(VPN), 전용망 등

※ 출처: OTP 인증 (SK쉴더스)

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 관리절차를 수립·이행하여야 한다
주요 확인사항	• 정보시스템 및 개인정보처리시스템에 대한 안전한 사용자 비밀번호 관리절차 및 작성규칙을 수립·이행하고 있는가? • 정보주체(이용자)가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성규칙을 수립·이행하고 있는가?
기준 요약도	
운영 방안	**◇ 정보시스템 및 개인정보처리시스템에 대한 안전한 사용자 비밀번호 관리절차 및 작성규칙을 수립·이행하고 있는가?** **→ 비밀번호 관리 절차 및 작성규칙 수립 (예시)** **「정보시스템 운영 관리지침」** 제 ○○조 (비밀번호 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 비밀번호 변경

해야한다

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

→ 비밀번호 정책 수립

「정보시스템 운영 관리지침」 제 ○○조 (비밀번호 관리)

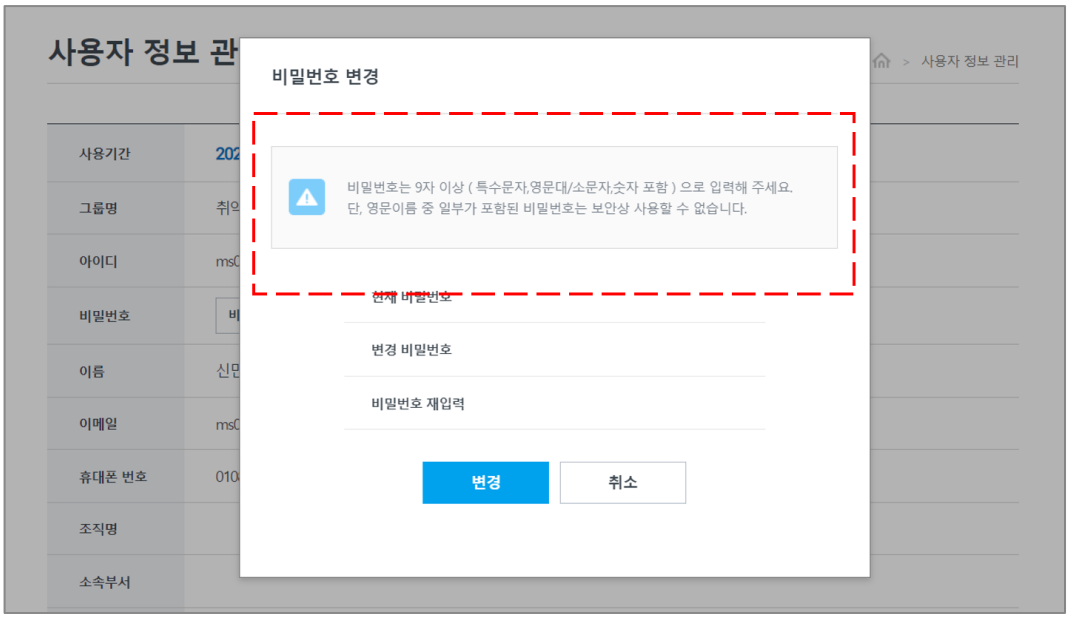
① 비밀번호는 숫자와 영문자, 특수문자 등을 혼합하여 9자리 이상으로 정하고, 분기별 1회 이상 주기적으로 변경 사용하여야 한다.

≫ 영문 대문자(26 개)

≫ 영문 소문자(26 개)

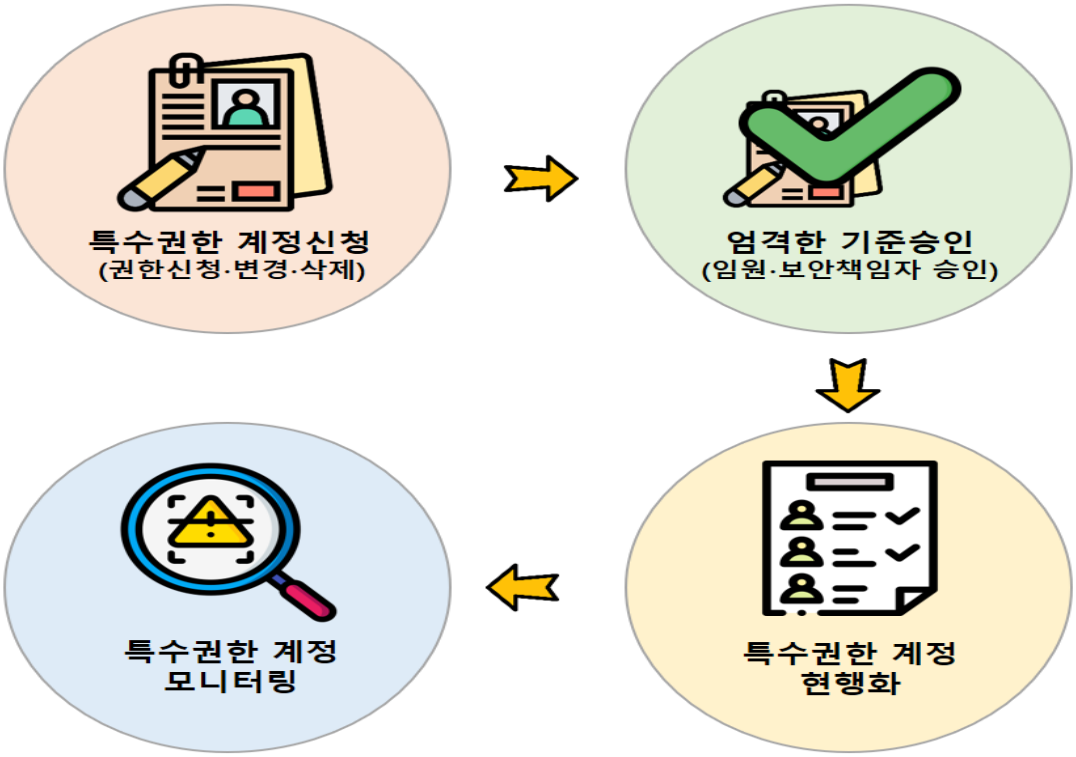
≫ 숫자(10 개)

≫ 특수문자(32개)



※ 출처: 비밀번호변경 (SK쉴더스)

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 특수권한은 최소한의 인원에게만 부여될 수 있도록 공식적인 권한신청 및 승인 절차를 수립·이행하고 있는가? • 특수 목적을 위하여 부여한 계정 및 권한을 식별하고 별도 목록으로 관리하는 등 통제절차를 수립·이행하고 있는가?
기준 요약도	
운영 방안	**◇ 관리자 권한 등 특수권한은 최소한의 인원에게만 부여될 수 있도록 공식적인 권한 신청 및 승인 절차를 수립·이행하고 있는가?** **→ 특수권한 관리절차 수립** **「정보시스템 권한관리 지침」** 제 ○○조 (특수계정 관리) ① 특수 계정·권한을 최소한의 업무 수행자에게만 부여할 수 있도록 하고 정보보호 담당자가 정보보호최고책임자의 승인을 득 한 후 발급한다.

※ 특수권한 계정발급신청 (이해를 돕기 위한 예시

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

→ 특수권한의 통제 절차 수립

「정보시스템 권한관리 지침」 제 ○○조 (특수계정 관리)

② 특수 계정·권한 다음 각 호의 통제절차를 이행해야 한다.

≫ 특수 권한계정은 일반 사용자에게 부여하지 않으며, 발급된 권한은 분기 1회 권한 재평가 및 현행화.

≫ 패스워드 관리절차 준수상태를 분기별 1회 이상 점검

≫ 서버관리자는 일반 계정을 접속한 후 슈퍼유저 계정을 획득

≫ 특수계정은 Console 및 특정 단말에서만 접속

2.5.6 접근권한 검토

<table>
<tr><th>세부분야</th><th>2.5.6 접근권한 검토</th></tr>
<tr><td>인증
기준</td><td>정보시스템과 개인정보 및 중요정보에 접근하는 사용자 계정의 등록·이용·삭제 및 접근권한의 부여·변경·삭제 이력을 남기고 주기적으로 검토하여 적정성 여부를 점검하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 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 검토기준, 검토주체, 검토방법, 주기 등을 수립하여 정기적 검토를 이행하고 있는가?
• 접근권한 검토 결과 접근권한 과다 부여, 권한부여 절차 미준수, 권한 오·남용 등 문제점이 발견된 경우 그에 따른 조치절차를 수립·이행하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근권한 생성·등록·부여·이용·변경·말소 등의 이력을 남기고 있는가?

→ 사용자 계정 및 접근권한 생성·등록·부여·이용·변경·말소 등의 이력 보관

「정보시스템 운영관리 지침」 제 ○○조 (계정 접속기록관리)
① 정보시스템 책임자는 책임추적성 및 사고발생 시 조사를 위해 각 호의 사항을 5년간 저장관리 해야 한다.</td></tr>
</table>

≫ 계정 및 관리구분(발급·변경·해지)

≫ 신청정보: 신청자, 신청일자, 신청목적, 사용기간

≫ 승인정보: 승인자, 승인일자

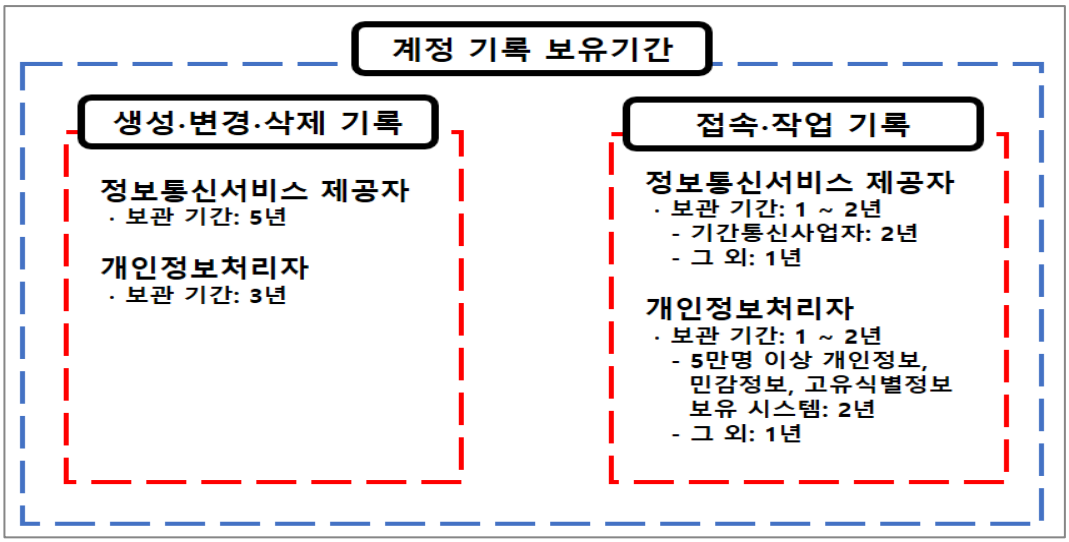
≫ 등록정보: 등록자, 등록일자

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

→ 개인정보처리시스템 로그 기록 법적 요구사항 반영

① **「개인정보 보호법」**에 따른 개인정보처리자: 최소 3년간 보관

② **「개인정보 보호법」** 특례조항에 따른 정보통신서비스 제공자 등: 최소 5년간 보관



※ 계정 생성 및 작업기록 보관 (이해를 돕기 위한 예시)

◇ 정보시스템과 개인정보 및 중요정보에 대한 사용자 계정 및 접근권한의 적정성 검토기준, 검토주체, 검토방법, 주기 등을 수립하여 정기적 검토를 이행하고 있는가?

→ 개인정보 및 중요정보에 계정 검토 분기 1회(권고) 실시

「정보시스템 운영관리 지침」 제 ○○조 (계정 접속기록관리)

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

② 접근권한 부여의 적정성 검토 항목(예시)

≫ 공식적인 절차에 따른 접근권한 부여 여부

≫ 접근권한 분류체계의 업무목적 및 보안정책 부합 여부

≫ 접근권한 승인자의 적절성

≫ 직무변경 시 기존 권한 회수 후 신규 업무에 대한 적절한 권한 부여 여부

≫ 업무 목적 외 과도한 접근권한 부여 여부

≫ 특수권한 부여·변경·발급 현황 및 적정성

≫ 협력업체 등 외부자 계정·권한 발급 현황 및 적정성

≫ 접근권한 신청·승인 내역과 실제 접근권한 부여 현황의 일치 여부

≫ 장기 미접속자 계정 현황 및 삭제(또는 잠금) 여부

≫ 휴직, 퇴직 시 지체 없이 계정 및 권한 회수 여부 등

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

→ 권한 관리 문제점 조치계획 수립 이행

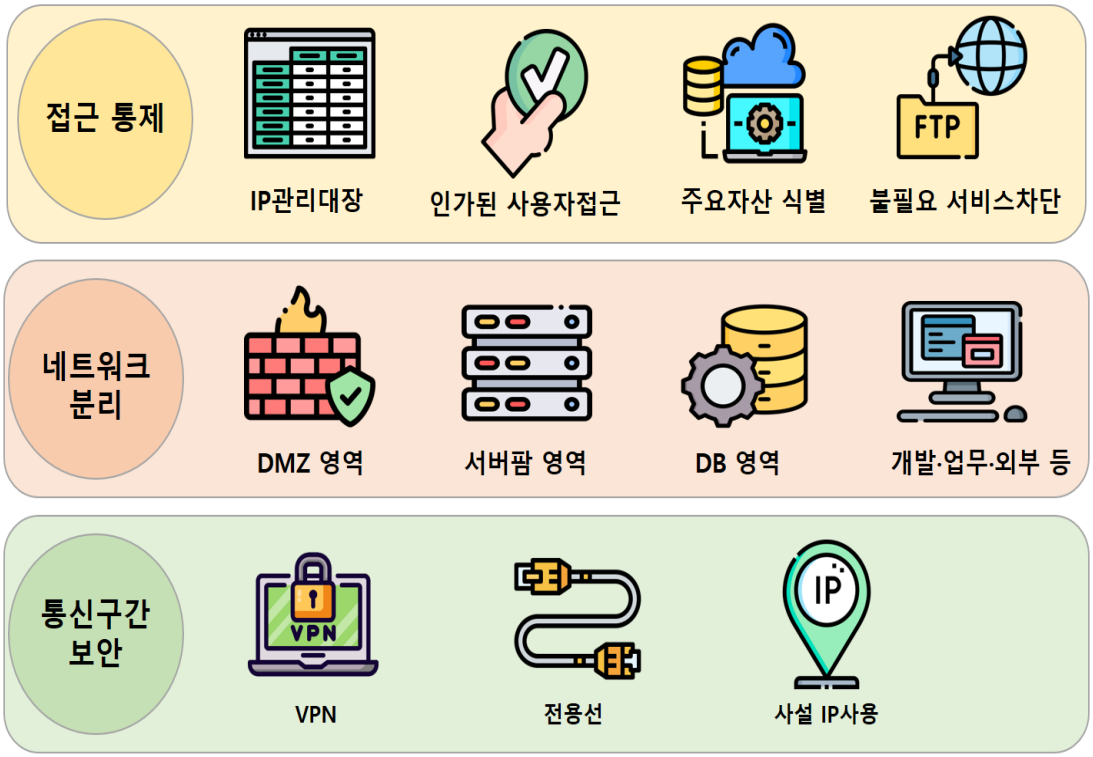
① 접근권한 검토 결과 권한의 과다 부여, 절차 미준수, 권한 오·남용 등 의심스러운 상황이 발견된 경우 소명요청 및 원인분석, 보완대책 마련, 보고체계 등이 포함된 절차 수립·이행

② 접근권한 검토 후 변경 적용된 권한에 대해서는 사용자 및 관련자에게 통지

③ 유사한 문제가 반복될 경우 근본 원인 분석 및 재발방지 대책 수립

2.6 접근통제

2.6.1 네트워크 접근

<table>
<tr><th>세부분야</th><th>2.6.1 네트워크 접근</th></tr>
<tr><td>인증
기준</td><td>네트워크에 대한 비인가 접근을 통제하기 위하여 IP관리, 단말인증 등 관리절차를 수립·이행하고, 업무목적 및 중요도에 따라 네트워크 분리[DMZ(Demilitarized Zone), 서버팜, 데이터베이스존, 개발존 등와 접근통제를 적용하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 조직의 네트워크에 접근할 수 있는 모든 경로를 식별하고 접근통제 정책에 따라 내부네트워크는 인가된 사용자만이 접근할 수 있도록 통제하고 있는가?
• 서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 네트워크 영역을물리적 또는 논리적으로 분리하고 각 영역 간 접근통제를 적용하고 있는가?
• 네트워크 대역별 IP주소 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 보호대책을 마련하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 조직의 네트워크에 접근할 수 있는 모든 경로를 식별하고 접근통제 정책에 따라 내부 네트워크는 인가된 사용자만이 접근할 수 있도록 통제하고 있는가?

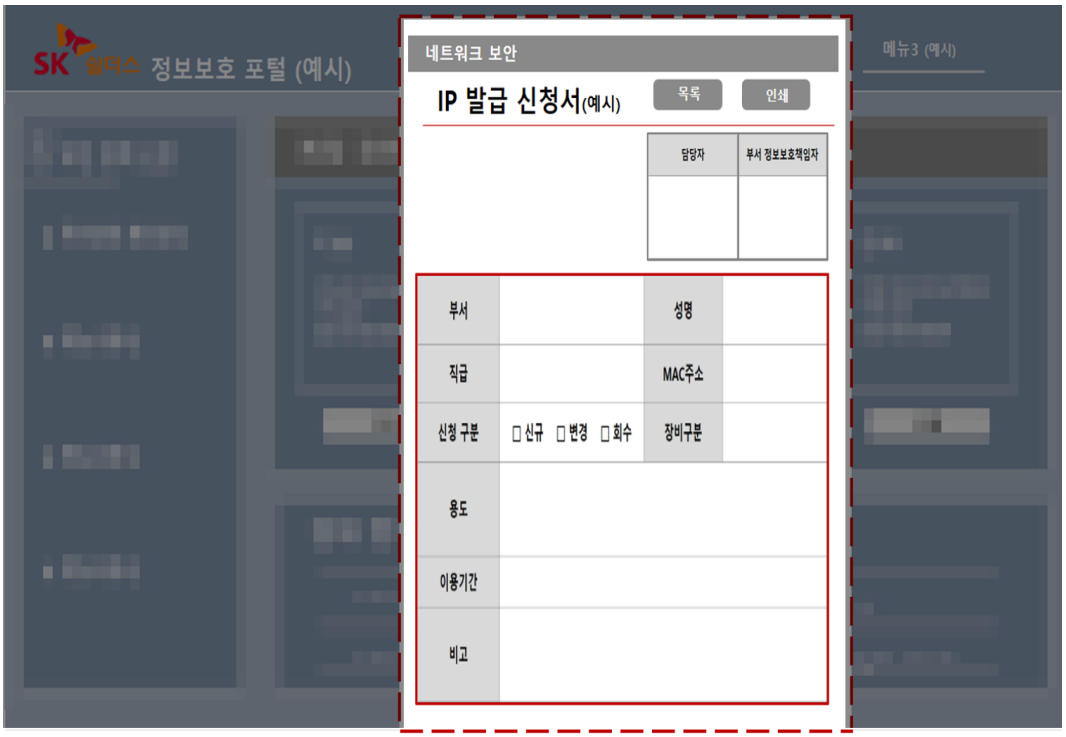
→ 네트워크 접근통제 관리절차를 수립·이행</td></tr>
</table>

「**정보시스템 운영관리지침**」 제 ○○조 (네트워크 접근)

① 사내 네트워크에 접근할 수 있는 모든 경로를 식별하고, 인가된 사용자만 접근할 수 있도록 통제 해야한다.

② IP주소는 발급은 'IP 발급신청서' 작성 부서 정보보호책임자의 승인을 득한 후 발급한다.

③ 네트워크 담당자는 'IP관리대장'에 현황을 기록 관리하며, 분기 1회 최신화 해야한다.



※ IP 발급신청서(이해를 돕기위한 작성 예시)

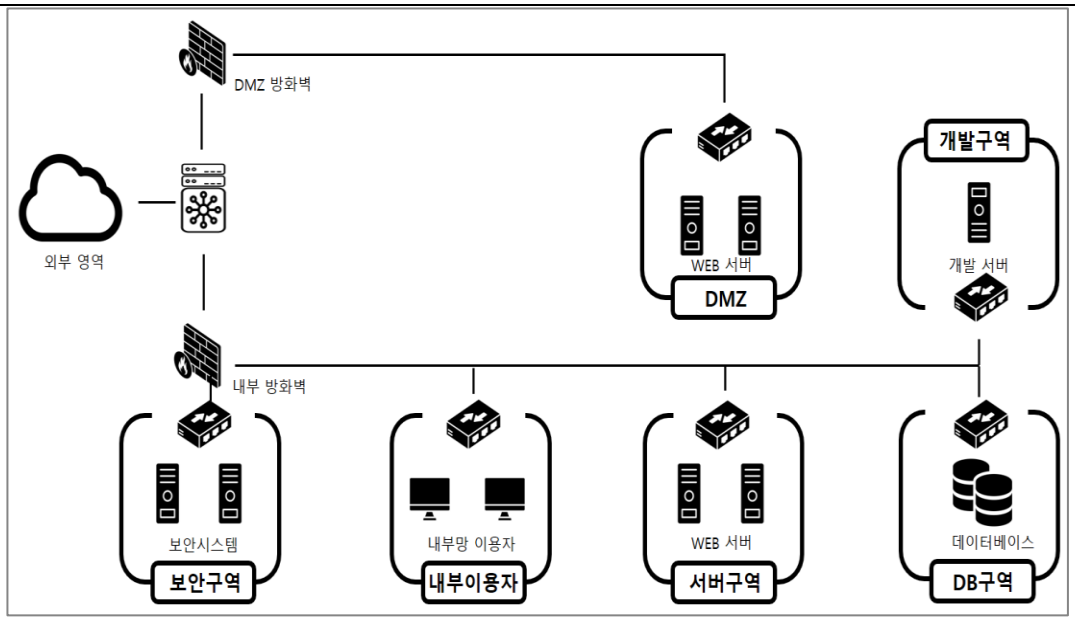
◇ 서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 각 영역 간 접근통제를 적용하고 있는가?

→ 네트워크 영역 분리

「**정보시스템 운영관리지침**」 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.

≫ DMZ, 서버팜, 데이터베이스, 운영환경, 개발환경, 외부자영역, 공개망 등



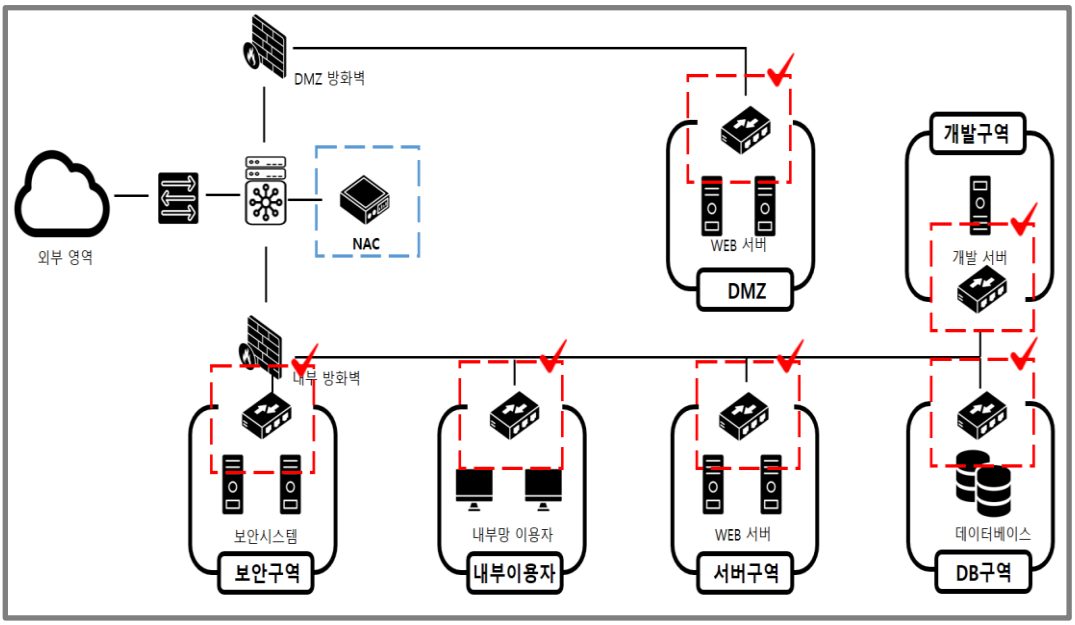
※ 네트워크 구성도 (이해를 돕기 위한 예시)

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

→ 사설 IP 할당 기준 수립

「**인증권한 관리지침**」 제 ○○조 (네트워크 접근)

① 내부 네트워크는 대역별 IP주소 부여 기준을 마련하여 데이터베이스 서버 등 중요 시스템이 외부와의 연결되지 않도록 사설 IP를 해야한다.

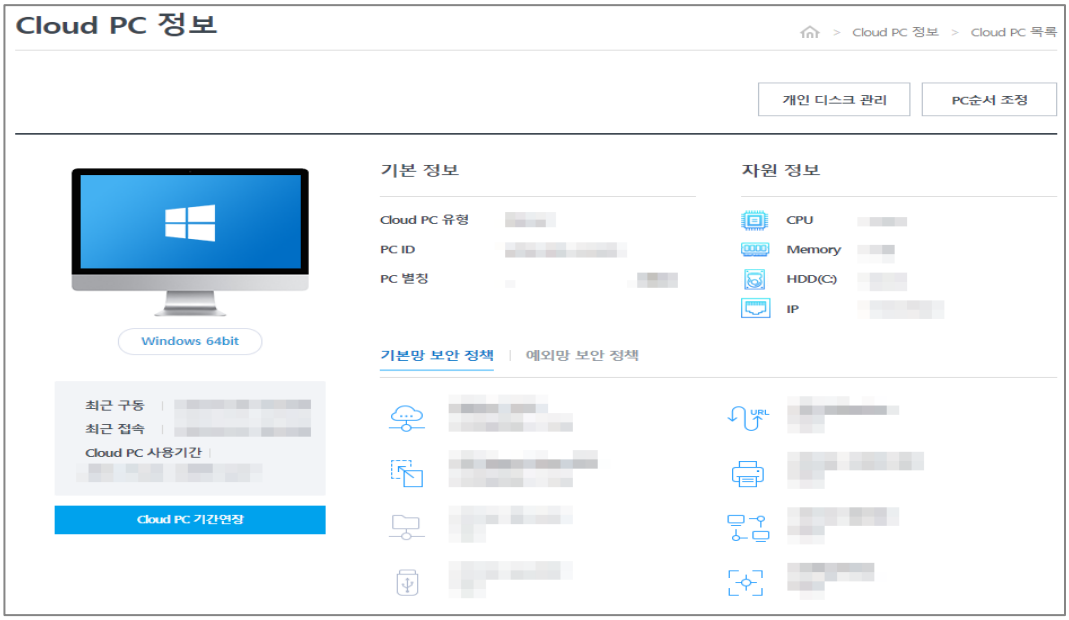


※ 네트워크 사설IP 적용 (이해를 돕기 위한 예시)

◇ 물리적으로 떨어진 IDC, 지사, 대리점 등과의 네트워크 연결 시 전송구간 보호대책을 마련하고 있는가?

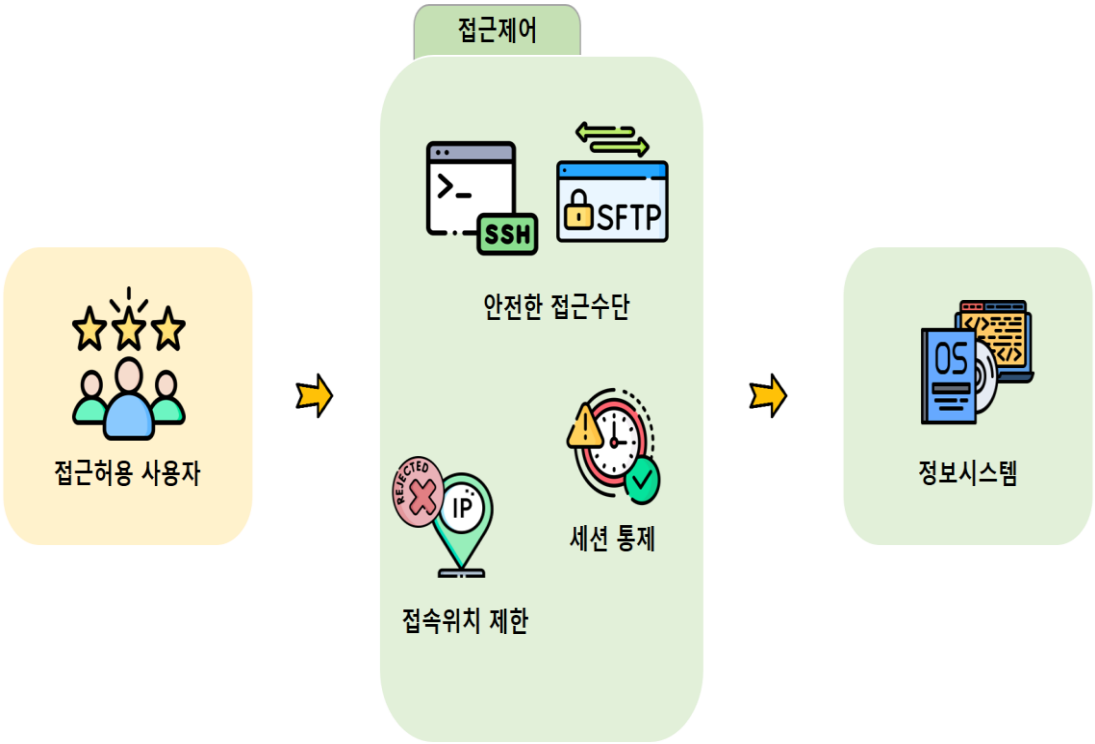
→ 안전한 접속 환경 구성

① 정보통신망을 이용해 외부망에 접근 시 안전한 통신수단(전용회신, VPN) 사용



※ 출처: 클라우드PC (SK 쉴더스)

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 일정시간 업무처리를 하지 않는 경우 자동으로 시스템 접속이 차단되도록 하고 있는가? • 정보시스템의 사용목적과 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?** **→ 정보시스템 접근통제 절차 수립(서버 예시)** 「**인증권한 관리지침**」 제 ○○조 (정보시스템 접근) ① 서버·네트워크시스템·보안시스템 등 정보시스템별 운영체제(OS)에 접근이 다음 각 호를 포함하여 통제해야한다. ≫ 계정 및 권한 신청·승인 절차

≫ 사용자별로 개별 계정 부여 및 공용 계정 사용 제한

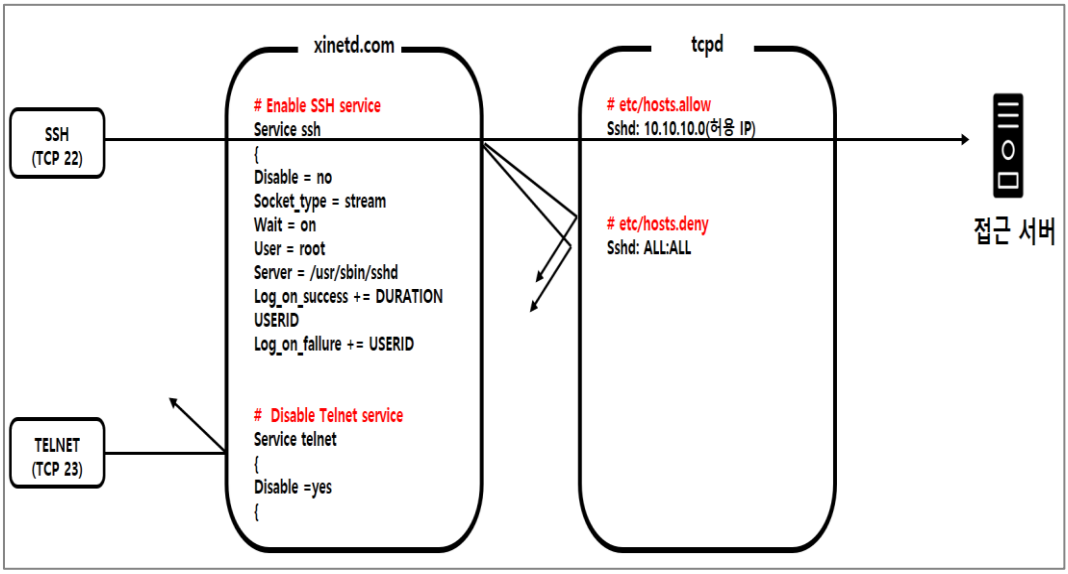
≫ 계정 사용 현황에 대한 정기 검토 및 현행화 관리

≫ 접속 위치 제한

≫ 관리자 등 특수권한에 대한 강화된 인증수단(인증서, OTP 등)

≫ 안전한 접근수단 적용(SFTP, SSH, SSL 등)

≫ 동일 네트워크 영역 내 서버 간 접속에 대한 접근통제 조치



※ 접근제어 설정 (이해를 돕기 위한 작성)

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

→ 정보시스템 세션 타임아웃 설정

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

OS별 점검 파일 위치 및 점검 방법	

SOLARIS, LINUX, AIX, HP-UX	<sh, ksh, bash 사용 시>
	#cat /etc/profile(.profile)
	TMOUT=600
	export TMOUT
	
	<csh 사용 시>
	#cat /etc/csh.login 또는, #cat /etc/csh.cshrc
	set autologout=10

위에 제시한 설정이 해당 파일에 적용되지 않은 경우 아래의 보안설정방법에 따라 설정을 변경함	

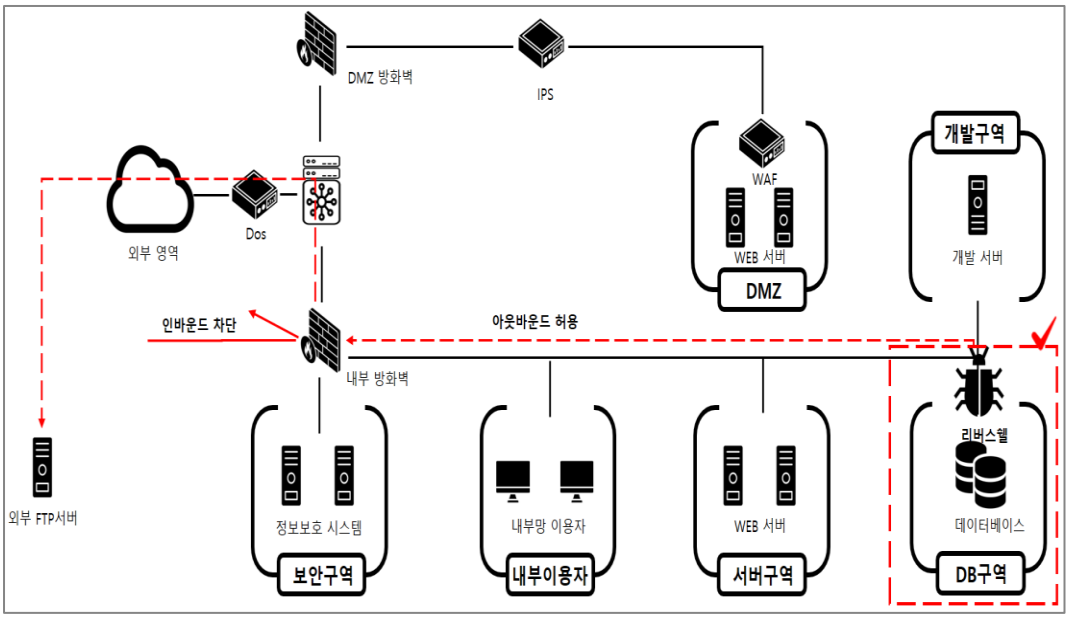
※ 출처: 주요통신기반시설 기술적 취약점 분석평가 방법 상세가이드 (과학기술정보통신부·KISA)

◇ 정보시스템의 사용목적과 관계없는 서비스를 제거하고 있는가?

→ 불필요한 서비스 또는 포트를 제거

② 안전하지 않은 서비스, 프로토콜, 데몬에 대해서는 추가 보안기능 구현

③ Netbios, File-Sharing, Telnet, FTP 등과 같은 안전하지 않은 서비스를 보호하기 위하여 SSH, SFTP, IPSec VPN 등과 같은 안전한 기술 사용



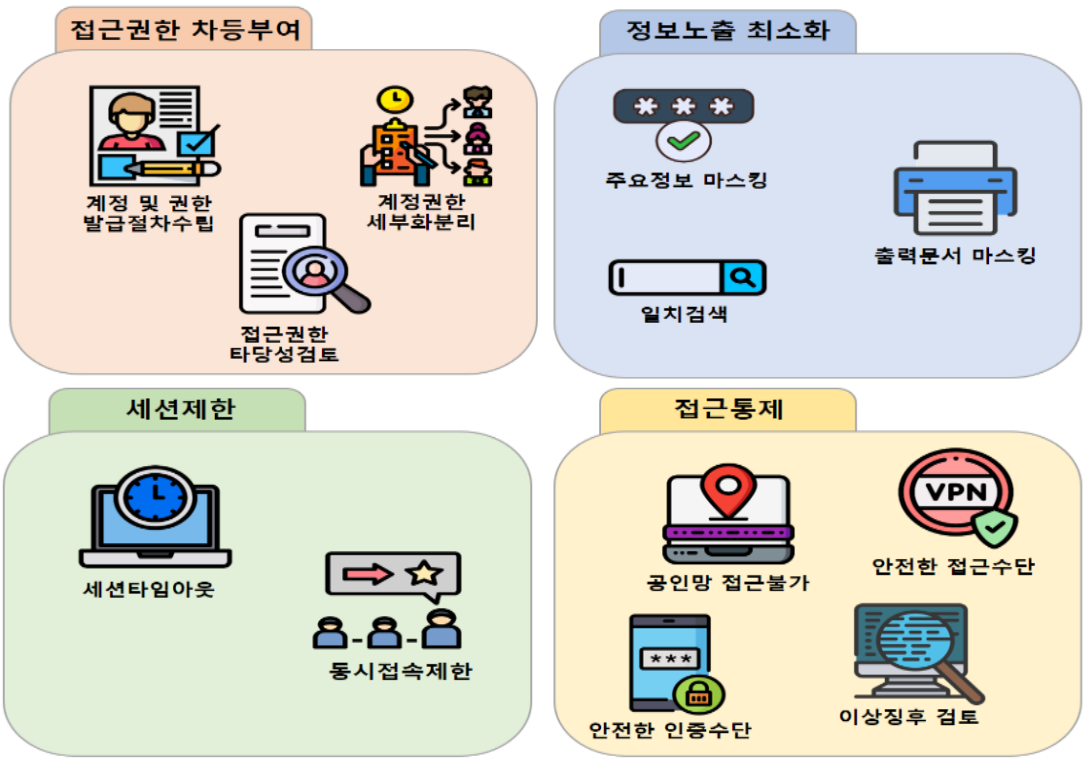
※ 불필요한 아웃바운드 서비스 오픈 (이해를 돕기 위한 예시))

◇ 주요 서비스를 제공하는 정보시스템은 독립된 서버로 운영하고 있는가?

→ 주요 서비스 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? • 중요정보의 불필요한 노출(조회, 화면표시, 인쇄, 다운로드 등)을 최소화할 수 있도록 응용프로그램을 구현하여 운영하고 있는가? • 일정시간 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?
기준 요약도	
운영 방안	**◇ 중요정보 접근을 통제하기 위하여 사용자의 업무에 따라 응용프로그램 접근권한을 차등 부여하고 있는가?** **→ 최소권한 원칙에 따라 접근권한 부여** **「인증권한 관리지침」** 제 ○○조 (정보시스템 접근)

① 응용프로그램에 대한 접근은 다음 각 호의 사항을 포함하여 중요정보의 접근을 통제하도록 응용프로그램을 구현 및 운영하여야 한다.

≫ 업무 목적 및 중요도에 따라 응용프로그램의 접근권한을 차등 부여

≫ 개인정보 등 중요정보를 처리(입력, 조회, 변경, 삭제, 다운로드, 출력 등) 시 접근권한을 세분화하여 설정

≫ 개인정보 등 중요정보의 불필요한 노출(조회, 화면표시, 인쇄, 다운로드 등) 최소화

≫ 개인정보 등 중요정보 출력(인쇄, 화면표시, 다운로드 등) 시 용도를 특정하고 용도에 따라 출력항목 최소화

≫ 개인정보 검색 시 과도한 정보가 조회되지 않도록 일치검색또는 두 가지 이상의 검색조건 사용

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

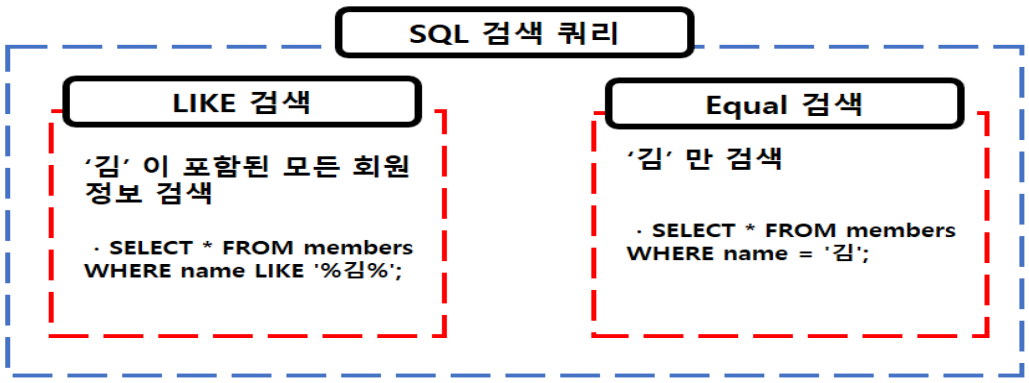
※ 권한 상세 부여현황(이해를 돕기 위한 예시)

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

→ 권한별 노출정보 최소화

① 응용프로그램(개인정보처리시스템 등)에서 개인정보 등 중요정보 출력 시(인쇄, 화면표시, 다운로드 등) 용도를 특정하고 용도에 따라 출력항목 최소화

② 개인정보 검색 시에는 과도한 정보가 조회되지 않도록 일치검색(equal검색)이나 두 가지 조건 이상의 검색조건 사용 등



※ SQL 검색쿼리 종류 (이해를 돕기 위한 예시)

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

→ 응용프로그램 세션 관리

① 응용프로그램 및 개인정보처리시스템 세션 타임아웃 설정

② 응용프로그램 및 개인정보처리시스템 세션 중복 통제

※ 출처: 세션타임아웃 (SK쉴더스)

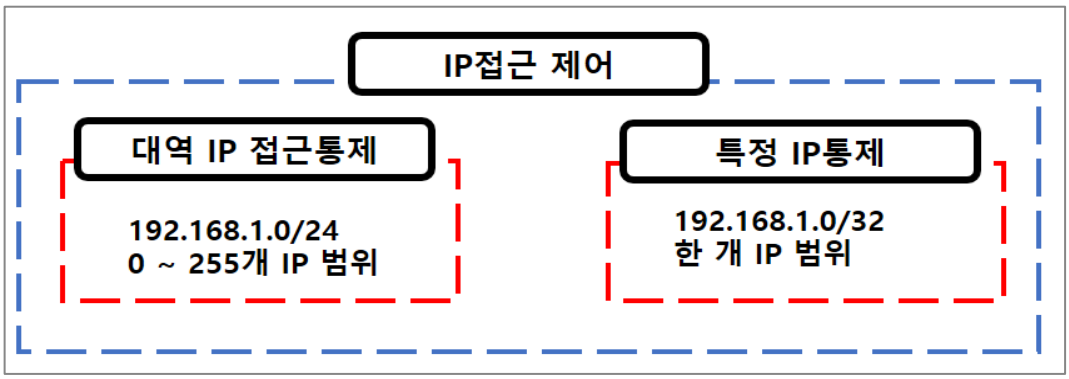
◇ 관리자 전용 응용프로그램(관리자 웹페이지, 관리콘솔 등)은 비인가자가 접근할 수 없도록 접근을 통제하고 있는가?

→ 관리자 전용 응용프로그램 접근통제

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

② 불가피하게 외부 공개가 필요한 경우 안전한 인증수단(OTP 등) 또는 안전한

	접속수단(VPN 등) 적용 ③ 관리자(사용자), 개인정보취급자의 접속 로그 및 이벤트 로그에 대한 정기적 모니터링 ④ 이상징후 발견 시 세부조사, 내부보고 등 사전에 정의된 절차에 따라 이행



※ IP 범위 설정 (이해를 돕기 위한 작성)

2.6.4 데이터베이스 접근

세부분야	2.6.4 데이터베이스 접근
인증 기준	테이블 목록 등 데이터베이스 내에서 저장·관리되고 있는 정보를 식별하고, 정보의 중요도와 응용프로그램 및 사용자 유형 등에 따른 접근통제 정책을 수립·이행하여야 한다.
주요 확인사항	• 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?
기준 요약도	
운영 방안	◇ 데이터베이스의 테이블 목록 등 저장·관리되고 있는 정보를 식별하고 있는가? → 데이터베이스 현황 정기적 현행화 ① 데이터 베이스 테이블 목록 및 컬럼 기록 변경 현행화

000 시스템 테이블 정의서

테이블 정의서		작성자		승인자	
		작성일		버전	
단계	설계	업무명		페이지	

순번	테이블명	테이블ID	컬럼명	컬럼ID	타입/길이	PK	FK	Null	비고

※ 테이블명세서(이해를 돕기 위한 예시)

◇ 데이터베이스 내 정보에 접근이 필요한 응용프로그램, 정보시스템(서버) 및 사용자를 명확히 식별하고 접근통제 정책에 따라 통제하고 있는가?

→ 데이터베이스 접근 권한 차등 부여

① 테이블, 뷰, 컬럼, 쿼리 등 사용명령어 권한 차등 부여

② 지정된 IP접근 설정을 통해 비인가 접근제한 (IP통제, 접근제어 솔루션 적용)

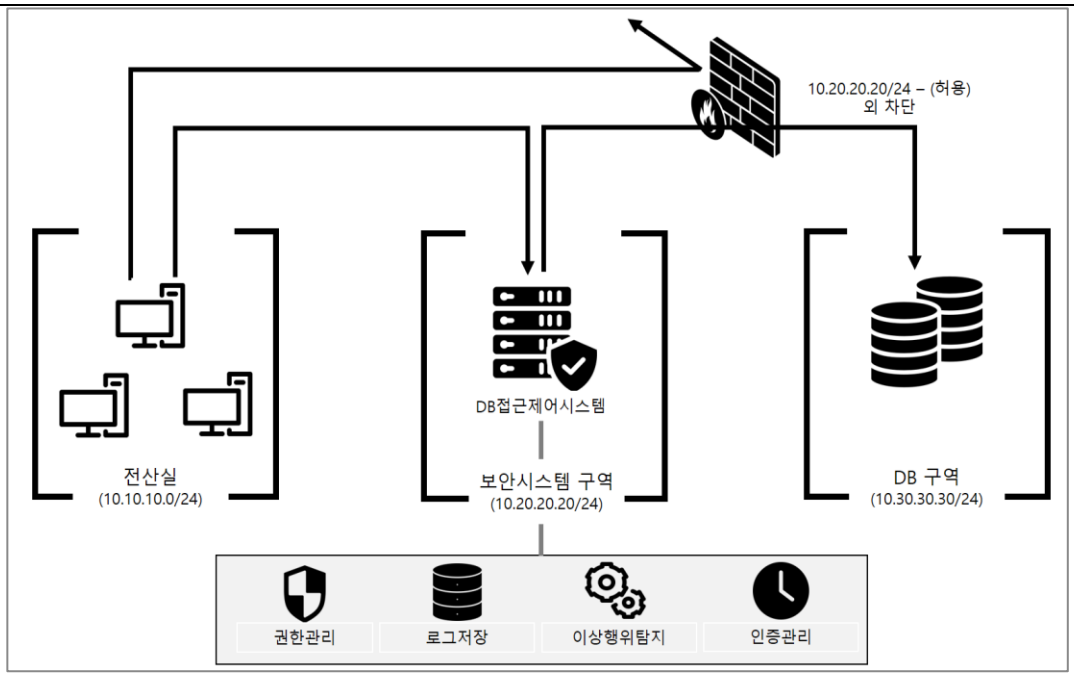
권한 명령어	설명	예시
SELECT	SELECT 권한 부여	GRANT SELECT ON mydatabase.mytable TO '권한 부여 ID';
INSERT	INSERT 권한 부여	GRANT INSERT ON mydatabase.mytable TO '권한 부여 ID';
UPDATE	UPDATE 권한 부여	GRANT UPDATE ON mydatabase.mytable TO '권한 부여 ID';
DELETE	DELETE 권한 부여	GRANT DELETE ON mydatabase.mytable TO '권한 부여 ID';
ALL PRIVILEGES	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

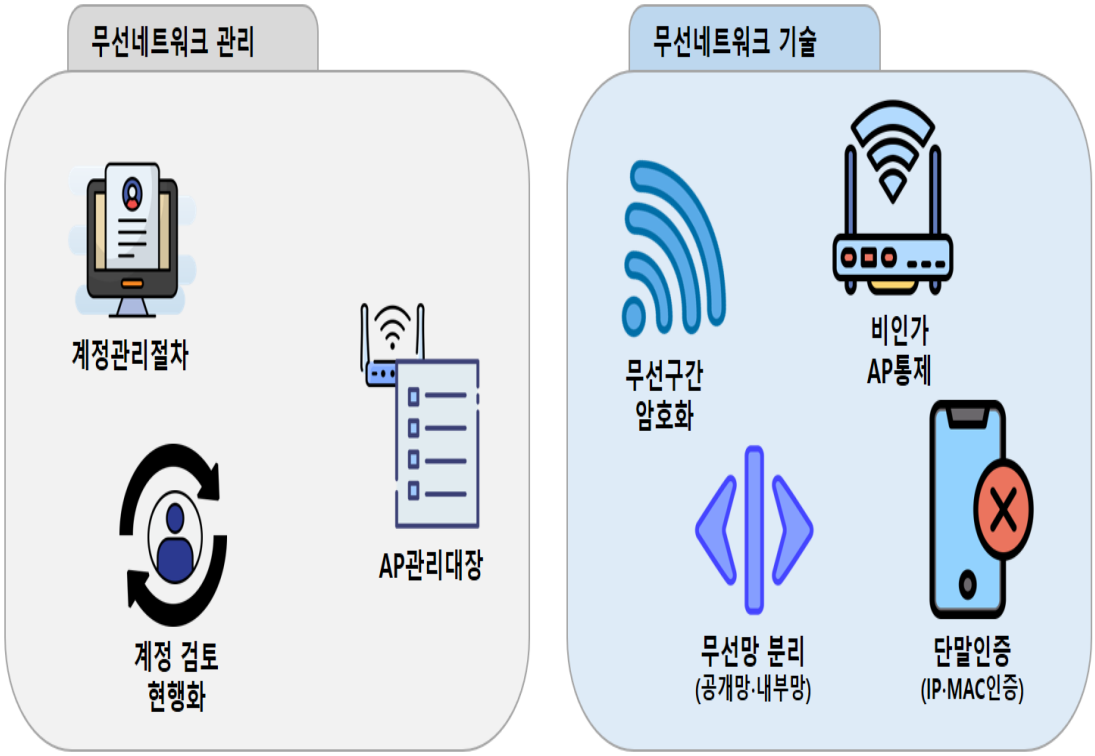
① 비인가자 접근제어

② 우회접속차단



※ 데이터베이스 접근제어시스템(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 보호대책을 적용하여야 한다. 또한 AD Hoc 접속, 비인가 AP 사용 등 비인가 무선 네트워크 접속으로부터 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 무선네트워크를 업무적으로 사용하는 경우 무선 AP 및 네트워크 구간 보안을 위하여 인증, 송수신 데이터 암호화 등 보호대책을 수립·이행하고 있는가? • 인가된 임직원만이 무선네트워크를 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 무선네트워크에 대한 보호대책을 수립·이행하고 있는가?
기준 요약도	
운영 방안	**◇ 무선네트워크를 업무적으로 사용하는 경우 무선 AP 및 네트워크 구간 보안을 위하여 인증, 송수신 데이터 암호화 등 보호대책을 수립·이행하고 있는가?** **→ 무선 네트워크 보호대책 수립** **「정보시스템 운영관리지침」** 제 ○○조 (AP관리) ① 무선랜 사용하여 업무자료를 전송하는 경우 각 호에 해당하는 보호 대책을

수립해야 한다.

≫ 네트워크 이름(SSID, Service Set Identifier) 브로드캐스팅 중지

≫ 추측이 어려운 복잡한 SSID 사용

≫ WPA2 이상(256비트 이상)의 암호체계를 사용하여 소통자료 암호화

•(예시) AP가 제공하는 WEP 키 중 128bit 이상의 키를 사용하도록 하고 WEP키를 주기적으로 변경하거나 Dynamic WEP Key 혹은 TKIP 등을 사용하여 데이터 암호화를 실시한다.

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

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

② 무선랜 및 AP 사용하고자 하는 경우 무선LAN 설치 의뢰서를 작성하여 네트워크 담당자에게 하고, 네트워크 담당자는 무선 랜/AP 사용대장에 기록·관리한다.

무선 AP 관리대장

운영담당자	운영책임자

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

※ 무선AP관리대장(이해를 돕기 위한 예시)

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

→ 사용 신청 및 해지 절차 수립

① 무선네트워크 사용권한 신청 및 승인 절차(사용자 및 접속단말 등록 등)

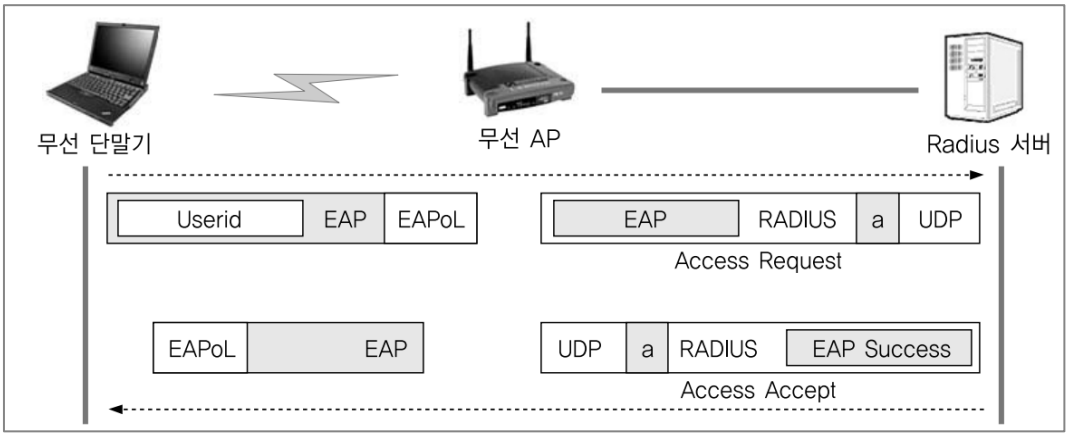
② 퇴직, 기간 만료 등의 사유로 무선네트워크 사용이 필요하지 않은 경우 접근권한 해지 절차

③ 외부인에게 제공하는 무선네트워크는 임직원이 사용하는 무선네트워크와 분리

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

→ **무선 단말 인증 (Remote Authentication Dial-In User Service)**

① RADIUS 서버 운영은 무선 AP에 참여할 수 있는 사용자에 대한 정보를 별도로 관리하여 허가받은 사용자에게만 무선랜의 사용을 허용



※ 출처: 금융부분 무선랜 보안가이드(KISA)

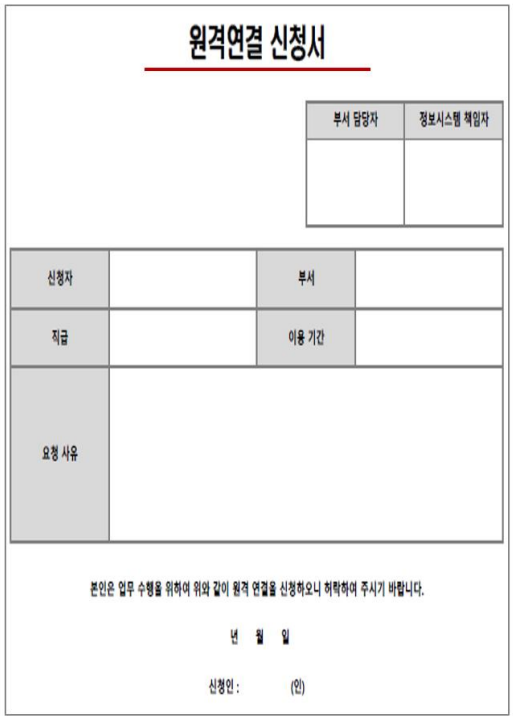
2.6.6 원격접근 통제

세부분야	2.6.6 원격접근 통제
인증 기준	보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지하고, 재택근무·장애대응·원격협업 등 불가피한 사유로 원격접근을 허용하는 경우 책임자 승인, 접근 단말 지정, 접근 허용범위 및 기간 설정, 강화된 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 인터넷과 같은 외부 네트워크를 통한 정보시스템 원격운영은 원칙적으로 금지하고 장애대응 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 원격업무 수행 시 중요정보 유출, 해킹 등 침해사고 예방을 위한 보호대책을 수립·이행하고 있는가? • 개인정보처리시스템의 관리, 운영, 개발, 보안 등을 목적으로 원격으로 개인정보처리시스템에 직접 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 장애대응 등 부득이하게 허용하는 경우 보완대책을 마련하고 있는가? → 외부 네트워크를 통한 접근 시 보호 대책

「**정보시스템 운영관리 지침**」 제 ○○조 (외부네트워크 통제)

① 외부에서 원격으로 정보시스템을 유지보수 하는 것을 원칙적으로 금지하여야 하며 부득이한 경우에는 '원격연결 요청서'를 작성하여 정보시스템책임자의 승인을 득한후 일시적인 원격접속을 허용한다.

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



원격연결 신청서

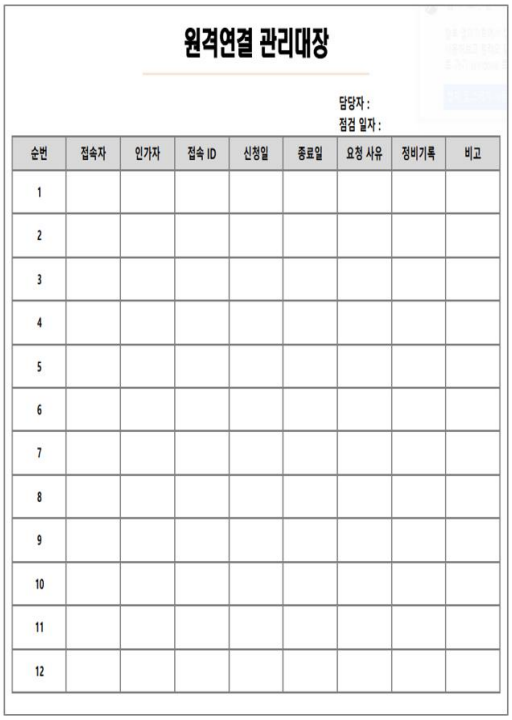
부서 담당자	정보시스템 책임자

신청자		부서	
직급		이용 기간	
요청 사유			

본인은 업무 수행을 위하여 위와 같이 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								

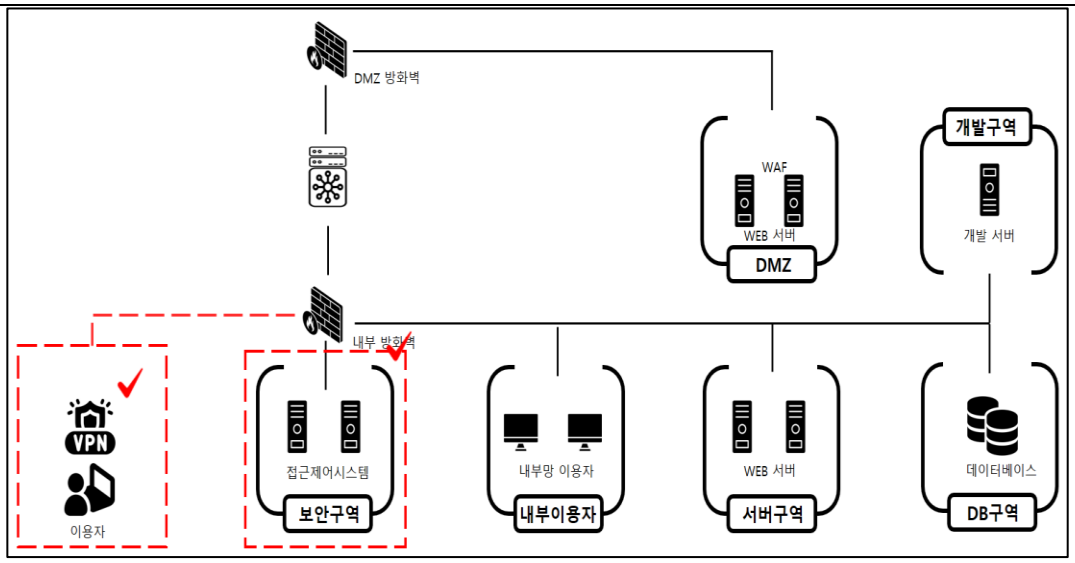
※ 원격연결 신청서(이해를 돕기위한 예시)

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

→ 원격 시스템 우회 접속 차단 필요

① 접속 가능한 단말을 IP주소, MAC주소 등으로 제한

② 정상적인 원격접속 경로를 우회한 접속경로 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 보호대책을 수립·이행하고 있는가?

→ 재택근무, 원격협업, 스마트워크 등 보호대책을 수립·이행 (예시)

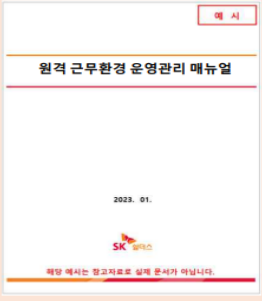
「**정보시스템 운영관리 지침**」 제 ○○조 (원격근무 보안관리)

① 원격 근무를 지원하기 위한 정보시스템을 도입·운영할 경우 기술적·관리적·물리적 보안대책을 수립하여 시행하여야 한다

≫ 주기적인 원격근무 보안점검을 수행하여 원격근무 보호대책 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**

담당	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?	
		가족, 손님 등 타인의 원격근무 단말기 사용이 불가능한 상태인가?	
	단말기설치 프로그램	원격근무용 단말기에 원격근무자가 임의로 신규 프로그램을 설치하는 것이 불가능한 상태인가?	
		원격근무자가 직원 간 대화에 사내 메신저만을 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 외부미디어	데이터 복사/전송을 위한 USB 외부 저장장치 사용을 제한하고 있는가?	
		제한적 USB 외부 저장장치 사용시, USB 자동 실행 방지 및 자동 바이러스 검사를 시행하고 있는가?	
		원격근무용 단말기의 USB 포트는 읽기 전용으로만 사용하고 있는가?	
		구글 드라이브, iCloud 등 상용 클라우드에 업무 자료 저장을 금지하고 있는가?	
	네트워크	원격근무 시 개방형 Wi-Fi를 사용한 사내망에 접속을 제한하고 있는가?	
		홈 네트워크 사용 시 공유기의 관리자 계정/암호를 안전하게 설정했는가?	
		홈 네트워크에 허가된 사용자만 접속할 수 있게 보안정책을 적용하는가?	
		무선 접속시 암호화방식은 WPA2 이상을 사용하고 있는가?	
		회사가 제공하는 안전한 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 보안상태(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 연결자원 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?	
		민감한 서버 로그인/관리자 계정에 다중 인증(MFA, multi-factor authentication)을 적용하고 있는가?	
		사용자 이상징후 탐지를 위해 사용자 접속 이력, 접속 출발지 등을 지속적으로 모니터링하고 있는가?	
	기업망 모니터링 강화	SIEM 운영 등을 이용하여 기업 전산시스템 시스템 로그를 상시 모니터링하여 외부 위협 탐지를 시행하고 있는가?	
		원격근무 사용자 전용 네트워크 주소를 할당하고 있는가?	
		백신 설치, 최신 보안 업데이트, 내부 자원 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 개인정보처리 시스템에 직접 접속하는 단말기는 관리용 단말기로 지정하고 임의조작 및 목적 외 사용 금지 등 안전조치를 적용하고 있는가?

→ 원격으로 개인정보처리시스템에 직접 접속하는 단말기 보호대책 구현

① 정보보호최고책임자(CISO) 역할

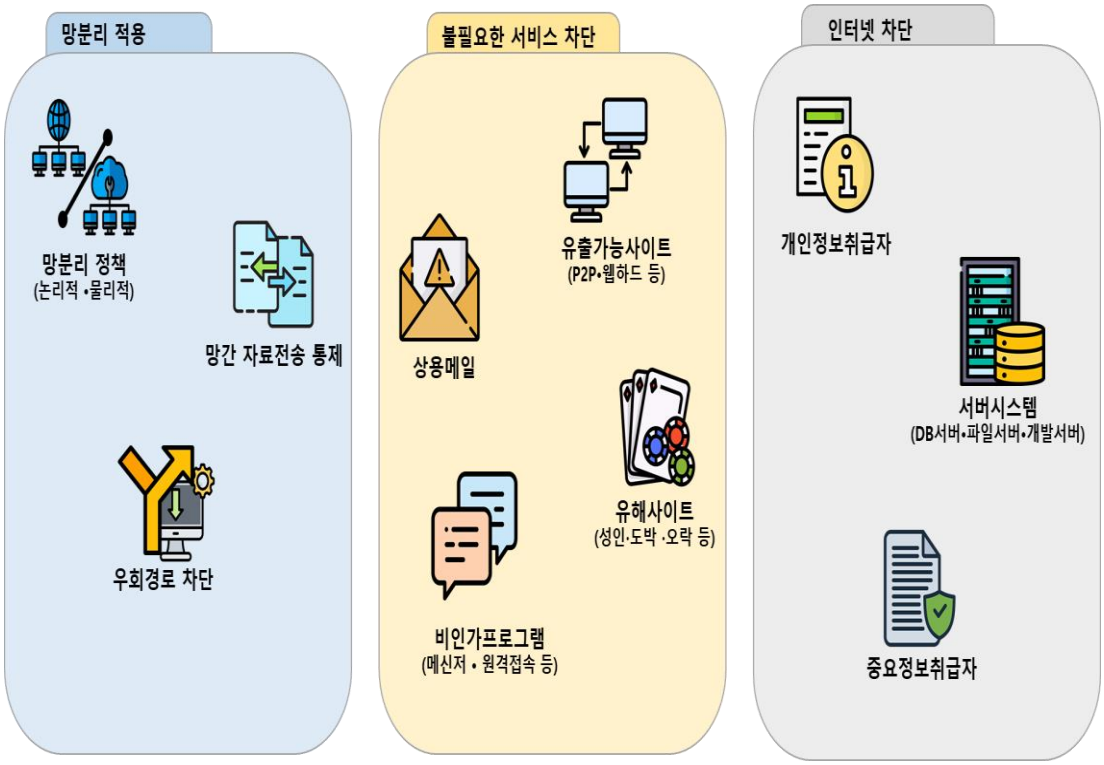
≫ 인가받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치

≫ 등록된 관리용 단말기 이외에는 접근하지 못하도록 조치

≫ 본래 목적 외로 사용되지 않도록 조치

≫ 관리용 단말기에 악성프로그램 감염 방지 등을 위한 보호조치 적용

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 통제정책을 수립·이행하고 있는가? • 주요 정보시스템(데이터베이스 서버 등)에서 불필요한 외부 인터넷 접속을 통제하고 있는가? • 관련 법령에 따라 인터넷 망분리 의무가 부과된 경우 망분리 대상자를 식별하여 안전한 방식으로 망분리를 적용하고 있는가?
기준 요약도	
운영 방안	**◇ 주요 직무 수행 및 개인정보 취급 단말기 등 업무용 PC의 인터넷 접속에 대한 통제정책을 수립·이행하고 있는가?** **→ 인터넷 접속 통제 정책 수립** **「정보시스템 운영관리 지침」** 제 ○○조 (인터넷 사용 보안) ① 정상적인 업무 활동을 위해 인터넷 상의 특정 사이트 접속 차단하며, 차단사이트 유형은 각 호와 같이 규정한다.

≫ 불건전 음란 정보를 포함하는 사이트

≫ 사이버 주식, 게임, 도박, 음란사이트

≫ 그 밖에 접속 시 정보유출이 우려되는 사이트

→ 망분리 관리 정책 수립

「정보시스템 운영관리 지침」 제 ○○조 (망간 자료전송)

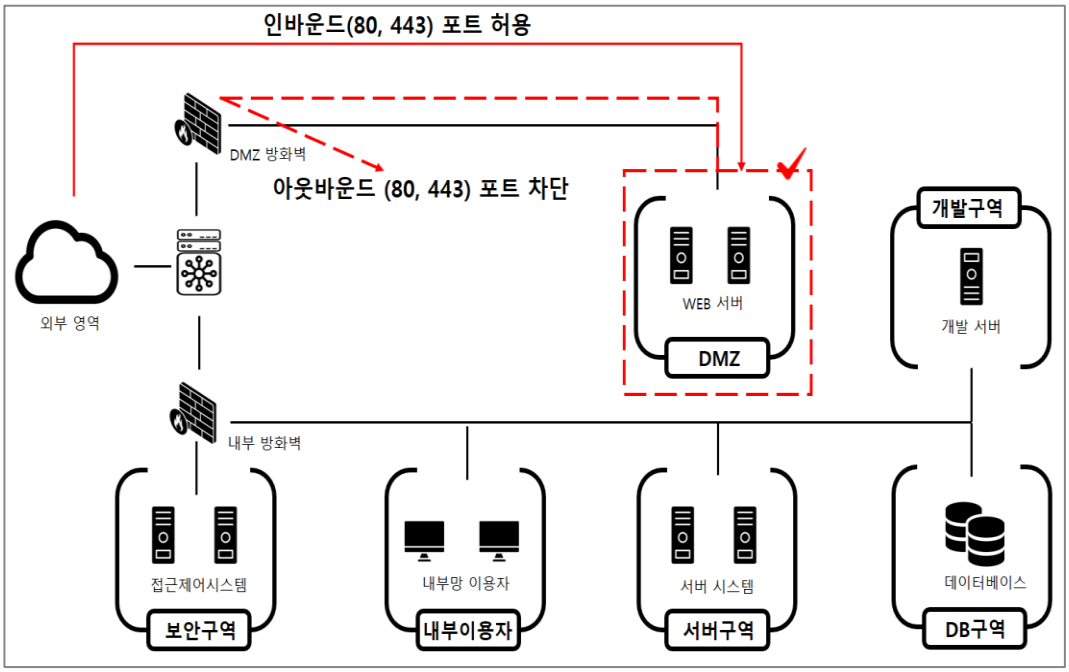
① 업무망 PC의 자료를 인터넷 PC로 전송 시에는 부서 정보보호담당자 또는 지정된 승인권자의 승인을 득한 후 자료를 전송해야한다.

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

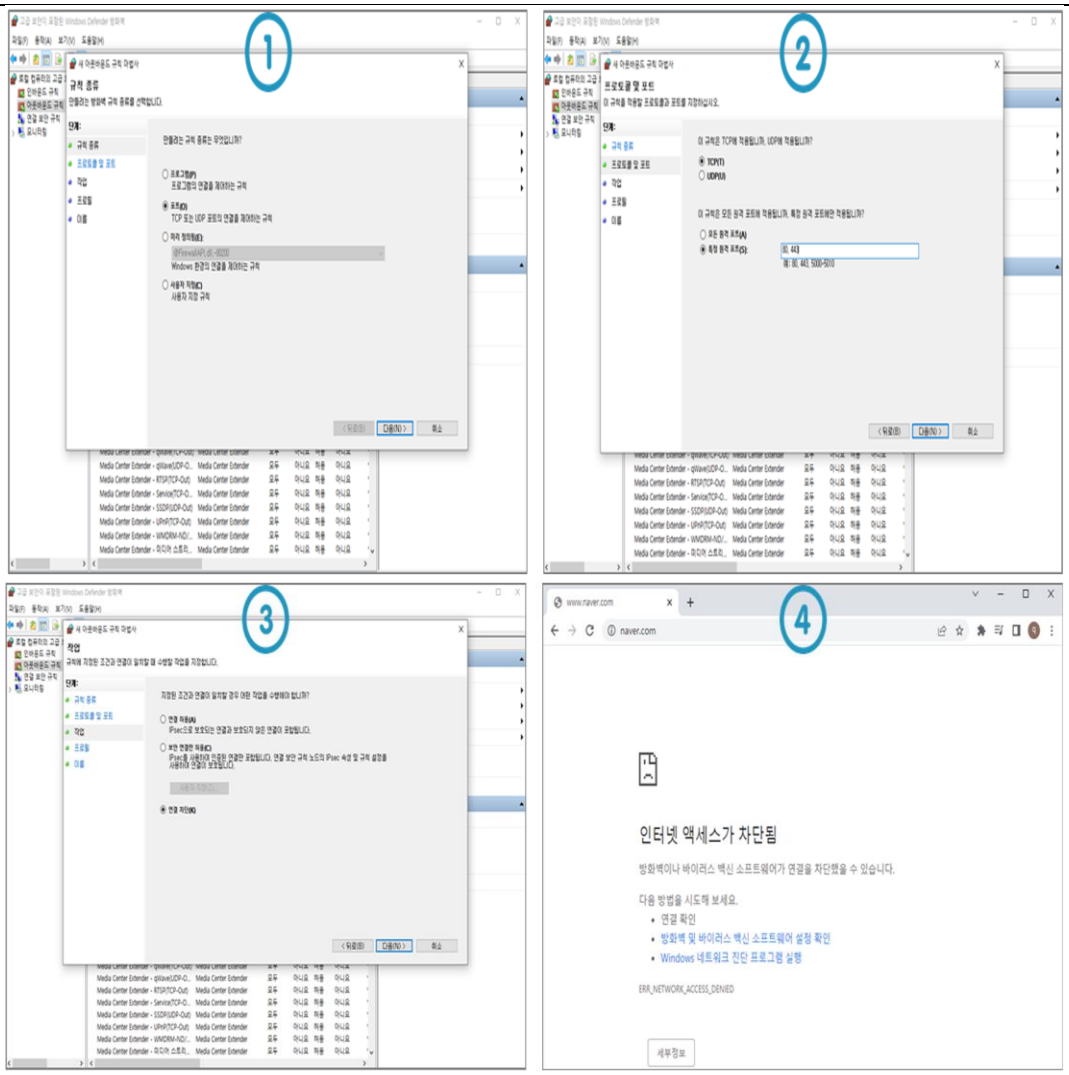
→ 주요 정보시스템 외부 인터넷 차단

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

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



※ 윈도우서버 80, 443 port 차단 (이해를 돕기 위한 예시)



※ 윈도우서버 80, 443 port 차단(이해를 돕기 위한 예시)

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

→ 망분리 대상

「개인정보의 기술적·관리적 보호조치 기준」제4조 (접근통제)

① 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자수가 일일평균 100만명 이상이거나, 정보통신서비스 부문 전년도(법인인 경우에는 전사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자 등

적용 대상
전년도말 기준 직전 3개월간 개인정보가 저장·관리되고 있는 이용자수가 일일평균 100만명 이상 ※ 일일평균 이용자수 = 일일 보유량(10, 11, 12월)의 총합 / 92(일수)
또는 정보통신서비스 부문 전년도(전 사업년도) 매출액이 100억원 이상

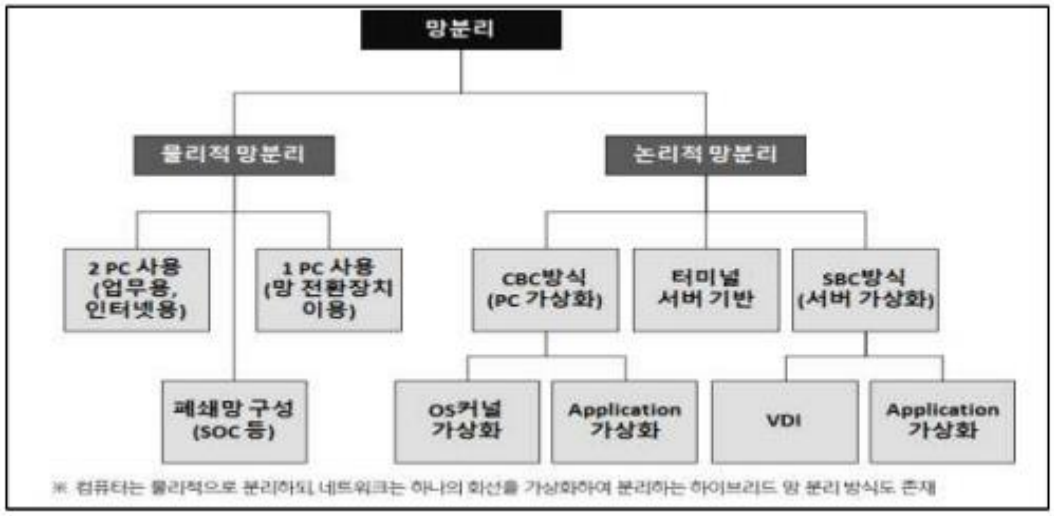
※ 출처: 개인정보 기술적 관리적 보호조치 (개인정보보호위원회•KISA)

→ 망분리 적용 대상

① 개인정보처리시스템에서 개인정보를 다운로드할 수 있는 컴퓨터 등

② 개인정보처리시스템에서 개인정보를 파기할 수 있는 개인정보취급자의 컴퓨터 등

③ 개인정보처리시스템에 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등



※ 출처: 개인정보 기술적 관리적 보호조치 (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, 암호강도, 암호사용 등이 포함된 암호정책을 수립하고 있는가? • 암호정책에 따라 개인정보 및 중요 정보의 저장, 전송, 전달 시 암호화를 수행하고 있는가?
기준 요약도	
운영 방안	**◇ 개인정보 및 주요정보의 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호강도, 암호사용 등이 포함된 암호정책을 수립하고 있는가?** **→ 암호화 정책 수립** 「**암호관리 매뉴얼**」 제 ○○조 (암호화 기술 선택 기준) ① 데이터 암호화 시에는 법적 요구사항 등을 고려한 안전한 암호화알고리즘 및 보안강도를 선택하여야 한다. 시스템 관리 및 기술적 한계 등으로 적용이 불가능한 경우 정보보호책임자의 승인을 받아 예외로 할 수 있다.

≫ 대칭키 암호 알고리즘: SEED, ARIA-128/192/256, AES-128/192/256, HIGHT, LEA

≫ 공개키 암호 알고리즘: RSAES-OAEP, RSAES-PKCS1

≫ 일방향 암호 알고리즘: SHA-256/384/512

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

→ 개인정보 및 중요정보의 저장, 전송, 전달 시 암호화

「**암호관리 매뉴얼**」 제0조 (암호화 기술 적용 대상)

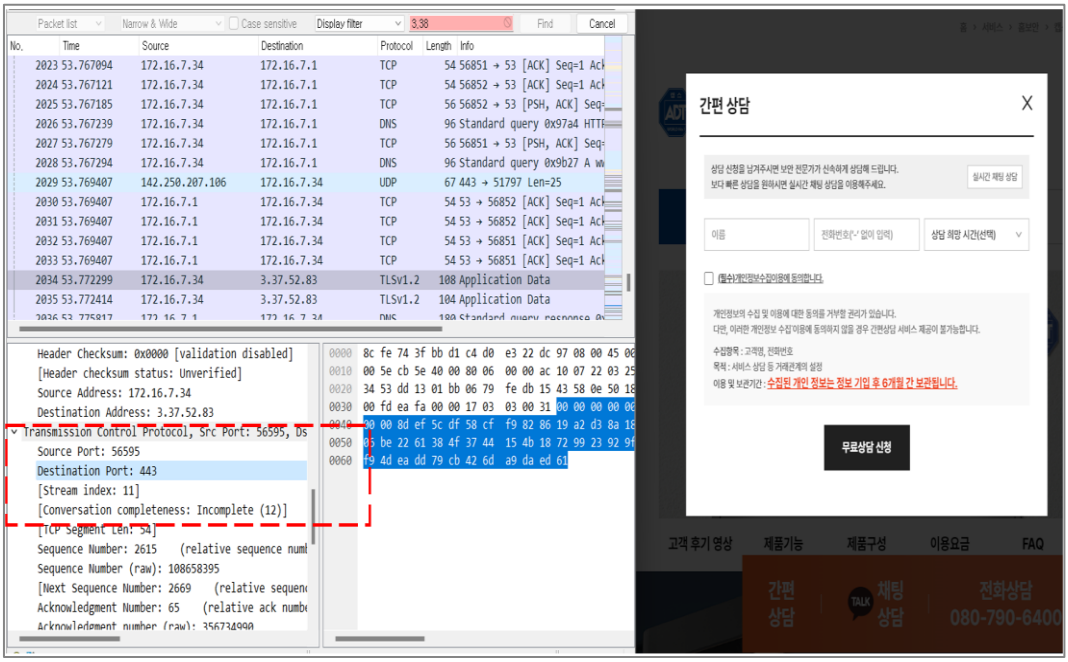
① 이용자 데이터의 무결성을 보장하기 위해 개인정보 및 중요정보의 저장, 전송, 전달 시 암호화를 수행하여야 한다.

≫ 정보통신망을 통한전송

≫ 보조저장매체로 전달

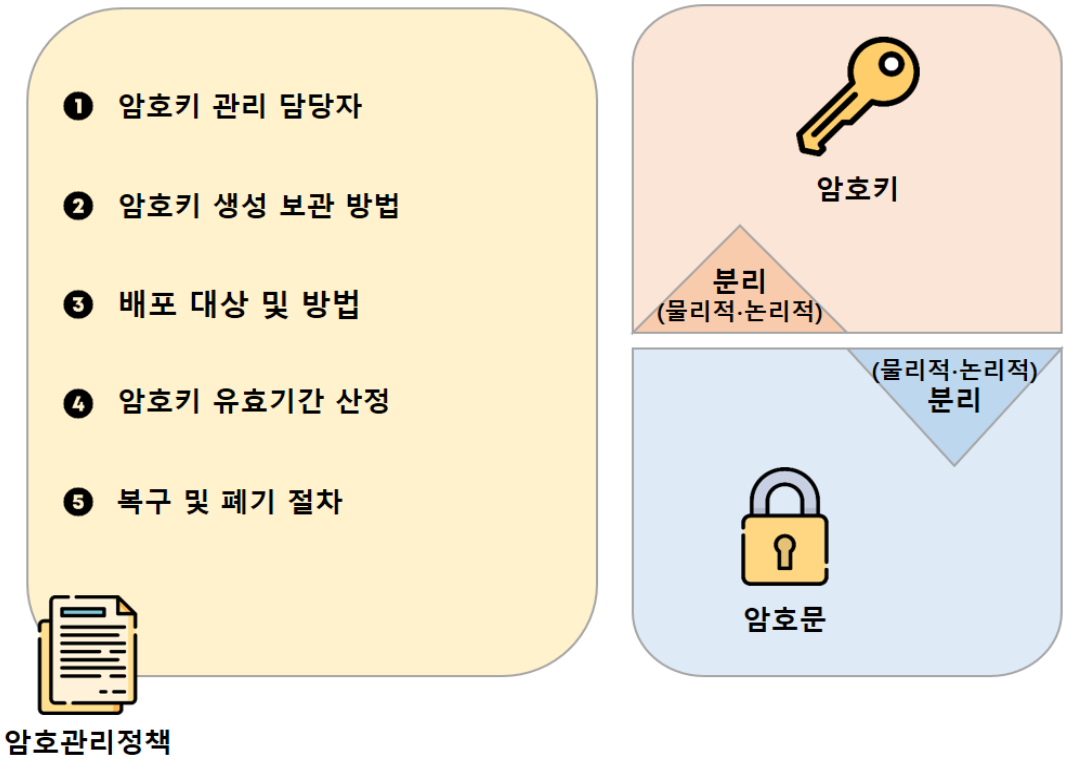
≫ 개인정보처리시스템 저장

≫ 업무용 컴퓨터 및 모바일 기기 저장



※ 중요 개인정보 전송구간 암호화 (이해를 돕기 위한 예시)

2.7.2 암호키 관리

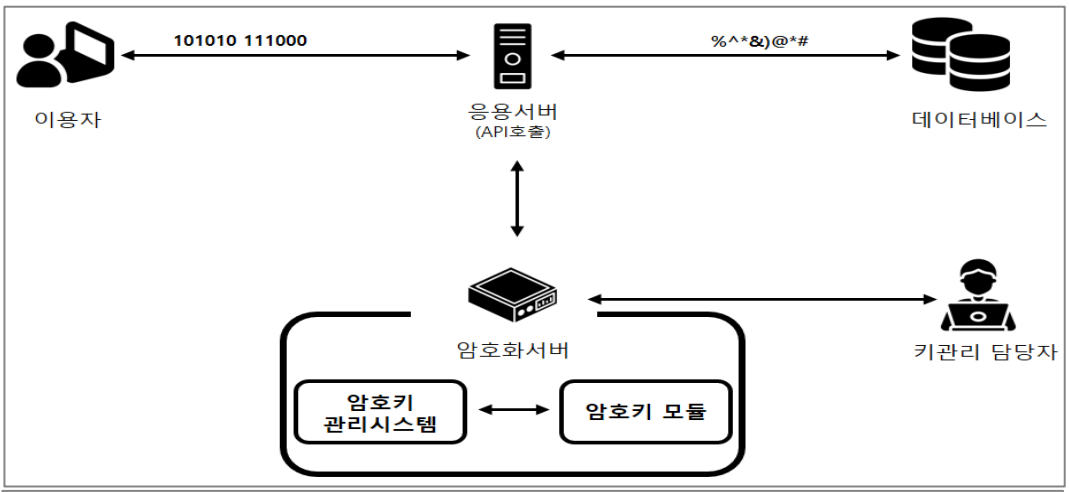
<table>
<tr><th>세부분야</th><th>2.7.2 암호키 관리</th></tr>
<tr><td>인증
기준</td><td>암호키의 안전한 생성·이용·보관·배포·파기를 위한 관리 절차를 수립·이행하고, 필요시 복구방안을 마련하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 암호키 생성, 이용, 보관, 배포, 변경, 복구, 파기 등에 관한 절차를 수립·이행하고 있는가?
• 암호키는 필요시 복구가 가능하도록 별도의 안전한 장소에 보관하고 암호키 사용에 관한 접근권한을 최소화하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 암호키 생성, 이용, 보관, 배포, 변경, 복구, 파기 등에 관한 절차를 수립·이행하고 있는가?

→ 암호키 관리 절차 수립 (예시)

「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.</td></tr>
</table>

③ 암호화 키는 노출 위협을 최소화하기 위해 1 년마다 변경해야 한다. 단 정보보호책임자가 암호화 키 변경이 필요 하다고 판단될 경우 변경할 수 있다.

④ 암호화 키는 사용 용도가 종료되거나 사용 주기가 만료된 경우 폐기한다. 암호화 키는 부서 정보보호 담당자가 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)

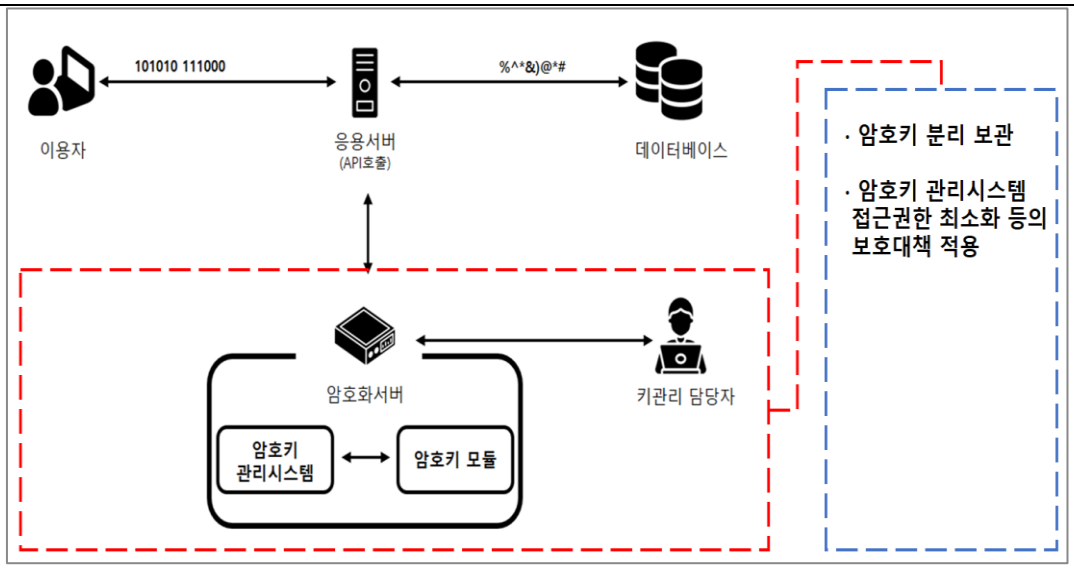
◇ 암호키는 필요시 복구가 가능하도록 별도의 안전한 장소에 보관하고 암호키 사용에 관한 접근권한을 최소화하고 있는가?

→ 암호키 접근 제어

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

≫ 암호키 손상 시 시스템 또는 암호화된 정보의 복구를 위하여 암호키는 별도의 매체에 저장한 후 안전한 장소에 보관(암호키 관리시스템, 물리적 분리된 곳 등)

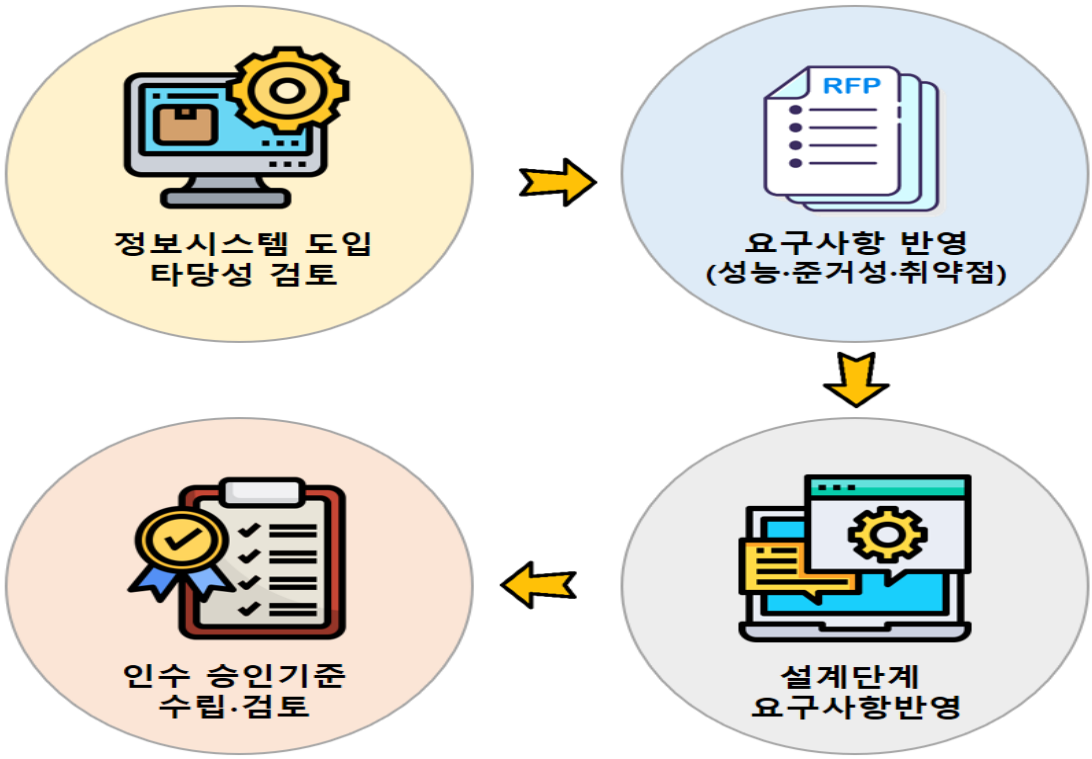
≫ 암호키에 대한 접근권한 최소화 및 접근 모니터링



※ 암호 키 분리보관 및 보호대책 구현 (이해를 돕기 위한 예시)

2.8 정보시스템 도입 및 개발 보안

2.8.1 보안 요구사항 정의

<table>
<tr><th>세부분야</th><th>2.8.1 보안 요구사항 정의</th></tr>
<tr><td>인증
기준</td><td>정보시스템의 도입·개발·변경 시 정보보호 및 개인정보보호 관련 법적 요구사항, 최신 보안취약점, 안전한 코딩방법 등 보안 요구사항을 정의하고 적용하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 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?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 정보시스템을 신규로 도입·개발 또는 변경하는 경우 정보보호 및 개인정보보호 측면의 타당성 검토 및 인수 절차를 수립·이행하고 있는가?

→ 보안요구사항 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 도입계획 수립
≫ 현재 시스템 자원의 이용률, 사용량, 능력한계에 대한 분석
≫ 성능, 안정성, 보안성, 신뢰성 및 기존시스템과의 호환성, 상호 운용성 요건</td></tr>
</table>

≫ 개인정보처리시스템에 해당될 경우 개인정보 보호법(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

≫ 도입계획 수립 시 정의된 성능, 보안성, 법적 요구사항 등을 반영한 인수 승인기준 수립

≫ 시스템 도입 과정에서 인수기준을 준수하도록 구매계약서 등에 반영

목표시스템과 관련된 정보보호 유관 법령 및 유관기관 정보보호 규정을 조사하여 목록화하고 관련 규정을 비교 매핑하도록 한다. 예를 들어, 정보통신 관련 서비스를 구축하는 경우, "정보통신 이용촉진 및 정보보호 등에 관한 법(동법 시행령 및 시행규칙)에서 정한 내용을 조사한다. 또한, 결제시스템에 연계되거나 금융 서비스를 제공하는 경우는 금융감독위원회에서 정한 규정 등을 조사·분석하여야 한다.

서비스를 구축할 경우 검토되어야 하는 법령 및 규정은 다음과 같으며, 서비스 업무담당자로부터 반드시 확인을 받고 정리하여야 한다.

No.	구분	관련 법령 및 규정	시행일자	비고
1	법령	개인정보 보호법	2017.7.26.	공통
2	법령	개인정보 보호법 시행령	2017.7.26.	공통
3	법령	개인정보 보호법 시행규칙	2017.7.26.	공통
4	행정규칙	개인정보의 안전성 확보조치 기준	2017.7.26.	공통
5	행정규칙	개인정보의 기술적·관리적 보호조치 기준	2015.5.19.	정보통신
6	행정규칙	표준개인정보보호지침	2017.7.26.	공통
7	법령	전자금융거래법	2017.7.26.	금융
8	법령	전자금융거래법(개정)	2017.10.19.	금융
9	법령	전자금융거래법 시행령	2017.7.26.	금융

1. 구축 사업자 평가지표

구분	평가 지표	배점
제안사 평가 (20점)	조직체계 및 구성원 현황	10점
	사업(용역) 및 제안사의 이해에 대한 이해도	10점
수행능력 평가 (30점)	사업 운영 및 참여인력의 전문성	10점
	사업 추진 일정의 적정성	10점
	구체적인 과제 수행 방법론 제시 여부	10점
사업관리 능력 평가 (25점)	제안사의 사업 운영 기획성	15점
	제안사의 사업 수행 및 관리 능력	10점
정보보안 평가 (20점)	목표시스템 보안기능 구현 정도	10점
	개발환경 보안관리	10점
기타 (5점)	사후 지원 계획	3점
	기타 지원사항의 실효성	2점
합계		100점

1. 정보보호 사전점검 추진일정

개발 단계			2017년 2월	3월	4월	5월	6월	7월	8월	9월
요구사항 정의	계획 수립	수행계획 수립								
		구축 사업자 평가(정보보호 영역)								
	요구사항 정의	관련 법령 및 규정 분석								
		정보보호 위험평가								
		정보보호 요구사항 정의								
	교육 실시	정보보호 교육 계획 수립 및 이행								
	정책 수립	개발환경 보안정책 수립								
		운영환경 보안정책 수립								
		시큐어코딩 정책 수립								
설계	보안설계	목표시스템 보안설계								
		목표시스템 보안기능 설계								
	개발보안	개발환경 보안설계								
구현	보안기능 구현	침입차단 시스템 구축	구축 일정계획 수립							
			시스템 구축							
			보안기능 구현 검토							
		DB 접근제어 시스템 구축	구축 일정계획 수립							
			시스템 구축							
			보안기능 구현 검토							
		저장매체 시스템 구축	구축 일정계획 수립							
			시스템 구축							
			보안기능 구현 검토							
		소스코드 보안점검								
	개발환경 관리	개발환경 보안점검								
		개발환경 취약점 진단								
테스트	보안점검	관리적 물리적 보안점검 수행								
		정밀 취약점 진단								
		모의해킹								
	이관	시스템 이관								
종료		산출물 검토								

※ 출처: 정보보호사전점검해설서 (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 설계단계에서 보안요구사항 반영

① 구조적인 보안설계를 위한 작업설계단계에서 구조적인 보안설계

1. 서비스 명

OOO 서비스

2. 구축 완료 예정일(오픈일)

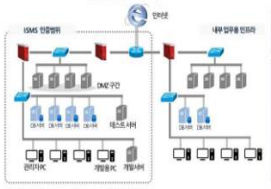
2017년 12월 31일

3. 구축 추진 일정

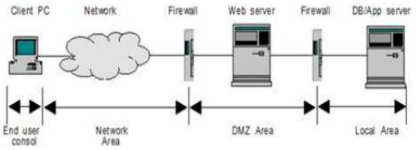
구축 단계	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	비고
분석													
설계													
구현													
테스트													
이관													

4. 네트워크 및 시스템 구성도

네트워크 구성도



시스템/소프트웨어 구성도



5.1 정보보호 관리

5.2 접근통제

5.3 인증

5.4 네트워크 보안

5.5 시스템 보안

5.6 장애 및 재해복구

5.7 물리적 보안

5. 보호대책

구축하고자하는 시스템을 보호하기 위한 정보보호 대책을 간략하게 정리한다.

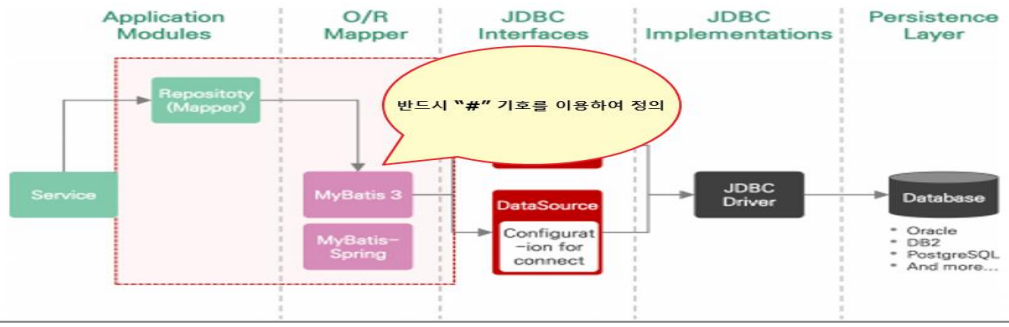
※ 출처: 정보보호사전점검해설서 (KISA)

◇ 정보시스템의 안전한 구현을 위한 코딩 표준을 수립하여 적용하고 있는가?

→ 개발단계에서 부터 안전한 코딩 표준 적용

① 구조적인 보안설계를 위한 작업설계단계에서 구조적인 보안설계

요구사항ID	SR-010102
요구사항 내용	
동적으로 SQL문이 생성, 실행되지 않도록 해야 한다.	
구현방안	
SQL 삽입 취약점을 방어할 수 있도록 외부 또는 사용자 입력값을 MyBatis의 쿼리맵에 바인딩하는 경우, 반드시 "#" 기호를 이용하여 정의하도록 한다. 만약, "$" 기호를 사용하는 경우에는 파라미터로 전달되는 값이 해당 애플리케이션에서 정의한 상수 또는 고정된 값인 것을 보장해야 한다.	




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

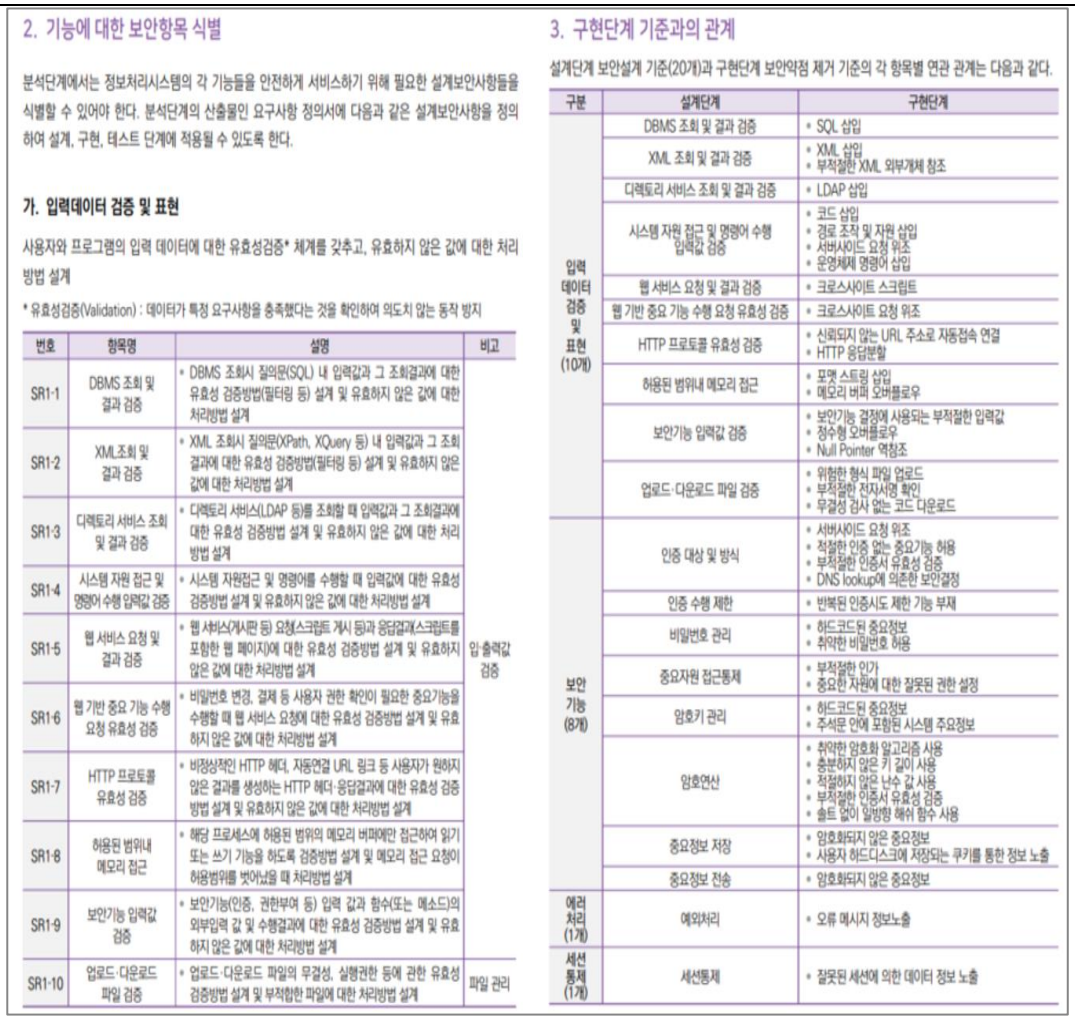
※ 출처: 소프트웨어 보안약점 진단가이드 (행정안전부·KISA)

2.8.2 보안 요구사항 검토 및 시험

<table>
<tr><th>세부분야</th><th>2.8.2 보안 요구사항 검토 및 시험</th></tr>
<tr><td>인증
기준</td><td>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 개선조치를 수행하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 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 개선계획 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?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 정보시스템의 도입, 개발, 변경 시 분석 및 설계 단계에서 정의한 보안 요구사항이 효과적으로 적용·확인하기 위한 시험을 수행하고 있는가?

→ 정보시스템을 인수하기 전 사전 정의한 인수기준과의 적합성 여부를 테스트</td></tr>
</table>

	① 정보시스템 인수 전 인수기준 적합성 여부를 확인하기 위한 시험 수행 ≫ 정보시스템이 사전에 정의한 보안 요구사항을 만족하여 개발·변경 및 도입되었는지 확인하기 위한 인수기준 및 절차 수립 ≫ 정보시스템을 인수하기 전 사전 정의한 인수기준과의 적합성 여부를 테스트 등을 통하여 확인한 후 인수 여부를 결정 ≫ 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 ≫ 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 코딩표준에 따라 구현하는지 소스코드 검증 ② 코딩이 완료된 프로그램은 운영환경과 동일한 환경에서 취약점 점검도구 또는 모의진단을 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 의도치 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	입·출력값 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 처리방법 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 서비스(게시판 등) 요청스크립트 게시 등)과 응답결과(스크립트를 포함한 웹 페이지)에 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 검증방법 설계 및 유효하지 않은 값에 대한 처리방법 설계	
SR1-8	허용된 범위내 메모리 접근	◦ 해당 프로세스에 허용된 범위의 메모리 버퍼에만 접근하여 읽기 또는 쓰기 기능을 하도록 검증방법 설계 및 메모리 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
입력 데이터 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 메모리 접근	◦ 포맷 스트링 삽입 ◦ 메모리 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
보안 기능 (8개)	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 해쉬 함수 사용
	중요정보 저장	◦ 암호화되지 않은 중요정보 ◦ 사용자 하드디스크에 저장되는 쿠키를 통한 정보 노출
	중요정보 전송	◦ 암호화되지 않은 중요정보
에러 처리 (1개)	예외처리	◦ 오류 메시지 정보노출
세션 통제 (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 개선계획 수립, 이행점검 등의 절차를 이행하고 있는가?

→ 도출 취약점 개선계획 수립

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

② 불가피한 사유로 시스템 오픈 전에 개선이 어려울 경우에는 이에 따른 영향도 평가, 보완 대책, 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 이상 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

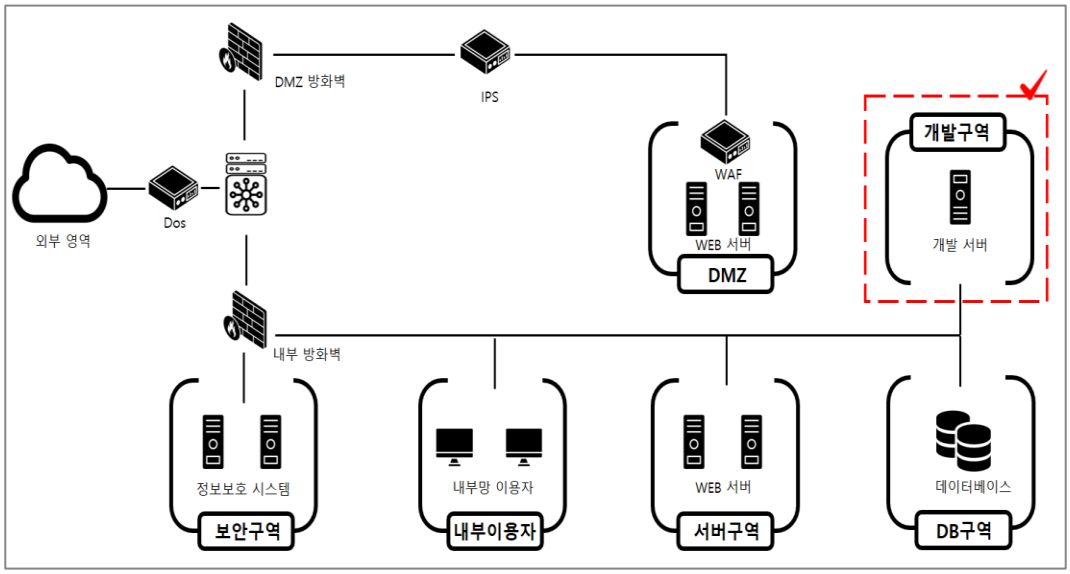
※ 출처: 개인정보 영향평가 수행안내서 (개인정보보호위원회·KISA)

2.8.3 시험과 운영 환경 분리

세부분야	2.8.3 시험과 운영 환경 분리
인증 기준	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소시키기 위하여 원칙적으로 분리하여야 한다.
주요 확인사항	• 정보시스템의 개발 및 시험 시스템을 운영시스템과 분리하고 있는가? • 불가피한 사유로 개발과 운영환경의 분리가 어려운 경우 상호검토, 상급자 모니터링, 변경 승인, 책임추적성 확보 등의 보안대책을 마련하고 있는가?
기준 요약도	
운영 방안	◇ 정보시스템의 개발 및 시험 시스템을 운영시스템과 분리하고 있는가? → 개발보안에 대한 정책 및 절차(예시) 「**개발보안 지침**」 제 ○○조 (개발환경 분리) ① 개발/시험 환경과 운영환경을 분리하기 어려운 경우 다음 사항을 포함한 보안대책을 수립한 ≫ 개발/시험으로 인하여 영향을 받는 부분에 대한 범위 산정 ≫ 개발/시험의 오류로 인하여 발생할 수 있는 장애의 유형 및 복구 대책 ≫ 장애 발생 시 대응을 위한 상세한 시험절차 수립 ≫ 개발/시험 중 서비스 운영의 정상 여부를 지속적으로 모니터링하기 위한 대책

≫ 운영환경에서 개발/시험을 수행하기 전에 정보보호 책임자 등으로부터의 승인

≫ 운영데이터가 시험데이터로 사용되는 경우 운영데이터 보호를 위한 대책



※ 개발환경 분리(이해를 돕기 위한 예시)

◇ 불가피한 사유로 개발과 운영환경의 분리가 어려운 경우 상호검토, 상급자 모니터링, 변경 승인, 책임추적성 확보 등의 보안대책을 마련하고 있는가?

→ 개발 운영 분리가 어려울 경우 보완통제수단 적용

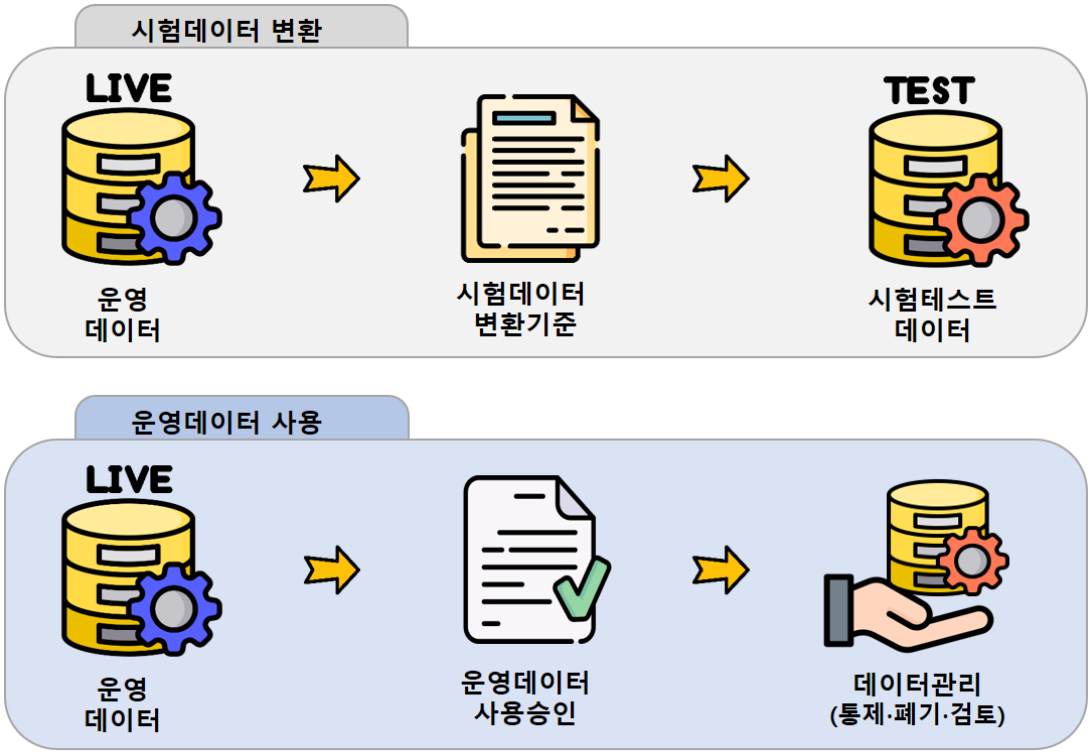
① 직무자 간 상호검토

② 변경 승인

③ 상급자의 모니터링 및 감사

④ 백업 및 복구 방안, 책임추적성 확보 등

2.8.4 시험 데이터 보안

세부분야	2.8.4 시험 데이터 보안
인증 기준	시스템 시험 과정에서 운영데이터의 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 운영데이터를 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 익명화을 통하여 테스트 데이터로 변환한 후 사용한다. 단, 실데이터를 변환하지 않고 테스트를 할 경우에는 정보보호 관리자의 승인을 득해야 한다.

① 테스트 데이터 사용 요청서 ②

정보시스템 책임자	정보보호 관리자

작성 일자 :

신청자	소속 구분		관리담당자	
	소 속		직급	
	성 명		연락처	
	사용 목적			

시험 데이터 사용 정보	요청 데이터			
	개인정보 항목			
	관리 방안			
	사용 기간		폐기 예정일	

※ 테스트 데이터 사용 신청서(이해를 돕기 위한 예시)

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

→ 운영데이터 사용 시 통제 절차 수립

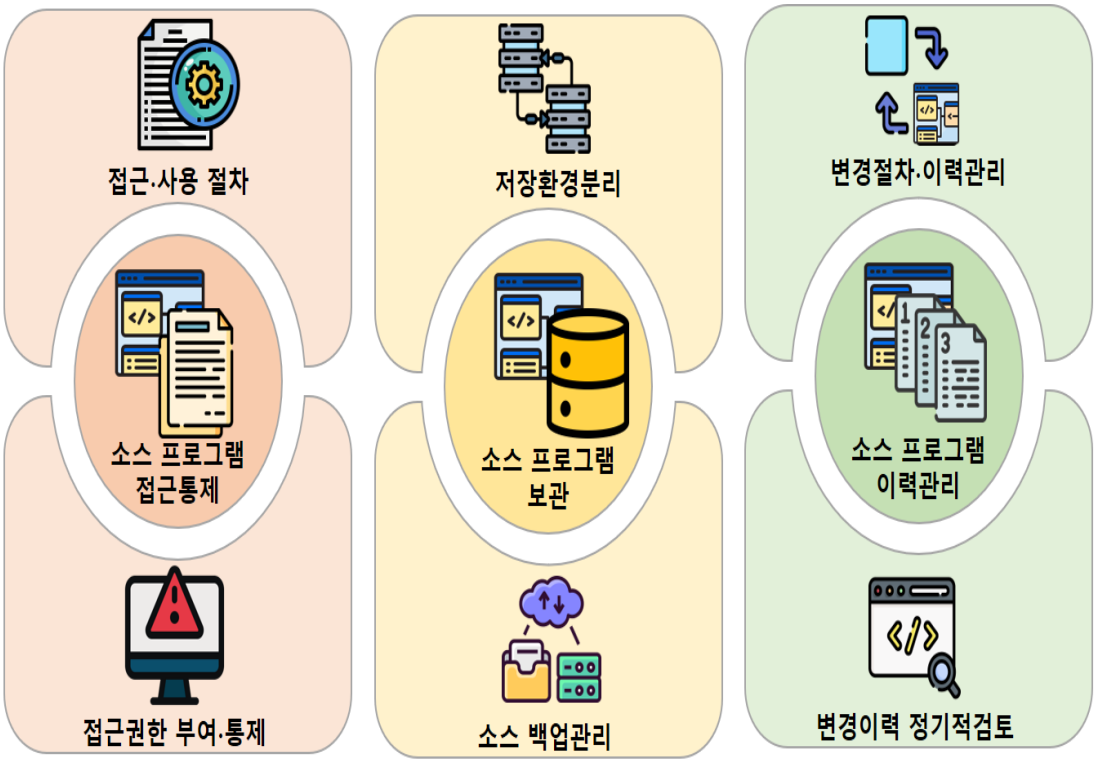
① 운영데이터 사용승인 절차 마련: 데이터 중요도에 따른 보고 및 승인체계 정의 등

② 시험 기한 만료 후 데이터 폐기절차 마련 및 이행

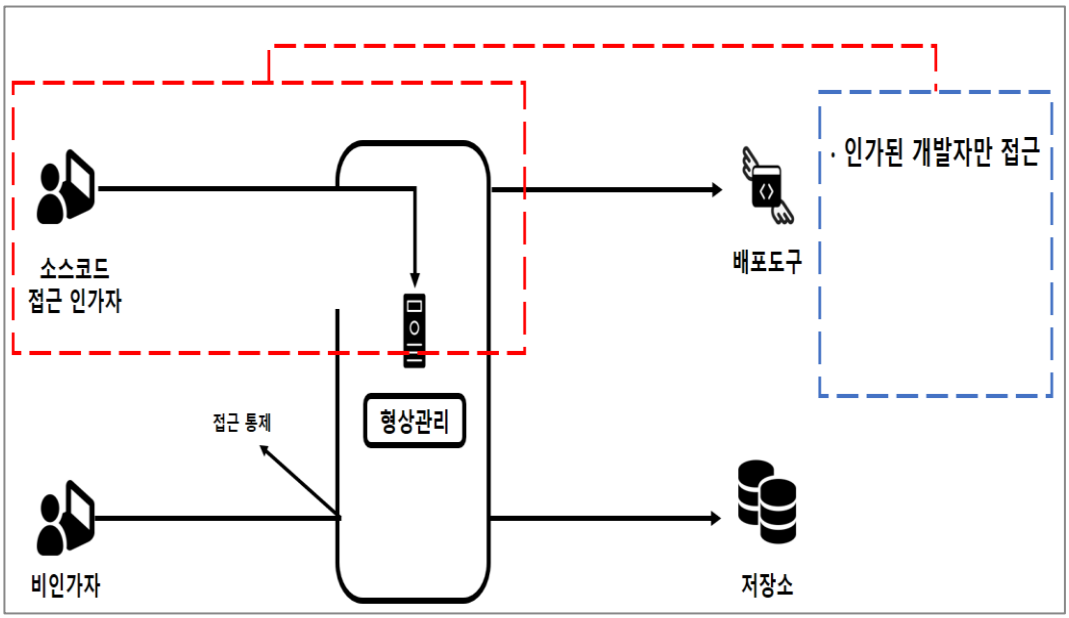
③ 운영데이터 사용에 대한 시험환경에서의 접근통제 대책 적용

④ 운영데이터 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, 운영환경에 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 운영환경이 아닌 곳에 안전하게 보관하고 있는가? • 소스 프로그램에 대한 변경이력을 관리하고 있는가?
기준 요약도	
운영 방안	**◇ 비인가자에 의한 소스 프로그램 접근을 통제하기 위한 절차를 수립·이행하고 있는가?** **→ 소스 프로그램 접근 통제 절차 수립** **「개발보안 관리지침」** 제 ○○조 (소스프로그램 관리) ① 소스 프로그램은 인가된 사용자만이 접근할 수 있도록 관리하고 비인가자의 소스 프로그램 접근을 다음과 같이 통제하여야 한다 ≫ 소스코드가 보관된 서버에 대한 접근통제 적용 ≫ 소스프로그램 접근 시 인가자만 접근 가능하도록 접근권한 부여

≫ SW개발과정 형상관리 도구: CVN·SVN·Git



※ 형상관리시스템 접근제어 (이해를 돕기 위한 예시)

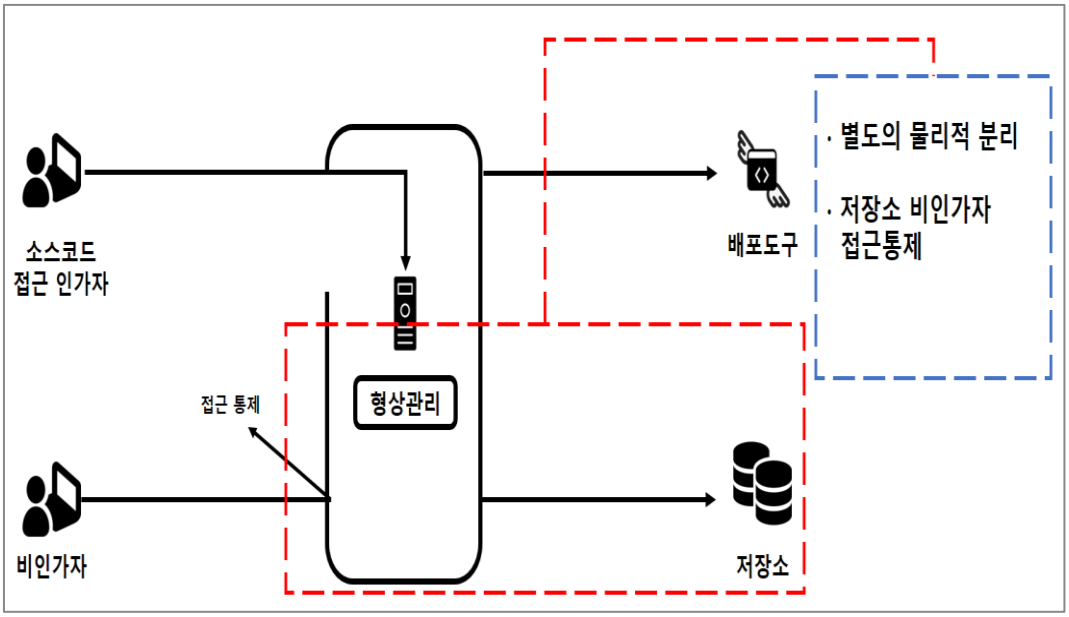
◇ 소스 프로그램은 장애 등 비상시를 대비하여 운영환경이 아닌 곳에 안전하게 보관하고 있는가?

→ 소스프로그램 백업 관리

① 최신 소스 프로그램 및 이전 소스 프로그램에 대한 백업 보관

② 운영환경이 아닌 별도의 환경에 저장·관리

③ 소스 프로그램 백업본에 대한 비인가자의 접근 통제



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

◇ 소스 프로그램에 대한 변경이력을 관리하고 있는가?

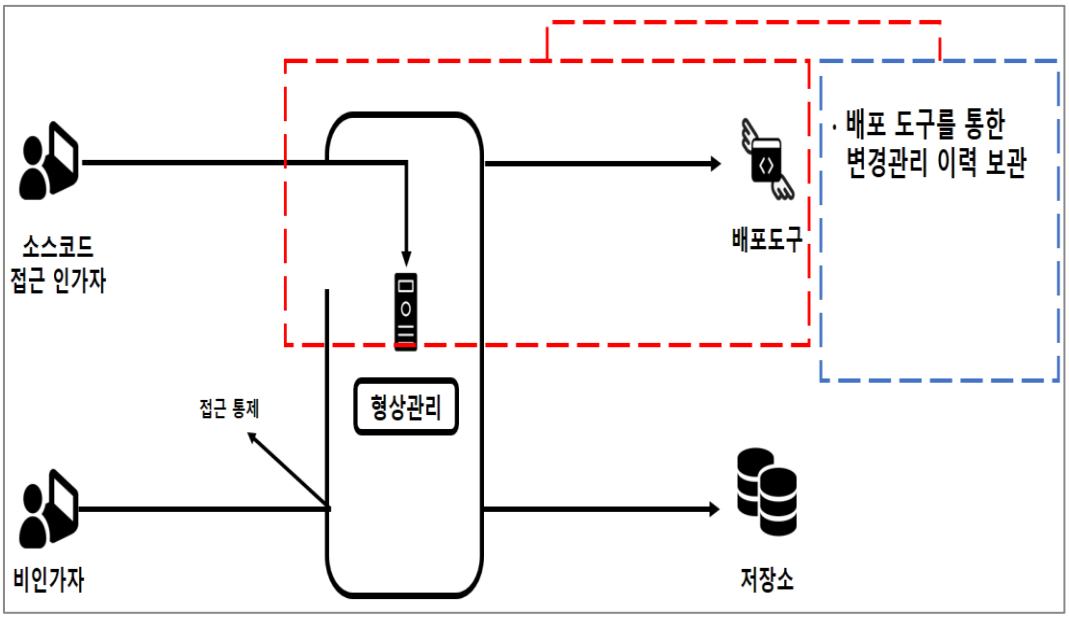
→ 소스코드 배포 및 변경 이력 관리

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

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

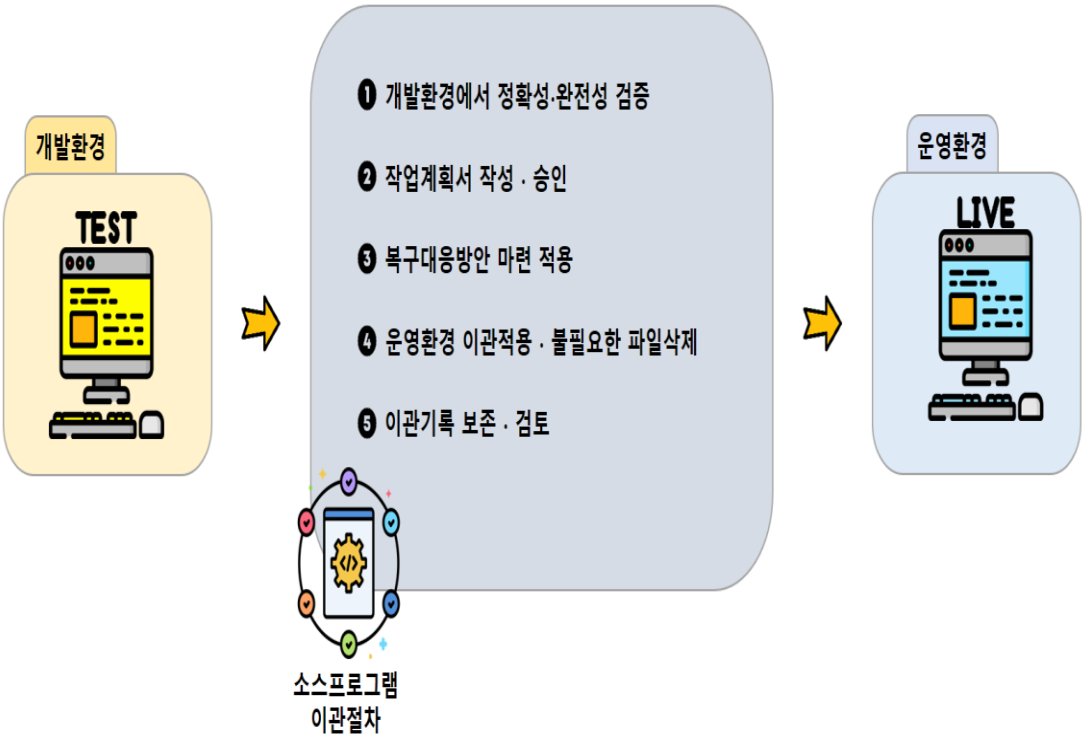
③ 소스 프로그램 변경에 따른 시스템 관련 문서(설계서 등)에 대한 변경통제 수행

④ 소스 프로그램 변경 이력 및 변경통제 수행내역에 대한 정기적인 검토 수행

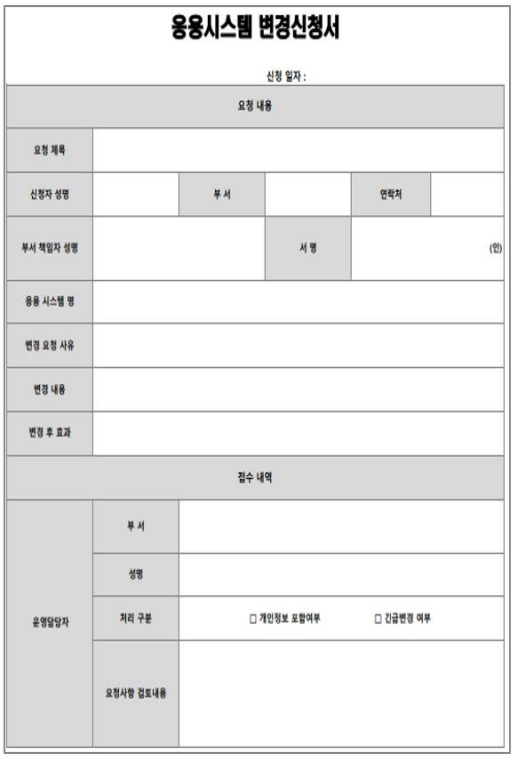


※ 소스프로그램 변경관리 이력 보관 (이해를 돕기 위한 예시)

2.8.6 운영환경 이관

세부분야	2.8.6 운영환경 이관
인증 기준	신규 도입·개발 또는 변경된 시스템을 운영환경으로 이관할 때는 통제된 절차를 따라야 하고, 실행코드는 시험 및 사용자 인수 절차에 따라 실행되어야 한다.
주요 확인사항	• 신규 도입·개발 및 변경된 시스템을 운영환경으로 안전하게 이관하기 위한 통제절차를 수립·이행하고 있는가? • 운영환경으로 이관 시 발생할 수 있는 문제에 대한 대응 방안을 마련하고 있는가? • 운영환경에는 서비스 실행에 필요한 파일만을 설치하고 있는가?
기준 요약도	
운영 방안	**◇ 신규 도입·개발 및 변경된 시스템을 운영환경으로 안전하게 이관하기 위한 통제 절차를 수립·이행하고 있는가?** **→ 운영환경 이전 계획 수립** **「개발보안 관리지침」** 제 ○○조 (응용시스템 변경관리) ① 응용시스템의 변경사항이 발생한 경우 '응용시스템 변경 요청서'를 작성하여 담당 정보시스템 책임자에게 변경요청 해야한다. ② 담당 정보시스템 책임자는 변경 요청서의 타당성을 검토 후 '응용시스템 변경 계획서'를 작성하여 반영한다. 단, 긴급한 상황 하에서 승인절차를 생략하고 응용

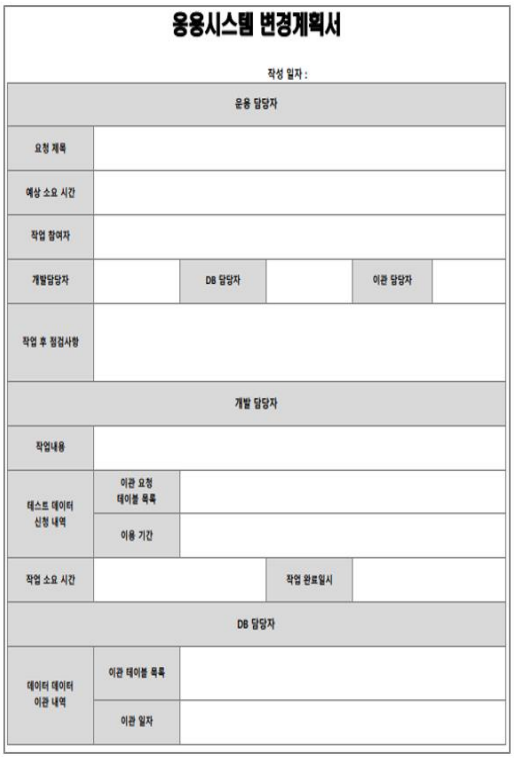
시스템을 변경한 경우 사후 승인을 득 해야한다.



응용시스템 변경신청서

신청 일자 :

요청 내용				
요청 제목				
신청자 성명		부 서		연락처
부서 책임자 성명		서 명		(인)
응용 시스템 명				
변경 요청 사유				
변경 내용				
변경 후 효과				
접수 내역				
운영담당자	부 서			
	성명			
	처리 구분	□ 개인정보 포함여부	□ 긴급변경 여부	
	요청사항 검토내용			



응용시스템 변경계획서

작성 일자 :

운용 담당자				
요청 제목				
예상 소요 시간				
작업 참여자				
개발담당자		DB 담당자		이관 담당자
작업 후 점검사항				
개발 담당자				
작업내용				
테스트 데이터 신청 내역	이관 요청 테이블 목록			
	이용 기간			
작업 소요 시간		작업 완료일시		
DB 담당자				
데이터 데이터 이관 내역	이관 테이블 목록			
	이관 일자			

※ 응용프로그램 변경신청서 및 계획서(이해를 돕기 위한 예시)

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

→ 운영환경 이관 문제 발생 시 대응 절차 수립

① 운영환경으로 정보시스템 이관이 원활하게 이루어지지 않았을 경우 Rollback 방안

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

◇ 운영환경에는 서비스 실행에 필요한 파일만을 설치하고 있는가?

→ 불필요한 테스트 소스 파일 삭제

① 운영환경에는 승인되지 않은 개발도구(편집기 등), 소스 프로그램 및 백업본, 업무문서 등 서비스 실행에 불필요한 파일이 존재하지 않도록 관리

2.9 시스템 및 서비스 운영관리

2.9.1 변경관리

세부분야	2.9.1 변경관리
인증 기준	정보시스템 관련 자산의 모든 변경내역을 관리할 수 있도록 절차를 수립·이행하고, 변경 전 시스템의 성능 및 보안에 미치는 영향을 분석하여야 한다.
주요 확인사항	• 정보시스템 관련 자산(하드웨어, 운영체제, 상용 소프트웨어 패키지 등) 변경에 관한절차를 수립·이행하고 있는가? • 정보시스템 관련 자산 변경을 수행하기 전 성능 및 보안에 미치는 영향을 분석하고 있는가?
기준 요약도	
운영 방안	**◇ 정보시스템 관련 자산(하드웨어, 운영체제, 상용 소프트웨어 패키지 등) 변경에 관한 절차를 수립·이행하고 있는가?** **→ 변경관리 절차 수립** **「정보시스템 운영 관리지침」** 제 ○○조 (변경관리 대상) ① 정보시스템 책임자는 다음 각호의 변경작업 수행 시 '변경 요청서'를 작성하고 정보보호최고책임자의 승인을 득한 후 변경작업을 실시한다. ≫ 정보시스템 구성 추가·증설·변경·교체·제게

≫ 시스템 설정변경·환경 설정 변경 추가

≫ 데이터 및 파일 백업·복구·전환·변경 작업

≫ 정보시스템 장애·성능향상 등 기타 작업

② 변경 작업 완료 후 5일 이내 '변경 결과보고서'를 작성하여 정보보호최고책임자의 승인 득한 후 기록 관리한다.

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: 구성 및 변경관리 지침(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 변경을 이행

③ 변경 실패에 따른 복구방안을 사전에 고려

변경관리 점검 체크리스트

점검일시		점검자	
점검대상 입주기관		입주기관 관리책임자명	

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

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 흐름이 변경 관리자의 통제를 통해 적절히 진행되고 있는가?		
6. 단순변경 사항에 대해서 사전에 정의되고 계속 추가 되고 있는가?		
7. 문제관리 및 구성관리 프로세스와 원활하게 연계 되고 있는가?		
8. 변경 철회시를 대비하여 업무에 혼란이 발생되지 않도록 필요한 사항이 사전에 준비가 되었는가?		

구성관리 점검 체크리스트

점검일시		점검자	
점검대상 입주기관		입주기관 관리책임자명	

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

항 목	Y/N/P/NA	부적합 건수
1. 구성요소중 부적합하게 등록되거나 미등록된 구성요소은 없는가 ?		
2. 구성관리 데이터베이스와 실제 구성요소의 상태가 갱신되지 않거나 불일치 하는 구성요소는 없는가?		
3. 변경관리 절차를 따르지 않고 구성변경이 수행된 경우는 없는가?		
4. 구성베이스라인이 최초 입주시점과 대규모 변경 등 규정된 시점마다 설정되었는가?		
5. 구성요소의 변경에 따라, 관련된 상위 및 하위 구성요소가 적절하게 갱신되었는가?		
6. 구성요소에 대한 변경, 장애, 문제이력이 적합하게 기록되었는가?		
7. 구성관리 데이터베이스와 DSL이 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 대응절차를 수립·이행하고 있는가? • 정보시스템 장애를 즉시 인지하고 대응하기 위한 절차를 수립·이행하고 있는가? • 장애 발생 시 절차에 따라 조치하고 장애조치보고서 등을 통하여 장애조치내역을 기록하여 관리하고 있는가? • 심각도가 높은 장애의 경우 원인분석을 통한 재발방지 대책을 마련하고 있는가?
기준 요약도	
운영 방안	**◇ 정보시스템의 가용성 보장을 위하여 성능 및 용량을 지속적으로 모니터링할 수 있는 절차를 수립·이행하고 있는가?** **→ 정보시스템 가용성 보장 모니터링 절차 수립** 「**정보시스템 운영 관리지침**」 제 ○○조 (시스템 성능관리 및 유지보수) ① 성능관리 대상은 1등급 정보시스템으로 정한다.

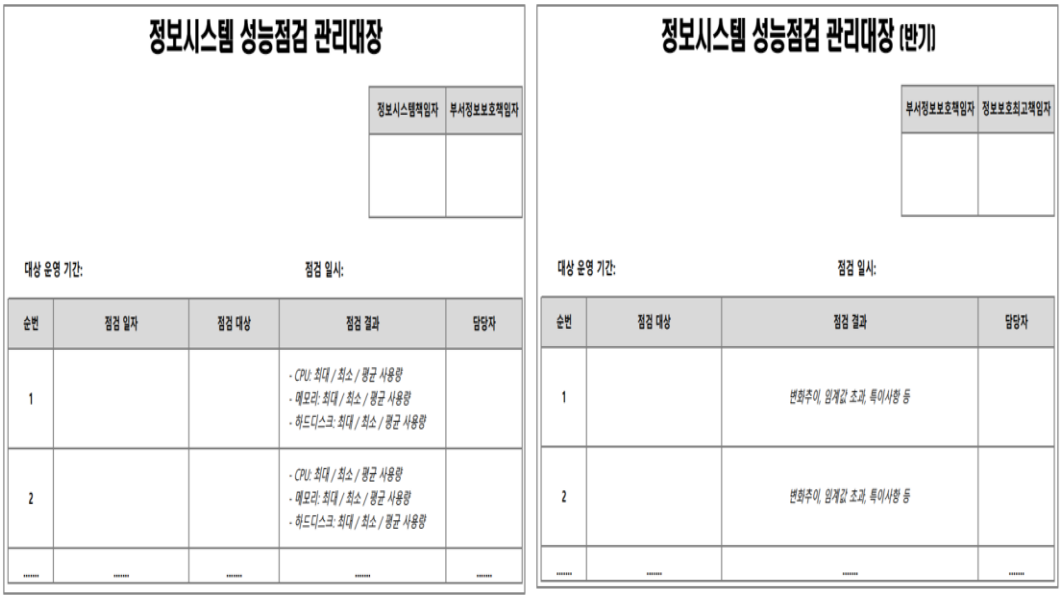
② 정보시스템책임자는 각 호의 임계값에 따라 월 1회 이상 모니터링 활동을 수행하고 '정보시스템 성점검검 관리대장'에 기록 관리 해야한다.

≫ CPU 사용률 임계치: 80% ~ 85% 이상일 경우 지속적인 모니터링

≫ 메모리 사용률 임계치: 80% ~ 85% 이상일 경우 지속적인 모니터링

≫ 디스크 사용률 임계치: 70% ~ 75% 이상일 경우 지속적인 모니터링

③ 부서 정보보호책임자는 성능점검 결과를 반기 1회 이상 정보보호최고책임자에게 보고해야 한다.



정보시스템 성능점검 관리대장

정보시스템책임자	부서정보보호책임자

대상 운영 기간: 점검 일시:

순번	점검 일자	점검 대상	점검 결과	담당자
1			- CPU: 최대 / 최소 / 평균 사용량 - 메모리: 최대 / 최소 / 평균 사용량 - 하드디스크: 최대 / 최소 / 평균 사용량	
2			- CPU: 최대 / 최소 / 평균 사용량 - 메모리: 최대 / 최소 / 평균 사용량 - 하드디스크: 최대 / 최소 / 평균 사용량	
.....	.....	.....	.....	.....

정보시스템 성능점검 관리대장 (반기)

부서정보보호책임자	정보보호최고책임자

대상 운영 기간: 점검 일시:

순번	점검 대상	점검 결과	담당자
1		변화추이, 임계값 초과, 특이사항 등	
2		변화추이, 임계값 초과, 특이사항 등	
.....	.....	.....	.....

※ 성능점검 관리대장(이해를 돕기 위한 예시 작성)

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

→ 지속적인 임계값 초과 위험 발생 모니터링 및 변경계획 수립

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

성능분석/조정 요청서

년 월 일(요일)

문서번호		연계문서번호	

요청부서		처리부서	
요청부서		접수	접수번호
담당자	(인)		접수일시
직급/직위		성능관리담당자	(인)
전화번호		성능관리책임자	(인)
E-Mail		협조부서	(인)

☐ 성능 분석 배경

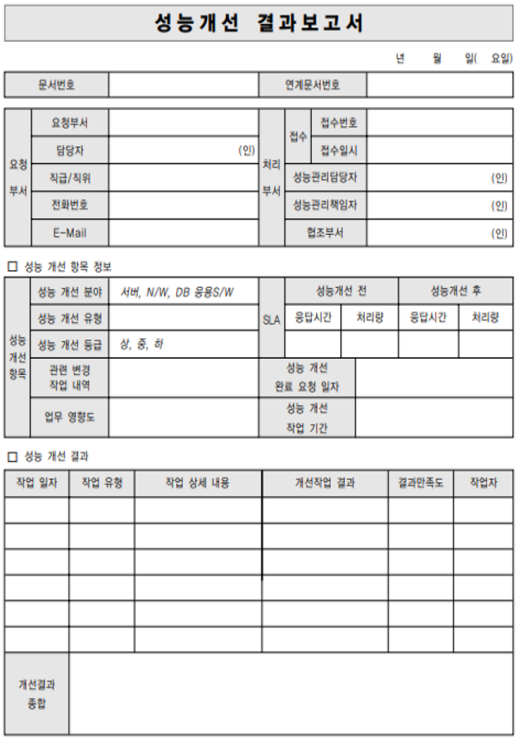
성능저하 현상 배경		SLA	요구수준		현상태	
	성능저하업무		응답시간	처리량	응답시간	처리량
	관련 프로그램					
	업무 영향도					
	성능 저하 발생 시점		성능분석/조정 완료시한			
	관련 변경 작업 내역	네트워크공사 어플리케이션 패치 등				

☐ 예상되는 성능 저하 원인

분야	서버	네트워크	DBMS	응용소프트웨어	기타
중상및측정데이터					
구성정보					
종합현황					

☐ 서비스 아키텍처 분석

서비스 아키텍처	3 Tier환경 C/S 환경		
적용업무		사용시간대	
		사용빈도	
		사용자 수	



성능개선 결과보고서

년 월 일(요일)

문서번호		연계문서번호	

요청부서		처리부서	
요청부서		접수	접수번호
담당자	(인)		접수일시
직급/직위		성능관리담당자	(인)
전화번호		성능관리책임자	(인)
E-Mail		협조부서	(인)

☐ 성능 개선 항목 정보

성능개선 항목	성능 개선 분야	서버, N/W, DB 응용S/W	SLA	성능개선 전		성능개선 후	
	성능 개선 유형			응답시간	처리량	응답시간	처리량
	성능 개선 등급	상, 중, 하					
	관련 변경 작업 내역		성능 개선 완료 요청 일자				
	업무 영향도		성능 개선 작업 기간				

☐ 성능 개선 결과

작업 일자	작업 유형	작업 상세 내용	개선작업 결과	결과만족도	작업자
개선결과 종합					

※ 출처: 성능관리지침(NIA)

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

→ 정보시스템 장애 대응 절차 수립

① 장애유형 및 심각도 정의

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)

② 장애유형 및 심각도별 보고 절차

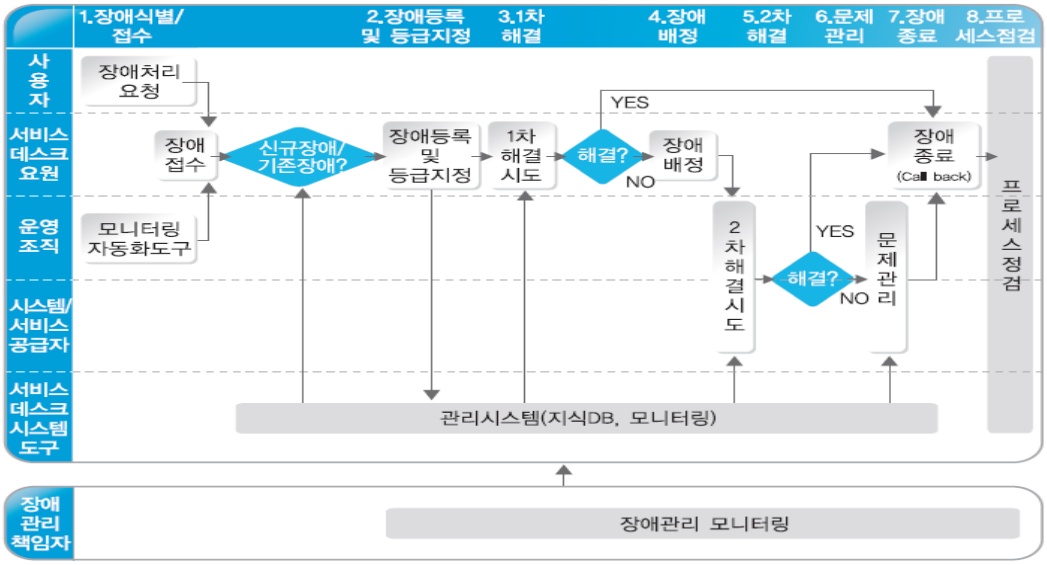
③ 장애유형별 탐지 방법 수립

④ 장애 대응 및 복구에 관한 책임과 역할 정의

⑤ 장애기록 및 분석

⑥ 대고객 서비스인 경우 고객 안내 절차

⑦ 비상연락체계(유지보수업체, 정보시스템 제조사) 등



※ 출처: 정보시스템 장애관리 지침(NIA)

◇ 장애 발생 시 절차에 따라 조치하고 장애조치보고서 등을 통하여 장애조치내역을 기록하여 관리하고 있는가?

→ 정보시스템 장애 조치 기록 관리

① 장애일시

② 장애심각도

③ 담당자, 책임자명

④ 장애내용

⑤ 장애원인, 조치내용, 복구내용, 재발방지대책 등

장 애 결 과 보 고 서

담 당	검 토	승 인	협조 1	협조 2

장애 제목	
내용/현상	
장애 원인	
영향 범위	

발생 일시		해결 일시		장애 시간	분
장애 번호		장애 유형		장애 등급	
작성 일자		작성 부서		작성자	

조치 시간	조치 내용 및 결과	조치자

향 후 이 행 대 책	완료일	이행 담당자

일 일 시 스 템 업 무 보 고

1. 일 시	(2004. 1. 16 (금) 00:00 ~ 24:00)
2. 보 고 자	(전산실 운영담당 홍길동 과장)
3. 주 요 장 애	(장애등급 1, 2, 3 위주로 내용 보고) - 장애제목 : - 장애일시 : - 장애등급 : - 장애현상 : - 장애원인 : - 영향범위 : - 비 고 :
4. 주 요 작 업	(주요 변경작업 위주로 내용 보고) - 작업내용 : - 담 당 자 : - 작업등급 : (Risk 1, 2, 3, 4) - 업무영향 : - 작업상태 : (정상완료, 부분완료, 원상복귀, 장애유발 등) - 비 고 :
5. 특 이 사 항	(주요 장애 또는 변경작업 이외의 특이사항 내용 보고) - 태풍 '민들레' 영향으로 인해 09:00 현재 전남지역 한전 전원 공급 불안정. - 웜 바이러스(Welchia)로 인해 09:00 현재 수도권 지역 네트워크 속도 지연.

장 애 관 리 대 장

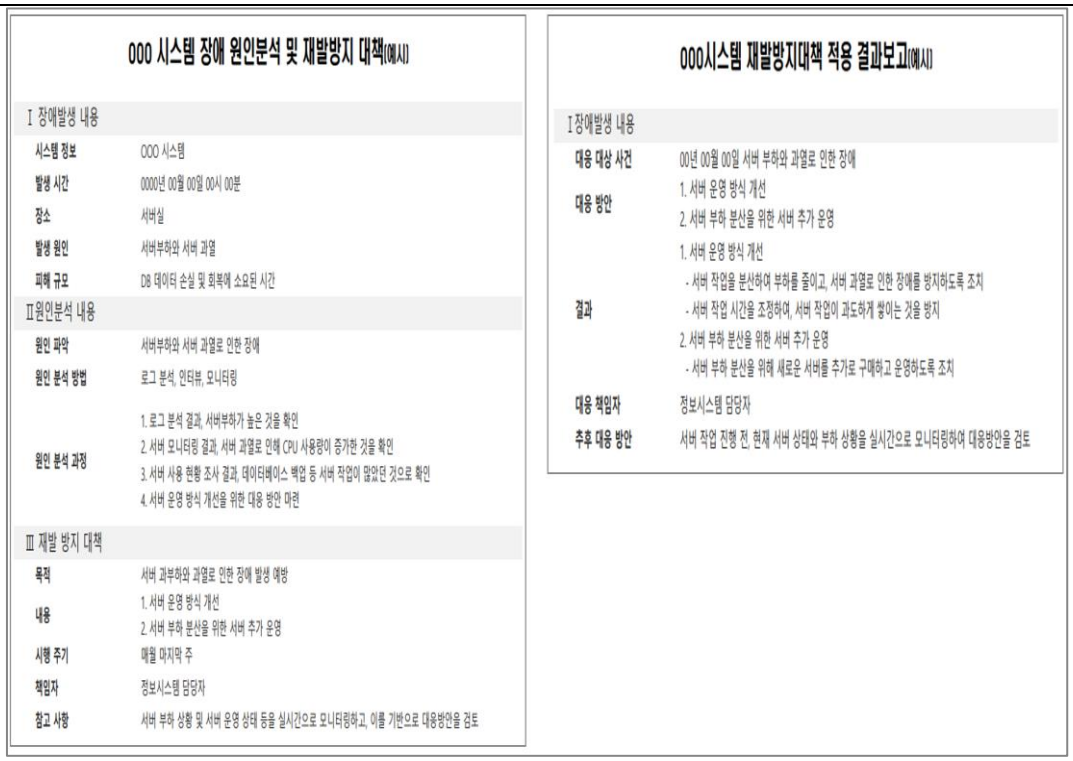
요청번호	발생일시	접수일자	조치기한일자	조치일자	조치 내용	조치자	장애 유형

※ 출처: 정보시스템 장애관리 지침(NIA)

◇ 심각도가 높은 장애의 경우 원인분석을 통한 재발방지 대책을 마련하고 있는가?

→ 원인분석을 통하여 재발방지 대책

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.



OOO 시스템 장애 원인분석 및 재발방지 대책(예시)

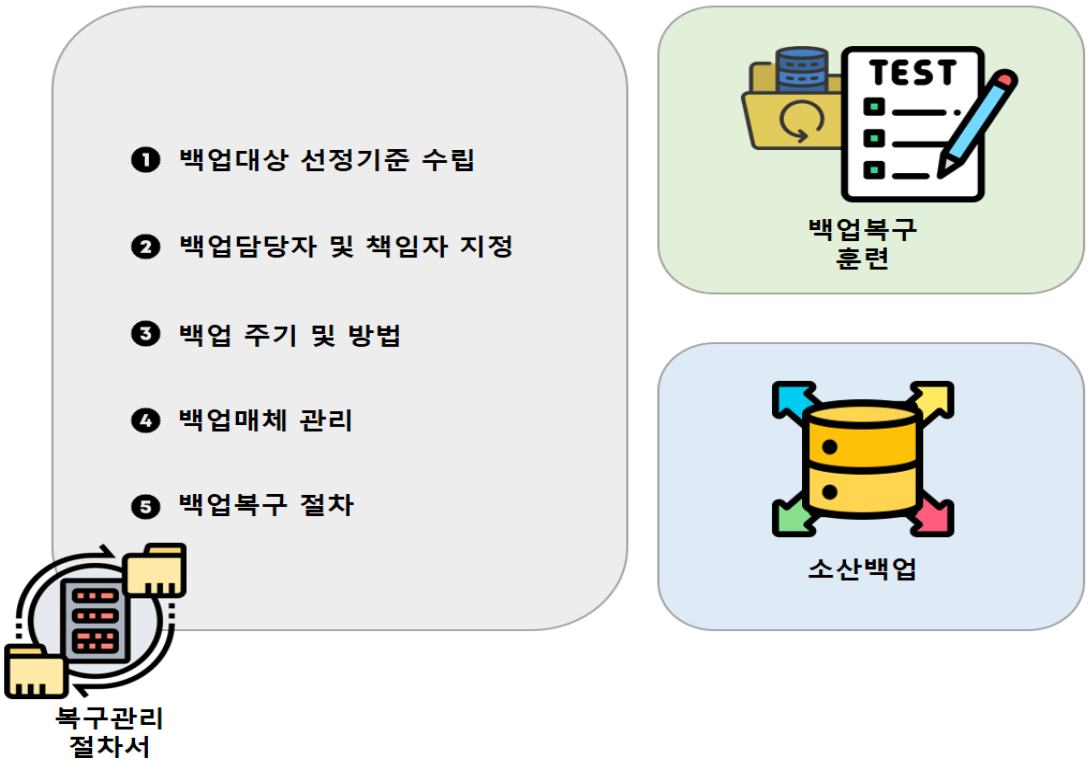
Ⅰ 장애발생 내용	
시스템 정보	OOO 시스템
발생 시간	0000년 00월 00일 00시 00분
장소	서버실
발생 원인	서버부하와 서버 과열
피해 규모	DB 데이터 손실 및 회복에 소요된 시간
Ⅱ원인분석 내용	
원인 파악	서버부하와 서버 과열로 인한 장애
원인 분석 방법	로그 분석, 인터뷰, 모니터링
원인 분석 과정	1. 로그 분석 결과, 서버부하가 높은 것을 확인 2. 서버 모니터링 결과, 서버 과열로 인해 CPU 사용량이 증가한 것을 확인 3. 서버 사용 현황 조사 결과, 데이터베이스 백업 등 서버 작업이 많았던 것으로 확인 4. 서버 운영 방식 개선을 위한 대응 방안 마련
Ⅲ 재발 방지 대책	
목적	서버 과부하와 과열로 인한 장애 발생 예방
내용	1. 서버 운영 방식 개선 2. 서버 부하 분산을 위한 서버 추가 운영
시행 주기	매월 마지막 주
책임자	정보시스템 담당자
참고 사항	서버 부하 상황 및 서버 운영 상태 등을 실시간으로 모니터링하고, 이를 기반으로 대응방안을 검토

OOO시스템 재발방지대책 적용 결과보고(예시)

Ⅰ장애발생 내용	
대응 대상 사건	00년 00월 00일 서버 부하와 과열로 인한 장애
대응 방안	1. 서버 운영 방식 개선 2. 서버 부하 분산을 위한 서버 추가 운영
결과	1. 서버 운영 방식 개선 - 서버 작업을 분산하여 부하를 줄이고, 서버 과열로 인한 장애를 방지하도록 조치 - 서버 작업 시간을 조정하여, 서버 작업이 과도하게 쌓이는 것을 방지 2. 서버 부하 분산을 위한 서버 추가 운영 - 서버 부하 분산을 위해 새로운 서버를 추가로 구매하고 운영하도록 조치
대응 책임자	정보시스템 담당자
추후 대응 방안	서버 작업 진행 전 현재 서버 상태와 부하 상황을 실시간으로 모니터링하여 대응방안을 검토

※ 시스템장애 재발방지대책(이해를 돕기 위한 예시)

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, 보관장소, 보관기간, 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 복구절차를 수립·이행하고 있는가? • 백업된 정보의 완전성과 정확성, 복구절차의 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 복구절차를 수립·이행하고 있는가?** **→ 백업 및 복구절차를 수립·이행** **「IT 업무 연속성 관리지침」** 제 ○○조 (백업 복구 계획) ① 백업대상 선정기준 데이터 파손 시 복구 필요성이 있는 주요 데이터로 각 호와 같은 정보들을 백업한다. ≫ 각종서버에 저장된 운영체제, 시스템프로그램, 업무개발 소스 및 DATA

② 백업담당자 및 책임자 지정

③ 백업대상별 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 돕기위한 예시 작성)

④ 백업방법 및 절차

⑤ 백업매체 관리

⑥ 백업 복구 절차

≫ 정보시스템 재해 및 장애 발생 시 데이터가 손실 또는 훼손된 경우 최신 데이터로 빠르게 복구해야한다.

≫ 사용자 부주의 또는 업무 착오 등으로 인한 데이터 훼손 시 '자료 복구 신청서' 작성하여 백업 운영자에게 요청하고 백업 운영자는 이를 근거로 자료 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	※ 백업적용 후 신청자에게 회신할 것		

※ 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 파일명	
전체 파일크기	
대상파일 백업일자	
※복구 불가시 대체백업일자	
복구 위치	
복구 완료 희망시간	
특기사항	

※작업완료정보

접수 일시			
작업자 성명		작업소요시간	
복구 결과			

※ 검토란은 승인자의 성명을 기입하여 결재가 가능함.

※ 출처: 정보시스템 백업지침(NIA)

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

→ 복구테스트 훈련

① 복구테스트 계획(복구테스트 주기 및 시점, 담당자, 방법 등)

② 복구테스트 시나리오 수립

③ 복구테스트 실시 및 결과 보고

④ 복구테스트 결과 문제점 발견 시 개선계획 수립 및 이행

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

→ 주기적 소산백업

「IT업무연속성관리지침」 제 ○○조 (백업관리)

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

※ 소산백업관리대장(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, 권한부여 내역 등의 로그유형, 보존기간, 보존방법 등을 정하고 위·변조, 도난, 분실되지 않도록 안전하게 보존·관리하여야 한다.
주요 확인사항	• 서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 로그관리절차를 수립하고 이에 따라 필요한 로그를 생성하여 보관하고 있는가? • 정보시스템의 로그기록은 별도 저장장치를 통하여 백업하고, 로그기록에 대한 접근 권한은 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 로그관리 절차를 수립하고 이에 따라 필요한 로그를 생성하여 보관하고 있는가?** **→ 로그기록관리 절차를 수립** **「정보시스템 운영보안 지침」** 제 ○○조 (로그기록 관리) ① 정보시스템 관리자는 운영하는 보존이 필요한 로그 유형 및 대상시스템 식별하고

정보시스템의 로그를 각 호의 상황을 포함하여 저장관리해야 한다.

≫ 이벤트 로그: 시스템 시작, 종료, 상태, 에러코드 등

≫ 네트워크 이벤트로그: IP 할당, 주요 구간 트래픽 로그 등

≫ 보안 시스템: 관리자 접속, 보안정책(룰셋) 변경내역 등

≫ 정보시스템 감사 로그: 사용자 접속기록, 인증 성공·실패, 파일 접근, 계정 발급·변경·해지내역, 접근권한 부여·변경·말소내역 등

≫ 개인정보처리시스템 접속 로그: 접속계정, 접속일시(시분초), 접속지IP, 수행업무

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 로그기록은 별도 저장장치를 통하여 백업하고, 로그기록에 대한 접근권한은 최소화하여 부여하고 있는가?

→ 접근권한은 최소화

① 로그기록은 스토리지 등 별도 저장장치를 사용하여 백업하고 로그기록에 대한 접근권한 부여는 최소화하여 비인가자에 의한 로그기록 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 검토기준을 수립하여 주기적으로 점검하며, 문제 발생 시 사후조치를 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 대응절차 등

개인정보처리시스템 접속기록 검토

점검항목	점검결과
1. 개인정보를 업무목적 외 생성 및 과다 생성 여부	
2. 개인정보를 업무목적 외 조회 및 과다 조회 여부	
3. 개인정보를 업무목적 외 과다 수정 여부	
4. 개인정보를 업무목적 외 삭제 및 과다 삭제 여부	
5. 개인정보를 업무목적 외 출력 및 과다 출력 여부	
...	...

서버 접속기록 검토

점검항목	점검결과
1. 사용자 로그인 기록	
2. 권한 상승 기록	
3. 비인가 접근 시도 기록	
4. 특정 파일/디렉터리/프로세스 접근 기록	
5. 비정상적인 파일 다운로드/업로드 기록	
...	...

※ 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 정보유출, 해킹, 오·남용, 부정행위 등 발생 여부를 확인하기 위한 절차를 수립하고 절차에 따라 대응

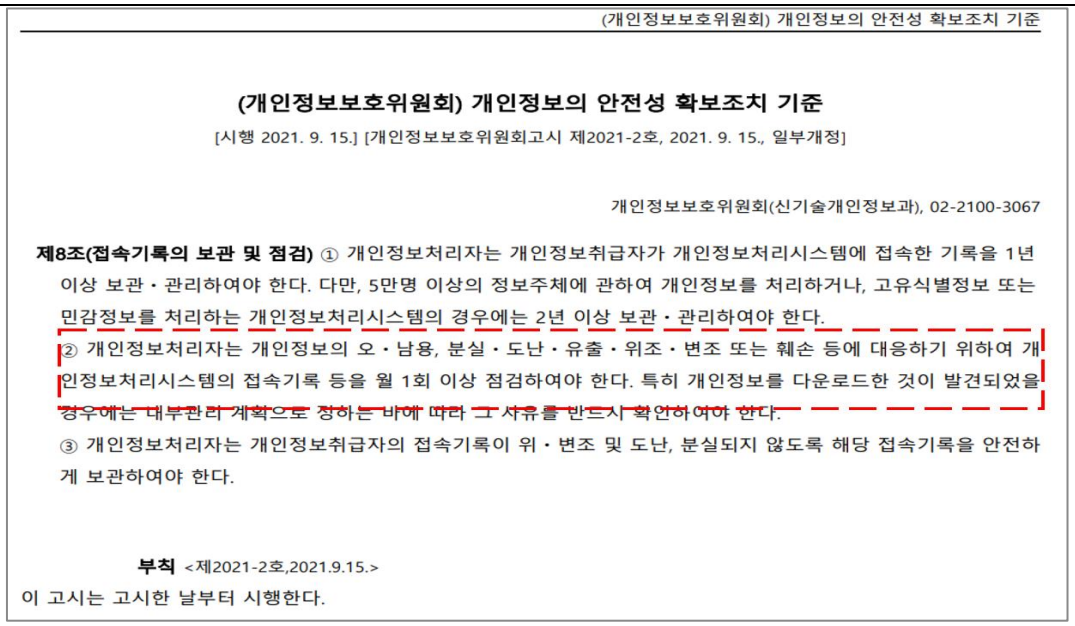
③ 개인정보를 다운로드한 것이 확인된 경우 내부관리계획 등 로그검토 기준에서 하는 바에 따라 그 사유를 확인하고, 개인정보의 오·남용이나 유출 목적으로 다운로드한 것이 확인되었다면 지체 없이

④ 개인정보취급자가 다운로드한 개인정보를 회수하여 파기하는 등의 필요한 조치이행

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

→ 개인정보처리시스템 접속기록 법정검토

① 법령에 따른 개인정보 접속기록 점검 주기: 월 1회 이상



(개인정보보호위원회) 개인정보의 안전성 확보조치 기준

(개인정보보호위원회) 개인정보의 안전성 확보조치 기준

[시행 2021. 9. 15.] [개인정보보호위원회고시 제2021-2호, 2021. 9. 15., 일부개정]

개인정보보호위원회(신기술개인정보과), 02-2100-3067

제8조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.

② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 내부관리 계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.

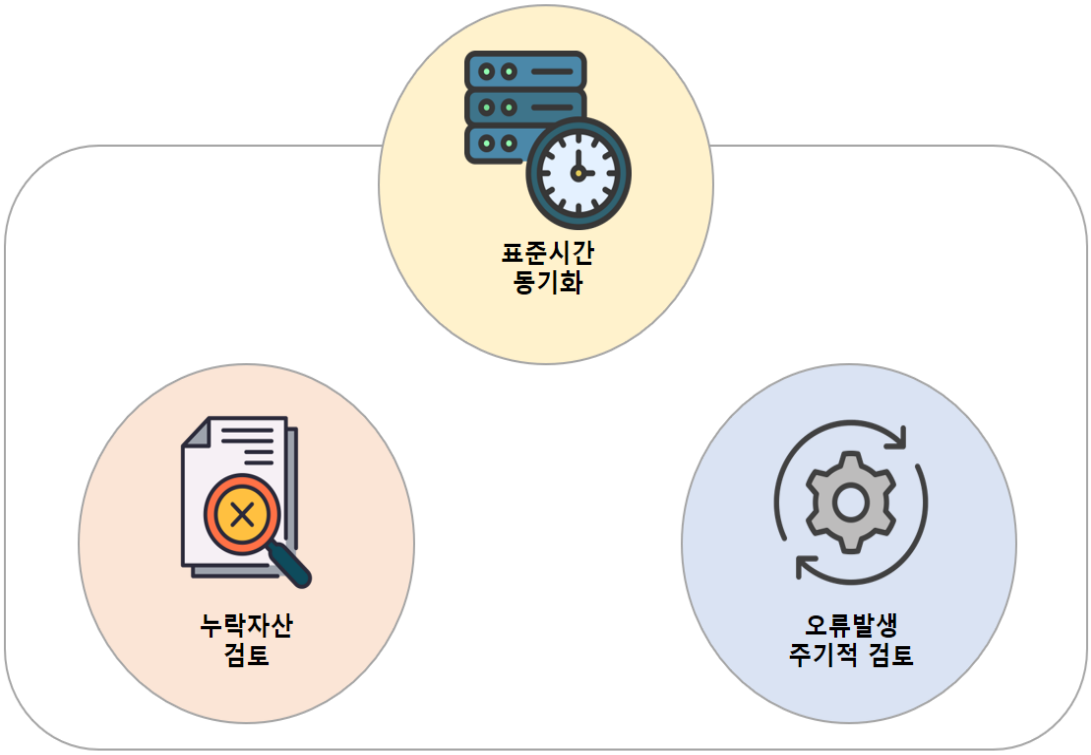
③ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

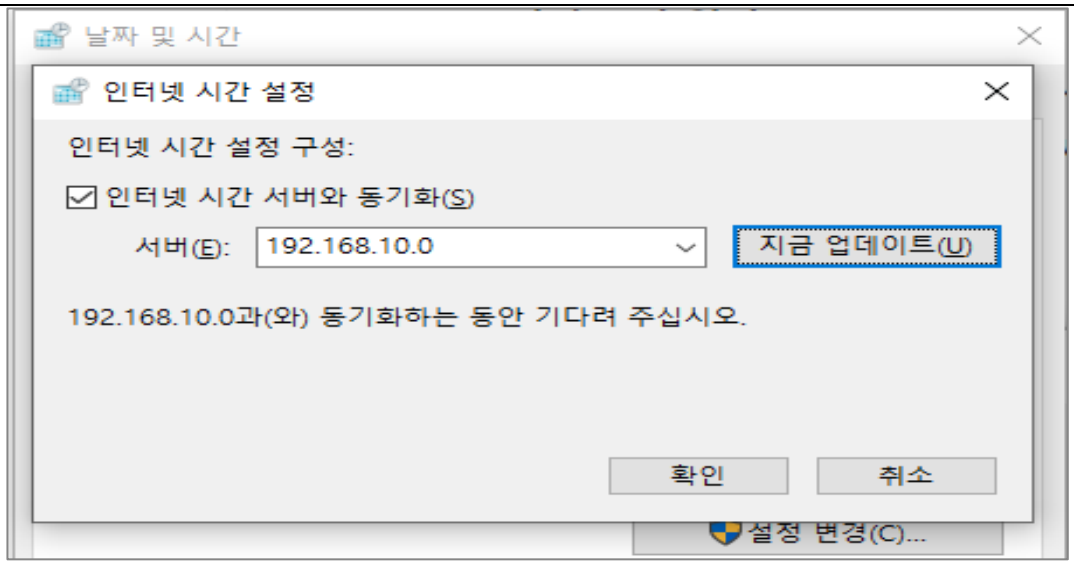
부칙 <제2021-2호,2021.9.15.>

이 고시는 고시한 날부터 시행한다.

※ 출처: 개인정보의 안전성확보조치 기준 (개인정보보호위원회)

2.9.6 시간 동기화

세부분야	2.9.6 시간 동기화
인증 기준	로그 및 접속기록의 정확성을 보장하고 신뢰성 있는 로그분석을 위하여 관련 정보시스템의 시각을 표준시각으로 동기화하고 주기적으로 관리하여야 한다.
주요 확인사항	• 정보시스템의 시간을 표준시간으로 동기화하고 있는가? • 시간 동기화가 정상적으로 이루어지고 있는지 주기적으로 점검하고 있는가?
기준 요약도	
운영 방안	◇ 정보시스템의 시간을 표준시간으로 동기화하고 있는가? → 정보시스템 시간 동기화 절차 「정보시스템 운영관리지침」 제 ○○조 (시간 동기화) ① 정보시스템 로그의 정확성을 보장하고 신뢰성 있는 로그 분석을 위하여 정보시스템의 시각을 표준화하고 동기화 하여야 한다. ≫ NTP(Network Time Protocol) 등 활용하여 정보시스템 간 시간 동기화



※ 윈도우 서버 NTP 설정 (이해를 돕기 위한 예시)

◇ 시간 동기화가 정상적으로 이루어지고 있는지 주기적으로 점검하고 있는가?

→ 시간동기화 주기적 점검

「**정보시스템 운영관리지침**」 제 ○○조 (시간 동기화)

① 시간 동기화가 정상적으로 이루어지고 있는지의 여부를 월 1회 이상 점검하여야 한다.

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 폐기이력을 남기고 폐기확인 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 저장 매체 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, 폐기관리대장 기록 등

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

→ 정보자산 복구되지 않도록 폐기

「**정보시스템 운영관리지침**」 제 ○○조 (정보자산 재사용 및 폐기)

① 정보자산 및 저장매체를 폐기하는 경우 개인정보 등 중요정보가 복구 또는 재생되지 않도록 각 호와 같이 안전하게 파기 해야한다.

≫ (물리적 파기)

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

≫ (논리적 파기)

- 전체 삭제: 로우레벨 포맷 3회
- 일부 삭제: 임의 데이터 3회 덮어쓰기
- DB 데이터 삭제 Dlete 쿼리 이용 삭제

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

→ 정보자산 폐기 이력관리

「**정보시스템 운영관리지침**」 제 ○○조 (정보시스템 등록 및 폐기)

① 정보시스템 자산 폐기 시 정보시스템 책임자는 자산등록/폐기 신청서를 작성하여 정보보호최고책임자의 승인을 득한 후 파기한다.

② 정보시스템 철수 또는 폐기 시 시스템 내 정보를 완전 삭제하고, 정보자산 관리대장 갱신 및 정보자산 폐기관리대장에 기록 관리해야한다.

정보자산 폐기관리대장

정보시스템책임자	정보보호담당자	정보보호책임자

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

※ 출처: 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 보호대책, 책임소재 등에 대하여 계약서에 반영

② 계약서에 반영된 폐기 절차에 따라 이행되고 있는지 사진촬영, 실사 등의 이행 증적확인

◇ 정보시스템, PC 등 유지보수, 수리 과정에서 저장매체 교체, 복구 등 발생 시 저장 매체 내 정보를 보호하기 위한 대책을 마련하고 있는가?

→ 수리·교체 시 정보보호

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

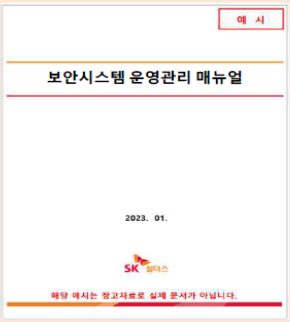
세부분야	2.10.1 보안시스템 운영
인증 기준	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립·이행하고 보안시스템별 정책적용 현황을 관리하여야 한다
주요 확인사항	• 조직에서 운영하고 있는 보안시스템에 대한 운영절차를 수립·이행하고 있는가? • 보안시스템 관리자 등 접근이 허용된 인원을 최소화하고 비인가자의 접근을 엄격하게 통제하고 있는가? • 보안시스템별로 정책의 신규 등록, 변경, 삭제 등을 위한 공식적인 절차를 수립·이행하고 있는가? • 보안시스템의 예외 정책 등록에 대하여 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 관련법령에서 정한 기능을 수행하는 보안시스템을 설치하여 운영하고 있는가?
기준 요약도	
운영 방안	◇ 조직에서 운영하고 있는 보안시스템에 대한 운영절차를 수립 · 이행하고 있는가?

→ 정보보안시스템 운영절차 수립

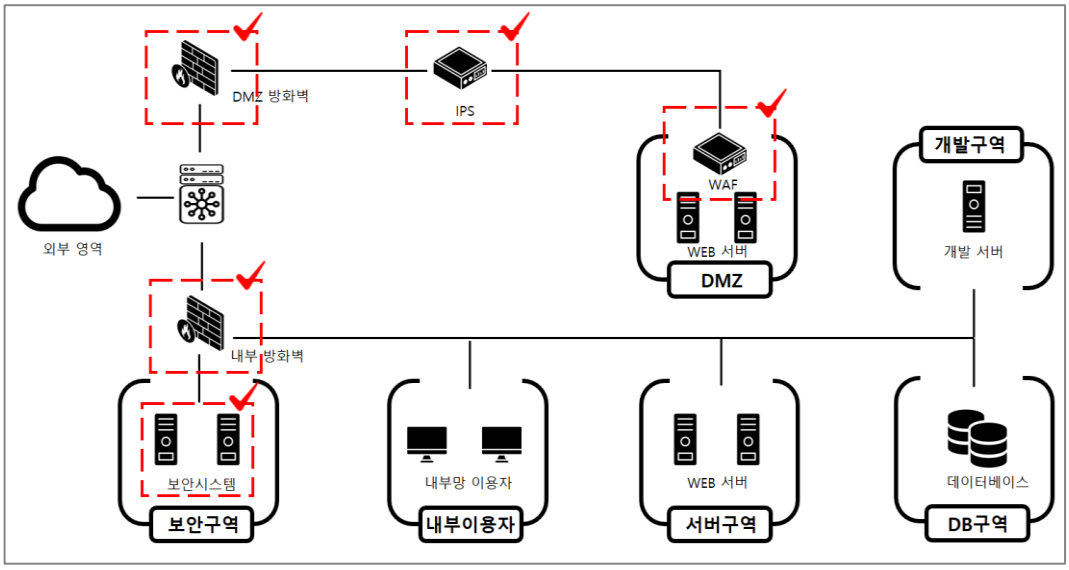
보안시스템 운영관리 매뉴얼

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	승 인
상신	정보보호 담당자	OOO	2022-12-20	-



방화벽	VPN	IPS / IDS	Anti Virus
스팸차단	Ddos	DRM	위·변조 방지



※ 출처: 정보보호 시스템운영관리(이해를 돕기위한 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 보호대책을 적용하여 보안시스템 관리자 등 접근이 허용된 인원 이외의 비인가자 접근을 엄격히 통제

② 주기적인 보안시스템 접속로그 분석을 통하여 비인가자에 의한 접근시도 여부

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

→ 보안시스템별 정책 변경 절차 수립 (F/W 예시)

「**정보시스템 운영관리지침**」 제 ○○조 (정보보호 시스템관리)

① 보안시스템운영자는 정책 변경 시 "방화벽 오픈 신청서"를 작성하여 정보보호담당자에게 승인을 득 한 후 정책을 적용 해야한다.

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

③ 보안시스템운영자는 침입차단 정책 현황을 '방화벽 정책관리대장'에 기록 해야하며, 분기별 1회 접근통제 정책을 검토 후 부서 정보보호담당자의 승인을 득해야한다.

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

보안시스템운영자	정보보호 담당자

구분	출발지 IP	목적지 IP	프로토콜	포트	신청기간	만료기간	신청 내용	적용 일시	작업자	삭제일시	작업자
신규	192.0.0.0	192.0.0.0	TCP	443	2023.01.01	2023.01.01	정보시스템 담당자 변경	2023.01.01	OOO	2023.01.01	OOO
삭제	...	...	...		...		...	...	...	...	...

※ 출처: 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 예외정책 만료 여부 및 예외 사용에 대한 모니터링 등

◇ 보안시스템에 설정된 정책의 타당성 여부를 주기적으로 검토하고 있는가?

→ 정보보호 시스템 주기적 검토

「**정보시스템 운영관리지침**」 제 ○○조 (정보보호 시스템관리)

① 정보보호 시스템운영자는 침입차단 정책 현황을 '방화벽 정책관리대장'에 기록해야하며, 분기별 1회 접근통제 정책을 검토 후 부서 정보보호담당자의 승인을 득해야한다.

방화벽 정책 점검 결과보고

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

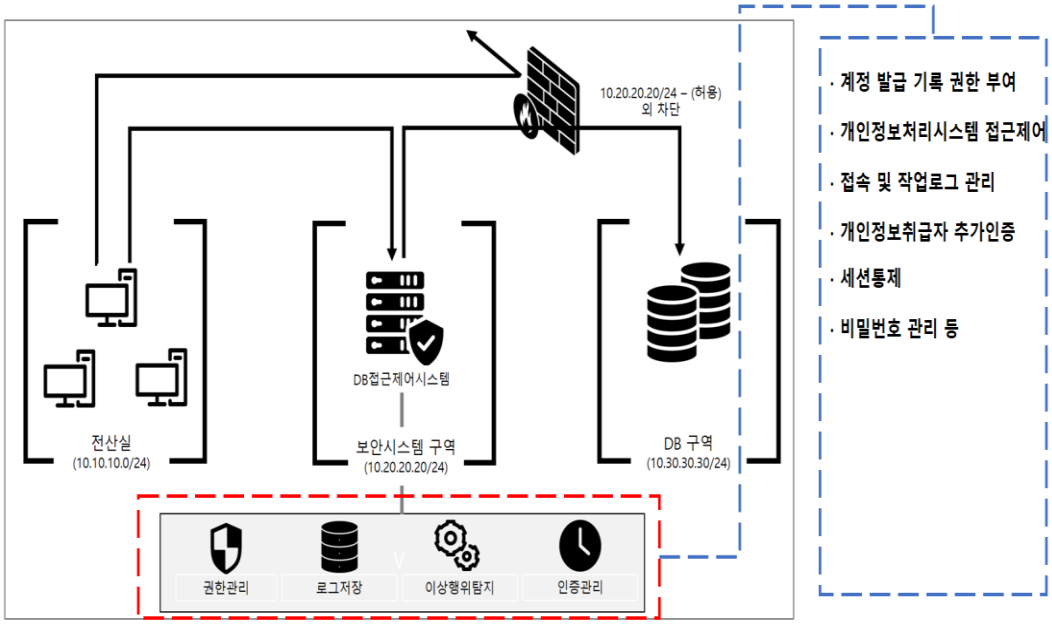
※ 출처: 방화벽 정책점검 결과보고(이해를 돕기 위한 예시)

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

→ 개인정보처리시스템 보안대책 운영

① 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한

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



※ 출처: 개인정보처리시스템 보안시스템 설치 운영(이해를 돕기 위한 예시)

2.10.2 클라우드 보안

<table>
<tr><th>세부분야</th><th>2.10.2 클라우드 보안</th></tr>
<tr><td>인증
기준</td><td>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 보호대책을 수립·이행하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 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, 설정오류 등을 방지할 수 있도록 보안 구성 및 설정 기준, 보안설정 변경 및 승인절차, 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 보호대책을 적용하고 있는가?
• 클라우드 서비스의 보안 설정 변경, 운영 현황 등을 모니터링하고 그 적절성을 정기적으로 검토하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 클라우드 서비스 제공자와 정보보호 및 개인정보보호에 대한 책임과 역할을 명확히 정의하고 이를 계약서(SLA 등)에 반영하고 있는가?

→ 클라우드 환경에서의 보안관리 책임
① 제공자: 클라우드컴퓨팅서비스의 기능과 그 기능을 제공하기 위해서 필요한</td></tr>
</table>

하드웨어 및 소프트웨어 등의 보안관리 수행

② 이용자: 계정관리 및 서비스 이용에 따른 사용자 설정 등에 대한 보안관리수행

〈클라우드 환경에서의 보안 관리 책임 주체〉

구분	물리 인프라 (서버, 네트워크)	하이퍼바이저 (운영 시스템)	가상머신	운영체제 (OS)	소프트웨어 (WEB,WAS)	인터페이스 (API,GUI)	데이터 (Data)
기존환경	이용자	–	–	이용자	이용자	이용자	이용자
IaaS	제공자	제공자	제공자	제공자/ 이용자	이용자	이용자	이용자
PaaS	제공자	제공자	제공자	제공자	제공자/ 이용자	이용자	이용자
SaaS	제공자	제공자	제공자	제공자	제공자	제공자/ 이용자	제공자/ 이용자

※ 클라우드컴퓨팅서비스 세부 특성에 따라 상이할 수 있음

※ 출처: 클라우드컴퓨팅 이용자 보호 길라잡이(NIPA)

→ **계약서 또는 서비스수준협약서(SLA) 반영**

① 책임 대한 내용을 계약서 또는 서비스수준협약서(SLA)에 상세 기록하고 해당 내용을 명시

클라우드컴퓨팅서비스 제공자와 이용자 간 표준계약서

제1장 총칙

제1조(목적) 이 계약서는 (_____)(이하 "회사")가 제공하는 클라우드컴퓨팅서비스 및 부가서비스의 이용과 관련하여, 회사와 클라우드컴퓨팅서비스를 소비 목적으로 이용하고자 하는 자(이하 "이용자") 간의 계약관계에서 발생하는 권리와 의무, 그 밖에 필요한 기본적인 사항을 규정함을 목적으로 한다.

제2조(정의) 이 계약서에서 사용하는 용어의 정의는 아래와 같다.

1. "클라우드컴퓨팅"이라 함은 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조 제1호에 따라 집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신축적으로 이용할 수 있도록 하는 정보처리체계를 말한다.
2. "클라우드컴퓨팅서비스"라 함은 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조 제3호에 따라 클라우드컴퓨팅을 활용하여 상용(商用)으로 타인에게 정보통신자원을 제공하는 서비스를 말한다.
3. "회사"라 함은 클라우드컴퓨팅서비스 및 부가서비스를 제공하는 사업자를 말한다.
4. "이용자"라 함은 회사와 클라우드컴퓨팅서비스 이용계약을 체결한 자로서, 회사가 제공하는 클라우드컴퓨팅서비스 및 부가서비스를 최종적으로 이용하는 고객을 말한다.
5. "이용자 정보"라 함은 이용자가 회사의 정보통신자원에 저장하는 정보(「국가정보화 기본법」 제3조 제1호에 따른 정보, 개인의 경우에는 개인정보와 신용정보를 포함한다.)로서 이용자가 소유 또는 관리하는 정보를 말한다.

제3조(계약서의 명시와 개정) ① 회사는 이 계약서의 내용을 이용자가 알 수 있도록 클라우드컴퓨팅서비스(이하 "서비스") 홈페이지(_____)에 게시하거나 그밖에 이용자가 쉽게 확인할 수 있는 방법으로 알려야 한다.

② 회사는 이용자가 회사와 이 계약서의 내용에 관하여 질의 및 응답을 할 수 있도록 적절한 절차를 마련하여야 한다.

③ 회사가 이 계약서를 개정할 경우에는 이용자가 알기 쉽도록 적용일자, 개정사유, 개정 전후의 내용 등을 명시하여 현행 계약서와 함께 그 적용일로부터 최소 7일 전부터 적용일 전일까지 서비스의 초기 화면 및 회사의 서비스 홈페이지에 게시하여 알려야 한다. 다만, 계약서의 개정내용이 이용자에게 불리하거나 중대한 사항의 변경은 최소 30일 전부터 전화, 휴대전화, 우편, 전자우편 또는 문자메시지 등으로 알려야 하며, 이용자에게 불리

제7장 손해배상 등

제22조(손해배상) ① 회사가 고의 또는 과실로 이용자에게 손해를 발생시킨 경우에는 손해를 배상하여야 한다.

② 회사는 고의 또는 과실로 이용자가 서비스를 일시 이용하지 못하는 경우에 회사가 미리 정한 서비스장애 운영지침에 따라 손해를 산출하여 이용자에게 통지한다.

③ 이용자가 고의 또는 과실로 회사에 손해를 발생시킨 경우에는 그 손해를 배상하여야 한다.

제23조(면책) ① 회사는 다음 각 호의 사유로 인하여 발생한 손해에 대하여는 책임이 면제된다.

1. 제15조(서비스의 중단) 제1항 각 호의 사유로 서비스 점검이 불가피하여 같은 조 제2항에서 정하는 절차에 따라 사전에 알린 경우로써 회사의 고의 또는 과실이 없는 경우
2. 천재지변, 전쟁·내란·폭동 등 비상사태, 현재의 기술수준으로는 해결이 불가능한 기술적 결함 그밖에 불가항력에 의하여 서비스를 제공할 수 없는 경우
3. 이용자의 고의 또는 과실로 인한 서비스의 중단, 장애 및 계약 해지의 경우
4. 기간통신사업자가 전기통신서비스를 중지하거나 정상적으로 제공하지 아니하여 이용자에게 손해가 발생한데 대하여 회사의 고의 또는 과실이 없는 경우
5. 이용자의 컴퓨터 환경으로 인하여 발생한 부가적인 문제 또는 회사의 고의 또는 과실이 없는 네트워크 환경으로 인하여 부가적인 문제가 발생한 경우
6. 이용자의 컴퓨터 오류로 인하여 손해가 발생한 경우 또는 신상정보 및 전자우편 주소를 부정확하게 기재하거나 기재하지 아니하여 손해가 발생한데 대하여 회사의 고의 또는 과실이 없는 경우

② 회사는 이용자 또는 제3자가 서비스 내 또는 서비스 홈페이지에 게시 또는 전송한 정보, 자료, 사실의 신뢰도, 정확성 등의 내용에 대하여 회사의 고의 또는 과실이 없는 한 책임이 면제된다.

③ 회사는 이용자 상호간 또는 이용자와 제3자 간에 서비스를 매개로 발생한 분쟁에 대하여 다음 각 호의 요건을 모두 갖춘 경우에 이로 인한 손해를 배상할 책임이 없다.

※ 출처 클라우드컴퓨팅서비스 표준계약서 (과학기술정보통신부)

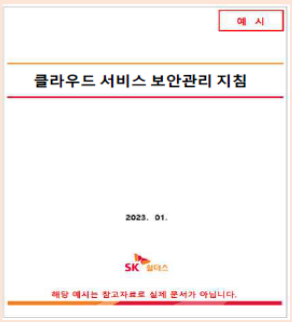
※ 출처: 행정공공기관 클라우드컴퓨팅서비스 이용안내서 (행정안전부·NIA)

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

→ 클라우드 서비스 보안통제 정책 수립

클라우드 서비스 보안관리 지침

순번	내용
1	보안 관리 관련 역할 및 책임
2	사설 네트워크 보안 구성 및 접근통제
3	클라우드 서비스 관리자 계정 및 권한 관리
4	클라우드 서비스 관리자에 대한 강화된 인증
5	보안 설정 기준
6	보안 설정 등록·변경·삭제 절차
7	보안 구성 및 설정에 대한 적절성 검토
8	클라우드 서비스 원격접속 경로 및 방법
9	클라우드 서비스 보안 관제 및 알람·모니터링 방안
10	보안감사 절차



※ 클라우드보안관리지침 (이해를 돕기 위한 예시)

「**클라우드서비스 운영지침**」 제 ○○조 (역할 및 책임)

① 클라우드 서비스 관리자는 운영 및 보안관리 업무를 총괄·감독하며 규정 및 지침에 따른 보안관리를 수행한다.

② 클라우드 서비스 관리자 권한을 각호와 같이 세분화한다.

≫ 보안관리자: 보안그룹 규칙 생성·수정·삭제

≫ 개발자: 개발 인스턴스 시작 · 중지 · 종료 권한

≫ 운영자: 프로덕션 시작·중지·종료 권한

≫ 계정 관리자: 사용자 추가·삭제

「**클라우드서비스 운영지침**」 제 ○○조 (접근통제)

① 클라우드 관리자 권한 접속 시 ID/PW 외 강화된 인증 수단(OTP, SMS, 바이오인증 등)을 사용해야 한다.

② Access Key 사용은 원칙적으로 금지하며, API 연동 등으로 Access Key를 사용해야 하는 경우에는 각 부서 정보보호담당자에 승인을 득한 후 key 관리방안 수립 및 안전한 장소 보관을 해야한다.

◇ 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 보호대책을 적용하고 있는가?

→ 클라우드 접근 권한 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?

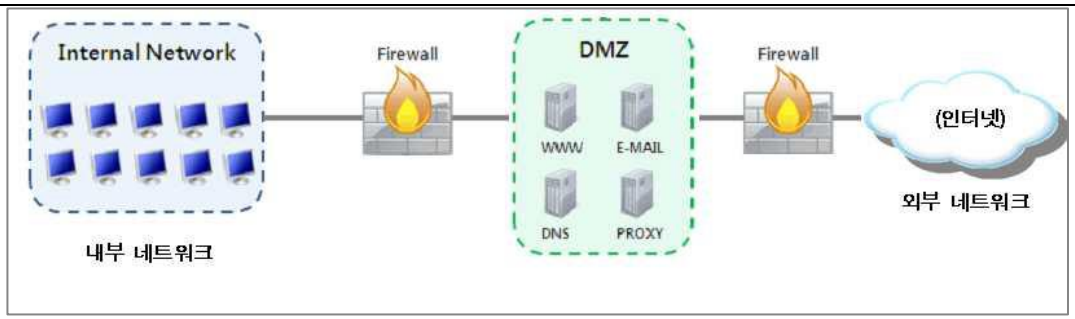
→ 클라우드 운영현황 정기적 검토

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

② 클라우드 서비스 보안설정의 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 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 공개서버를 운영하는 경우 이에 대한 보호대책을 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 게시절차를 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 보호대책을 수립·이행하고 있는가? → 공개서버 보호대책을 수립 (예시) 「정보시스템 운영관리 지침」 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 각호의 보안조치를 적용해야한다.

≫ 웹서버를 통한 개인정보 송수신 시 SSL/TLS인증서

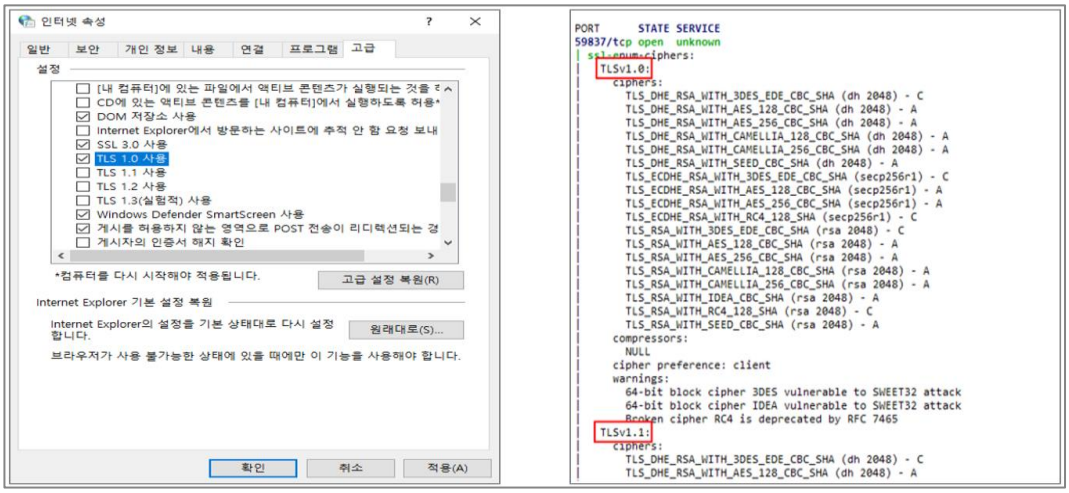
≫ 백신설치 및 업데이트 설정

≫ 응용프로그램(웹서버, OpenSSL 등), 운영체제 등에 대한 최신 보안패치 설치

≫ 불필요한 서비스 제거 및 포트 차단

≫ 에러 처리 페이지, 테스트 페이지 등 불필요한 페이지 노출 금지

≫ 주기적 취약점 점검 수행



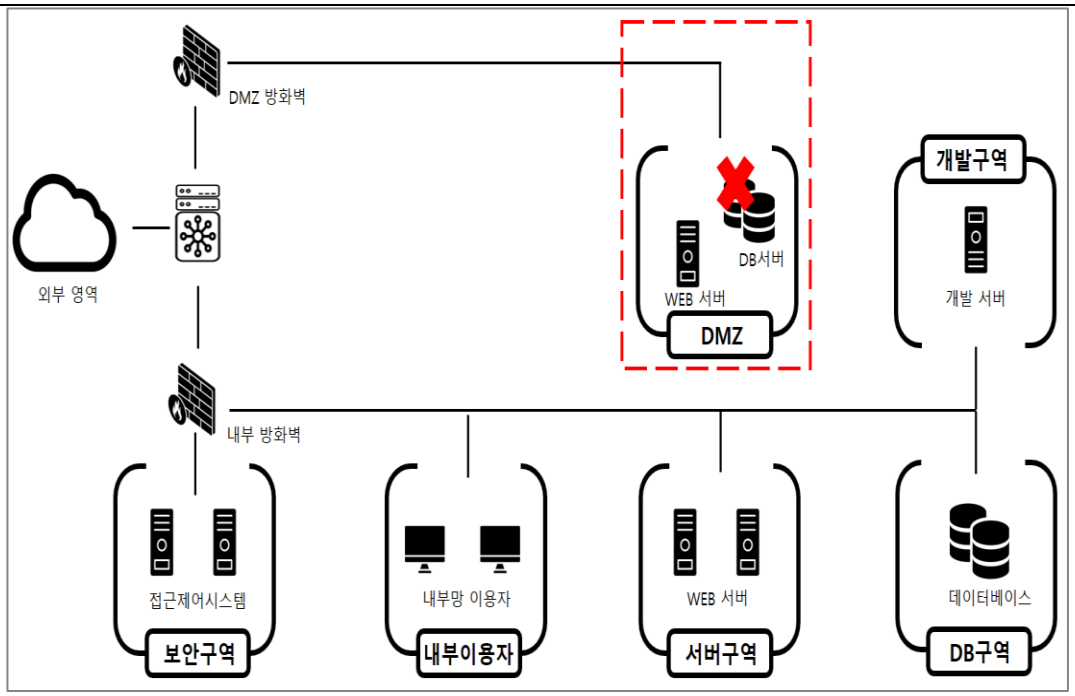
※ 출처: 전송구간 암호화 조치 확인(이해를 돕기 위한 예시)

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

→ 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 게시절차를 수립·이행하고 있는가?

→ 개인정보 및 중요정보를 게시 절차 수립

「**서버보안 지침**」 제 ○○조 (게시자료 보안관리)

① 개인정보 및 중요 업무자료를 저장할 경우 '홈페이지 자료등록 신청서'를 작성하여 정보보호책임자의 승인을 득한 후 게시해야 한다.

홈페이지 자료등록 신청서

신청 부서	
담당자	(인)
부서장	(인)

신청 부서			
신 청 자		연락처	
등록자료 위치		분량	페이지
등록자료 제목			
첨부 파일			

등록 자료 내용 요약	
희망 등록일	
등록 처리일	

※ 등록 자료 상세내용 및 첨부파일은 메일 전송
※ 등록처리 내용은 정보보안 담당부서에서 기록 관리

보안 부서	
보안관리자	(인)
보안책임자	(인)

※ 홈페이지 자료등록 신청서(이해를 돕기 위한 예시)

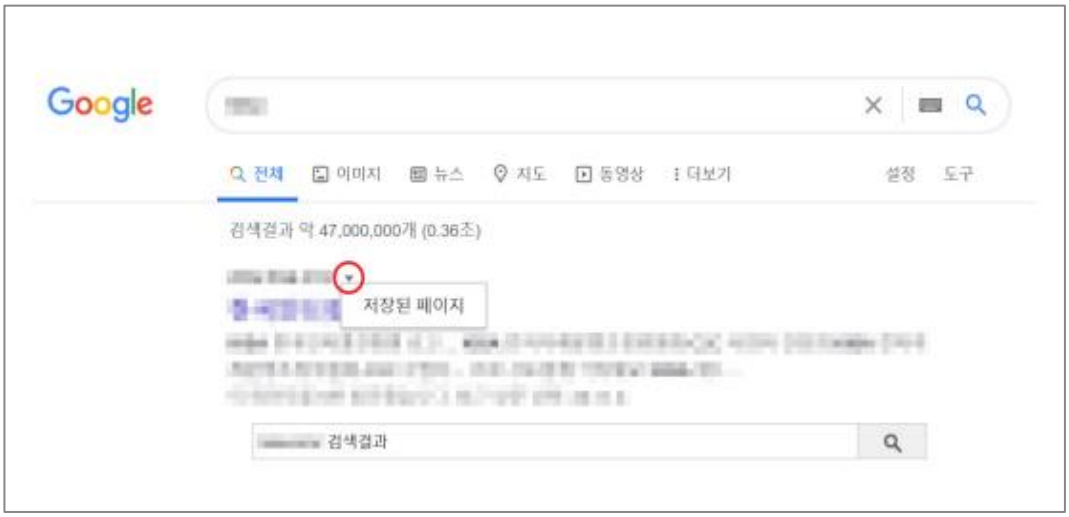
◇ 조직의 중요정보가 웹사이트 및 웹서버를 통하여 노출되고 있는지 여부를 주기적으로 확인하여 중요정보 노출을 인지한 경우 이를 즉시 차단하는 등의 조치를 취하고 있는가?

→ 개인정보 및 중요정보 노출 점검

① 검색엔진 등을 통하여 주기적으로 점검 및 필요한 조치 적용

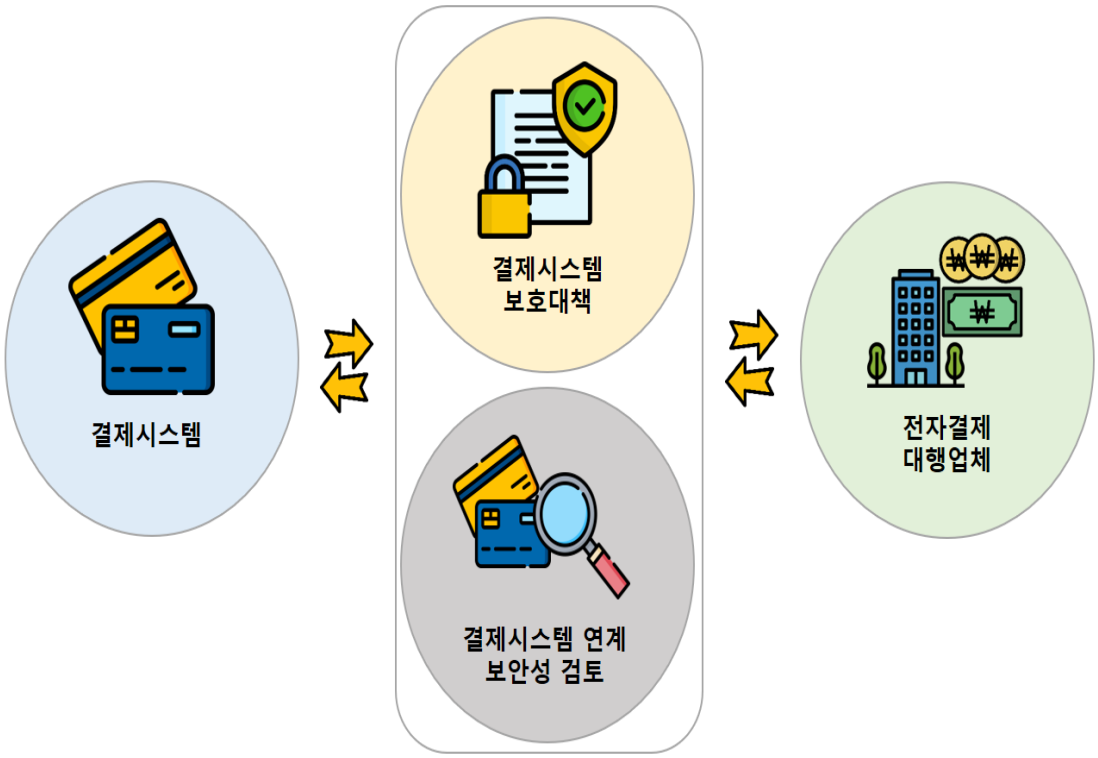
② 공개 웹 상에 개인정보 또는 내부 중요정보 게시 유무 정기적 점검 실시

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 정보유출이나 데이터 조작·사기 등의 침해사고 예방을 위하여 인증·암호화 등의 보호대책을 수립하고, 결제시스템 등 외부 시스템과 연계할 경우 안전성을 점검하여야 한다.
주요 확인사항	• 전자거래 및 핀테크 서비스를 제공하는 경우 거래의 안전성과 신뢰성 확보를 위한 보호대책을 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 보호대책을 수립·이행하고 있는가?** **→ 핀테크 서비스를 제공자 보호대책 수립** ① 영역별 발생 가능한 주요 위험 및 보안 대책 도출 ② 이용기관은 자체적으로 보안점검 항목을 구현 및 점검

위협	설명/영향	보안 대책(예시)
오픈API 관련 정보처리시스템의 악성코드 감염	대량의 이용자 데이터 및 인증정보가 침해되거나 부정행위 발생 가능	(이용기관) - 오픈API 관련 정보처리시스템에 대한 악성코드 감염 방지 대책 마련 및 적용 (운영기관) - 고위험 금융거래 요청에 대한 OOB인증/인가 시도 - 이상거래 모니터링
정상적으로 획득한 계좌정보의 침해	API를 통해 정상적인 방법으로 획득한 계좌정보가 이용기관 시스템에 저장된 이후 침해될 위험	(이용기관) - API를 통해 획득한 이용자의 계좌 관련 정보를 안전하게 보호하기 위한 대책 마련 및 적용
API 데이터를 제3자에 제공하는 이용기관에 대한 관리 미흡	이용기관이 보안 수준이 검증되지 않은 제3의 주체에 API 데이터를 제공하는 경우, 고객정보의 침해 위험이 증가하며, 고객정보가 침해되거나 부정행위가 발생 시 책임 소재가 모호할 수 있음	(이용기관) - 이용기관으로부터 데이터를 전달받는 제3의 주체에 대해 데이터 보호 역량 확인 및 계약 시 사고에 대한 책임을 계약서에 명시 (운영기관) - 제3자에 API 데이터를 전달하는 방법을 관리하는 규칙을 포함하여, 전달 체인에 참여하는 당사자들의 보안 요구사항을 명확히 함 - 보안 점검을 받지 않거나 인가되지 않은 주체가 API를 통해 획득한 데이터를 처리하지 않도록 관리
이용기관 시스템의 침해로 인한 오픈API 접근키의 대규모 도난 발생	오픈API 접근키는 데이터와 서비스에 접근하는 핵심 데이터로, 유출시 고객 데이터의 대규모 침해와 부정사용 발생이 가능	(이용기관) - 시스템이 비인가 접근으로부터 보호되도록 보안 표준 적용 - 오픈API 접근키를 보호하기 위한 대책(예: 암호화 저장 등) 적용 (운영기관) - 고위험 거래 API에 대해서는 가급적 유효기간이 짧은 접근키를 부여 - 탈취된 접근키의 악용을 막기 위해 기술적 대책을 적용 (예: IP화이트리스트, TLS 상호 인증을 통한 이용기관 오픈API 접근서버 인증)

위협	설명/영향	보안 대책(예시)
이용기관을 사회공학적 공격 대상으로 선택	공격자는 이용자의 계좌정보 등을 얻기 위해 이용기관을 대상으로 사회공학적 공격을 실행할 수 있으며(예: 비밀번호 초기화 요청), 이를 통해 고객 정보의 침해 및 부정행위 발생 가능	(이용기관) - 이용기관 고객 서비스 담당 직원을 대상으로 사회공학적 공격 관련 교육 - 고객 서비스 지원 과정에서 견고한 이용자 인증을 요구
오픈API 이용 애플리케이션 침해/오류로 인한 비정상적 API요청	오픈API를 이용하는 애플리케이션이 침해되거나 오류가 발생하여 계획되지 않은 동작을 할 경우 운영기관 시스템에 악영향을 미칠 수 있음	(이용기관) - 오픈API 이용 애플리케이션에 대한 위변조 방지, 접근통제, 변경관리 등 통제 대책 마련 - 이상행위 모니터링 (운영기관) - 과도한 API요청 등 이상행위 모니터링

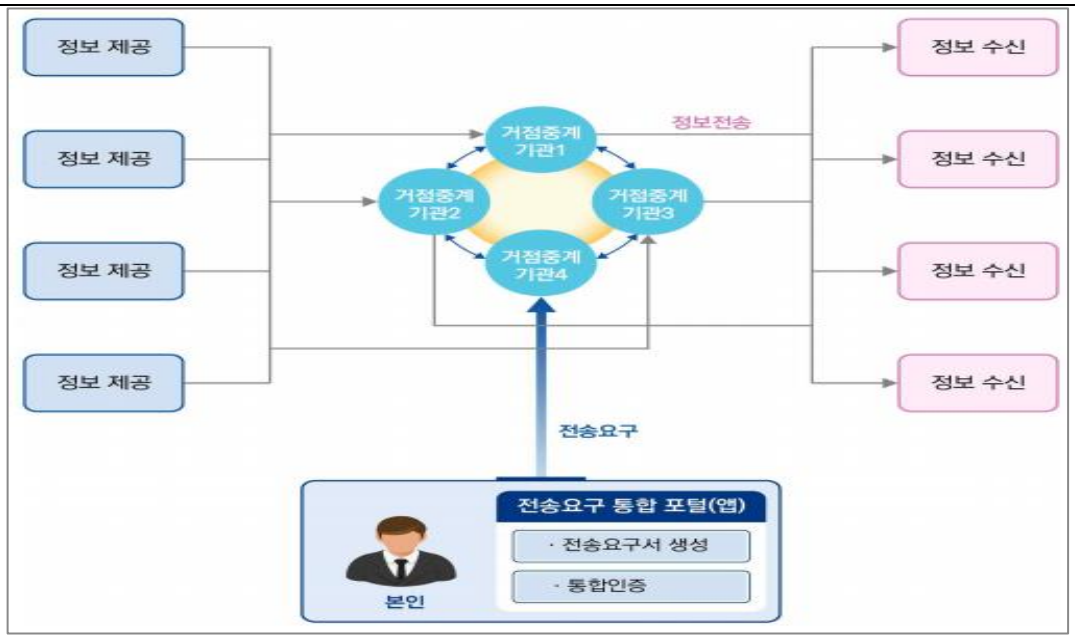
※ 출처: 금융권 오픈api 이용기관 자체 보안점검 가이드(금융보안원)

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

→ 시스템 연계 보호대책 수립

「**정보시스템 운영관리 지침**」제 ○○조 (업무망 보안관리)

① 업무망을 다른 시스템 및 인터넷과 연계할 경우 보안대책을 마련하고 보안성검토를 실시 해야한다.



※ 출처: 금융분야 마이데이터 서비스 가이드라인(금융위원회·한국신용정보원)

2.10.5 정보전송 보안

<table>
<tr><th>세부분야</th><th>2.10.5 정보전송 보안</th></tr>
<tr><td>인증
기준</td><td>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</td></tr>
<tr><td>주요
확인사항</td><td>• 외부 조직에 개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립하고 있는가?
• 업무상 조직 간 개인정보 및 중요정보를 상호교환하는 경우 안전한 전송을 위한 협약 체결 등 보호대책을 수립·이행하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 외부 조직에 개인정보 및 중요정보를 전송할 경우 안전한 전송 정책을 수립하고 있는가?

→ 전송 정책 수립

「정보시스템 운영관리 지침」 제 ○○조 (정보전송 보안)
① 외부기관에 개인정보 등 중요정보를 전송할 경우 안전한 전송을 위한 협약을 체결하고 이행하여야 한다.
≫ 업무정의: 개인정보 제3자 제공, 신용카드결제 정보 전달 등
≫ 범위정의: 필요 최소한의 정보 송 수신</td></tr>
</table>

≫ 기술표준: 암호화 방식, 키 교환 및 관리, 연계 및 통신 방식 등

≫ 검토절차: 보고 및 승인, 관련 조직간 역할 및 책임, 보안성 검토 등

≫ 협약기준: 보안약정서, 계약서, 부속합의서, SLA 등

≫ 법적 요구사항을 반영한 보호조치: 전송·저장·파기 시 기술적 보호대책 등

≫ 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 상호교환하는 경우 안전한 전송을 위한 협약체결 등 보호대책을 수립·이행하고 있는가?

→ 조직 간 상호교환 보호대책 수립 이행

① 조직 또는 계열사 간 다음과 같은 업무수행을 위하여 중요정보를 전자적으로 상호교환하는 경우 안전한 전송을 위한 협약을 체결하고 이에 따라 이행.

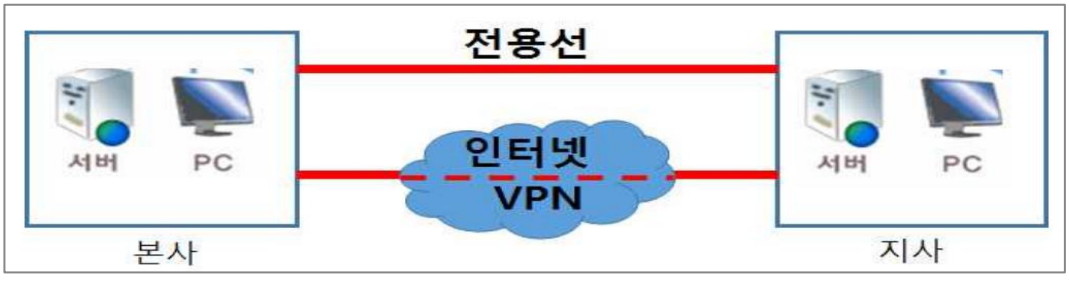
≫ 관련 업무 정의: DM 발송을 위한 개인정보 DM업체 전달, 채권추심업체에 추심정보 전달, 개인정보 제3자 제공, 신용카드결제 정보 VAN 전달 등

≫ 정보전송 범위 정의: 법규 준수 또는 정보유출 위험을 예방하기 위하여 업무상 필요한 최소한의 정보만을 송수신

≫ 담당자 및 책임자 지정

≫ 정보 전송 기술 표준 정의

≫ 정보 전송, 저장, 파기 시 관리적·기술적·물리적 보호대책 등



※ 출처: 개인정보 안전성 확보조치(개인정보보호 위원회·KISA)

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 보안설정 등의 접근통제 대책을 수립하고 주기적으로 점검하여야 한다.
주요 확인사항	• PC, 노트북, 가상PC, 태블릿 등 업무에 사용되는 단말기에 대하여 기기인증, 승인, 접근범위 설정, 기기 보안설정 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 보안설정 등의 보안 통제 정책을 수립·이행하고 있는가? → 업무용 단말기기 보안 정책 수립 (예시)

「**업무용 단말보안 매뉴얼**」 제 ○○조 (업무용 단말기 관리)

비인가자가 단말기(PC. 노트북. 스마트폰 등) 무단으로 조작하여 전산자료를 절취, 위. 변조 및 훼손하지 못하도록 보안대책을 시행하도록 하여야 한다.

① 업무용 단말기 허용기준

② 업무용 단말기 통한 업무 사용범위

③ 업무용 단말기 사용 시 승인 절차 및 방법

≫ PC등 단말기의 비밀번호, IP등을 단말기취급자관리대장을 작성· 운용 관리하도록 한다.

④ 업무망 연결 시 인증 방안: 기기인증, MAC 인증 등

⑤ 백신 설치, 보안프로그램 설치 등 업무용 단말기 사용에 따른 보안 설정 정책

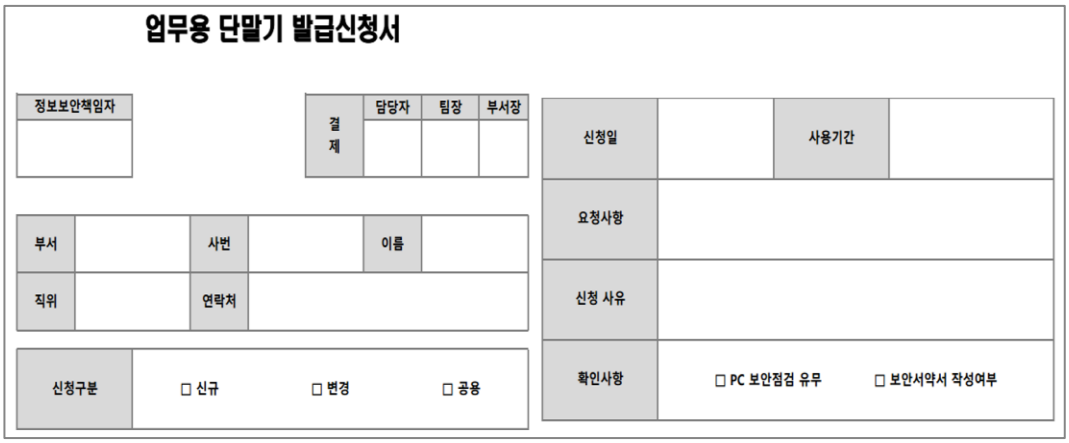
≫ 모든 사용자가 단말기 보안 관리를 위해 보안프로그램 설치·운용 해야한다.

→ 바이러스 방역 에이전트 및 백신프로그램

→ 개인정보 유출 방지 시스템

→ 매체제어 시스템

⑥ 업무용 단말기 사용에 따른 보안 설정 정책 및 오·남용 모니터링 대책 등



업무용 단말기 발급신청서

정보보안책임자		결제	담당자	팀장	부서장

부서		사번		이름	
직위		연락처			

신청구분	□ 신규	□ 변경	□ 공용

신청일		사용기간	
요청사항			
신청 사유			
확인사항	□ PC 보안점검 유무	□ 보안서약서 작성여부	

※ 업무용 단말기 발급신청서 (이해를 돕기위한 예시)

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

→ 무형 단말기 보안정책 수립(예시)

「**업무용 단말관리 매뉴얼**」 제 ○○조 (공유폴더 관리)

① 공유폴더는 사용하지 않는 것을 원칙으로 하나, 업무 목적으로 불가피한 경우 보안설정을 적용해야 한다.

≫ 파일공유 기능 비밀번호설정

≫ 사용 후 공유폴더 삭제

≫ 읽기 쓰기 권한 개별 설정

≫ 최소한의 파일공유 등

② 공유폴더의 별도관리 통제를 해야하며 공유폴더관리대장에 기록 관리해야한다.

공유폴더 관리대장

순번	소속	관리자	단말형태 (PC구분)	자산번호	사용자	비밀번호 설정유무	시작일	종료일	사용목적	비고
1										
2										
3										
4										
5										

※ 공유폴더 관리대장(이해를 돕기 위한 예시)

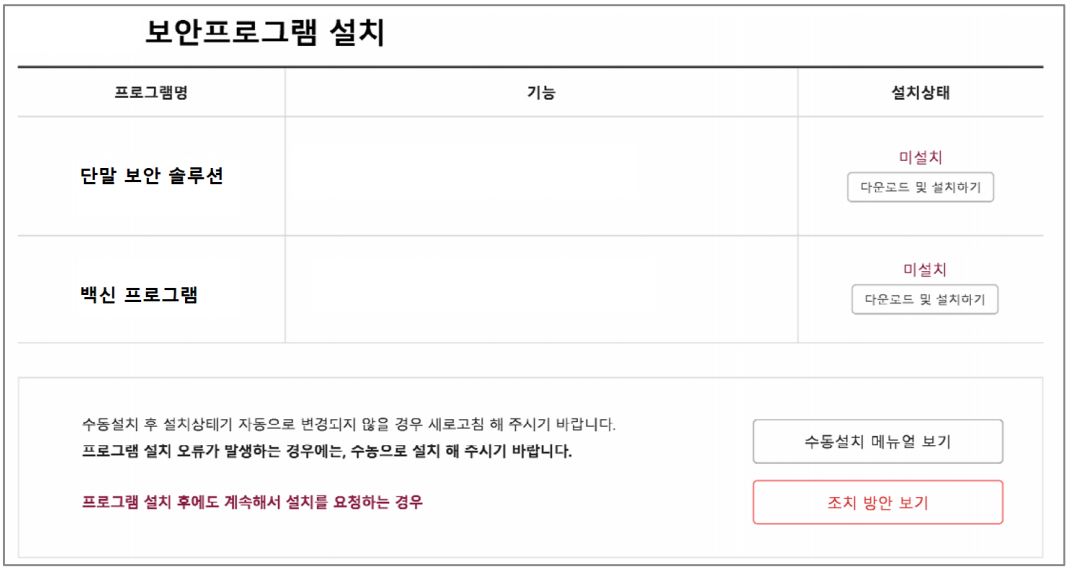
◇ 업무용 모바일 기기의 분실, 도난 등으로 인한 개인정보 및 중요정보의 유·노출을 방지하기 위하여 보안대책을 적용하고 있는가?

→ 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 보안프로그램설치 (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 보안설정 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?** **→ 보조저장매체 관리 절차(일부 예시)** 「**휴대용 저장매체 관리 매뉴얼**」 제 ○○조 (보조저장매체 관리)

① 보조저장매체 보유 현황 관리 방안

≫ 정보보호 담당자는 보조기억매체의 등록 및 불용처리 등에 관한 기록을 보조기억매체 관리대장에 기록관리하여야 한다.

≫ 부서 정보보호책임자는 월1회 이상 보조기억매체 수량 및 보관상태를 점검하고 정보보호 담당자에게 승인을 득해야한다.

② 보조저장매체 사용허가 및 등록 절차

③ 보조저장매체 반출·입 관리 절차

≫ 관리책임자는 휴대용 저장매체의 반·출입을 통제하여야 하며 보조기억매체 반출입관리대장에 기록관리 해야한다.

④ 보조저장매체 폐기 및 재사용 절차

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

보조저장매체 보호대책 등

보조저장매체 관리 대장

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

※ 보조기억매체 관리대장 (이해를 돕기 위한 예시)

◇ 보조저장매체 보유현황, 사용 및 관리실태를 주기적으로 점검하고 있는가?

→ 보조저장매체 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		

※ 보조기억매체 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 보호대책 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 보호대책을 마련하고 있는가?
기준 요약도	❶ 패치적용대상 ❷ 패치 주기 ❸ 패치 배포 전 사전 검토절차 ❹ 긴급 패치 적용절차 ❺ 패치 미적용 시 보안성 검토 ❻ 패치 담당자 및 밴더사 정보 패치관리 절차서 주요자산 현황관리 패치 미적용 자산 보완대책 주요시스템 공개망 패치제한 패치관리시스템 보안대책 수립
운영 방안	◇ 서버, 네트워크시스템, 보안시스템, PC 등 자산별 특성 및 중요도에 따라 운영체제(OS)와 소프트웨어의 패치관리 정책 및 절차를 수립·이행하고 있는가? → 자산별 패치관리 절차 수립 「정보보호시스템 운영관리 지침」 제 ○○조 (패치관리)

① 보안패치는 각종 소프트웨어, 운영체제 등에서 발견되는 보안상의 취약성을 보완해주는 프로그램으로 새로운 취약성에 대한 보안패치가 발표되는 즉시 시스템에 적용한다. 다만, 서비스 영향도 등에 따라 최신 패치 적용이 어려운 경우 각 호에 따라 보안대책을 마련한다.

≫ 운영시스템의 경우 시스템 가용성에 영향이 미칠 수 있으므로 영향도 분석 후 패치

≫ 운영환경에 따라 패치 적용이 어려운 경우 그 사유와 추가 보안대책을 마련하여 정보시스템 책임자에게 보고하고 그 현황을 관리한다.

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

→ 패치관리시스템(PMS) 보안

「정보보호시스템 운영관리 지침」 제 ○○조 (패치관리)

① 서버의 OS 및 소프트웨어 패치 적용현황을 '패치관리대장'에 기록하고, 서버관리자는 최신 보안패치 여부를 반기 1 회 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 작성 예시)

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

→ 서비스 중요도에 따른 보안대책 적용

① 운영시스템에 패치를 적용하는 경우 시스템 가용성에 영향을 미칠 수 있으므로 운영시스템의 중요도와 특성을 고려하여 영향도 분석 등 정해진 절차에 따라

분하게 영향을 분석한 후 적용

② 운영환경에 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 제한하여야 한다.

≫ 불가피한 경우 사전 위험분석을 통하여 보호대책을 마련하여 책임자 승인 적용

◇ 패치관리시스템을 활용하는 경우 접근통제 등 충분한 보호대책을 마련하고 있는가?

→ 패치관리시스템 보호대책 수립

「**정보보호시스템 관리지침**」 제 ○○조 (패치관리)

① 패치관리시스템(PMS) 활용 시 다음 각 호의 보호대책을 마련해야한다.

≫ 패치관리시스템에 대한 안전성 확보 조치(접근제어, 보안 취약점 제거 등

≫ 업데이트 파일 배포 시 파일 무결성 검사

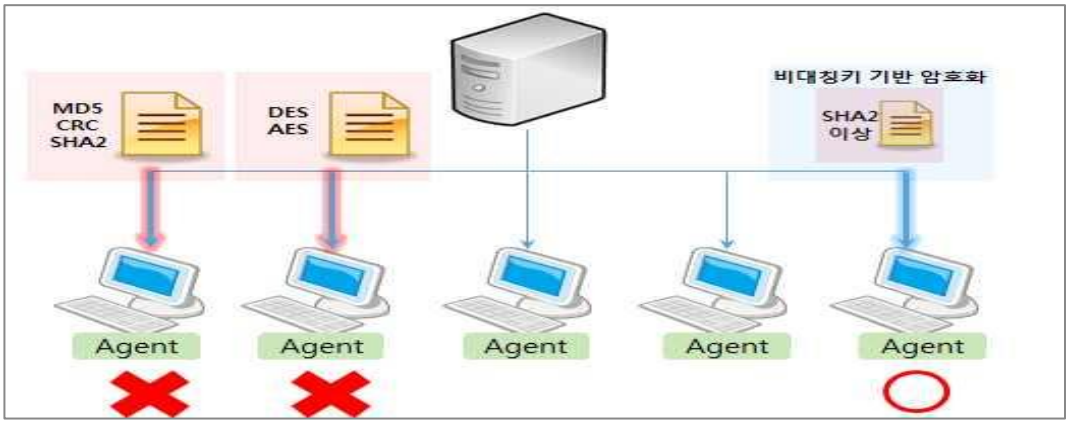
중앙관리소프트웨어 보안

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

관리프로그램 보안

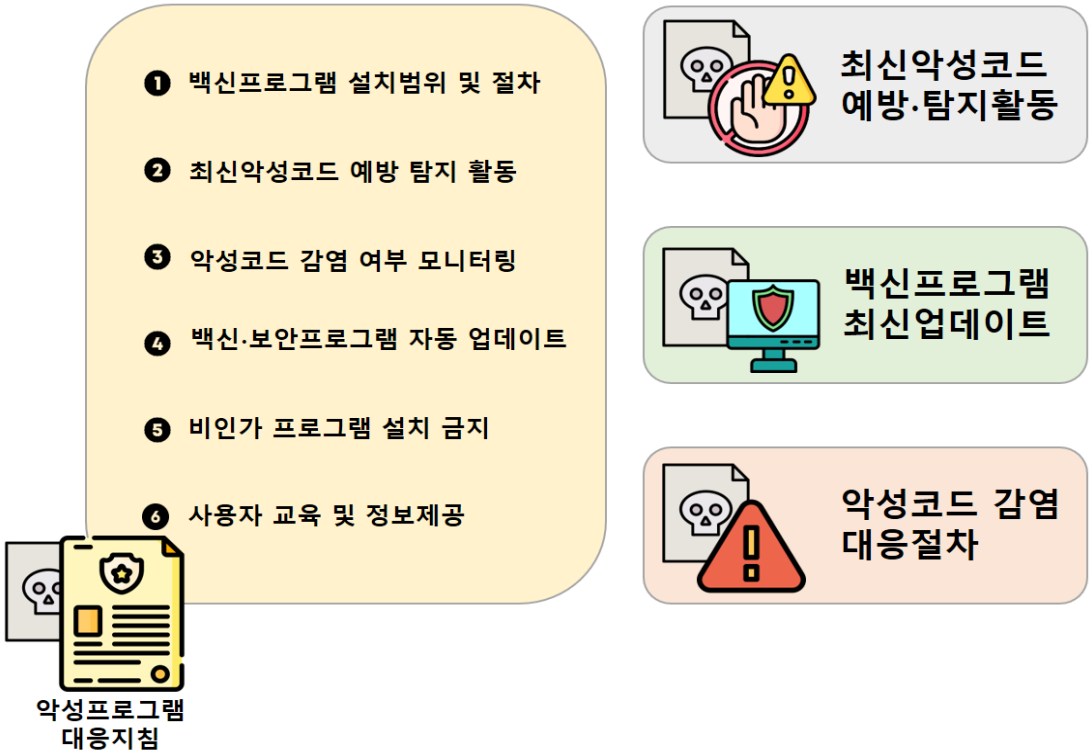
- o **(계정 관리)** 개발사에서 관리 목적으로 만든 불필요한 계정이 없어야 한다.
- o **(패스워드 관리)** 관리자 계정 생성 시 비밀번호 복잡도(2조합 10글자 또는 3조합 8글자)를 만족하도록 설정해야 하며, 최초 설치 시 사용자에게 패스워드를 설정하도록 유도해야 한다.
- o **(접근통제)** 접근 가능한 관리자 IP 지정 등을 통한 중앙 관리 프로그램에 대한 접근 통제 기능을 제공해야 한다.
- o **(세션 타임 아웃 설정)** 관리 프로그램을 일정 시간 동안 사용하지 않을 경우, 로그아웃 되도록 세션 타임아웃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

※ 출처: 중앙 관리형 소프트웨어 보안가이드(KISA)



※ 출처: 중앙 관리형 소프트웨어 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 보호대책을 수립·이행하여야 한다
주요 확인사항	• 바이러스, 웜, 트로이목마, 랜섬웨어 등의 악성코드로부터 정보시스템 및 업무용 단말기 등을 보호하기 위하여 보호대책을 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 대응절차를 수립·이행하고 있는가?
기준 요약도	
운영 방안	◇ 바이러스, 웜, 트로이목마, 랜섬웨어 등의 악성코드로부터 정보시스템 및 업무용 단말기 등을 보호하기 위하여 보호대책을 수립·이행하고 있는가? → 악성코드 보호대책 수립 「정보보호시스템 운영관리 지침」 제 ○○조 (악성코드 관리) ① 모든 PC·노트북은 사내 백신프로그램을 설치하여야 한다.

② 백신프로그램은 항상 최신 버전으로 업데이트하여 해야하며, 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 설치 금지한다.

→ 백신프그램 설치 및 사용 방법 고지

① 사내 정보보안 포털 접속

② 정보보안포털 → 보안프로그램 자료실 → 백신프로그램 설치파일 다운로드

③ 다운로드 받은 설치파일 관리자 권한으로 실행

④ 바탕화면에 백신프로그램 아이콘 생성·실행

◇ 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 소프트웨어 정책 수립 관리

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

③ 접근통제, 배포 파일에 대한 무결성 검증 등 보호대책 마련

◇ 악성코드 감염 발견 시 악성코드 확산 및 피해 최소화 등의 대응절차를 수립·이행하고 있는가?

→ 악성코드 감염 대응절차

「침해사고 대응 매뉴얼」

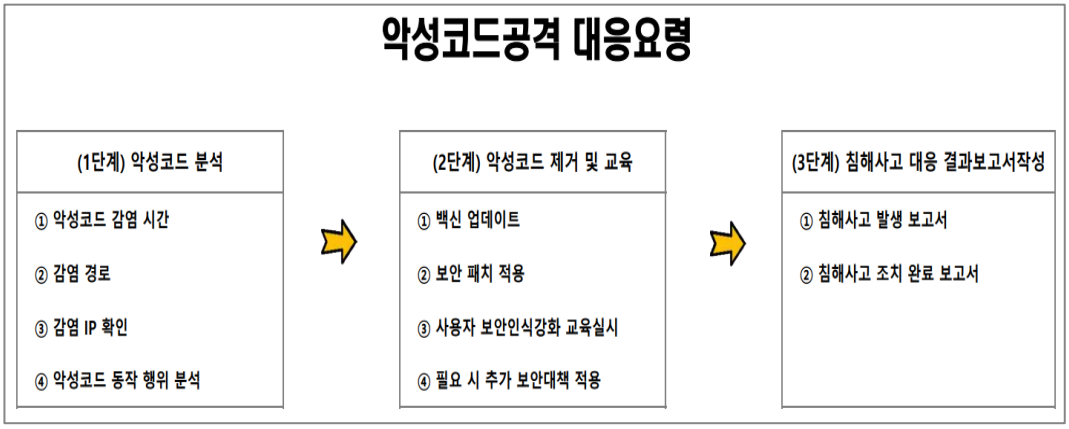
① 악성코드감염 대응절차

≫ 악성코드 공격 확인

≫ 감염시스템 분리 및 경로 차단

≫ 외부 네트워크 연결 차단

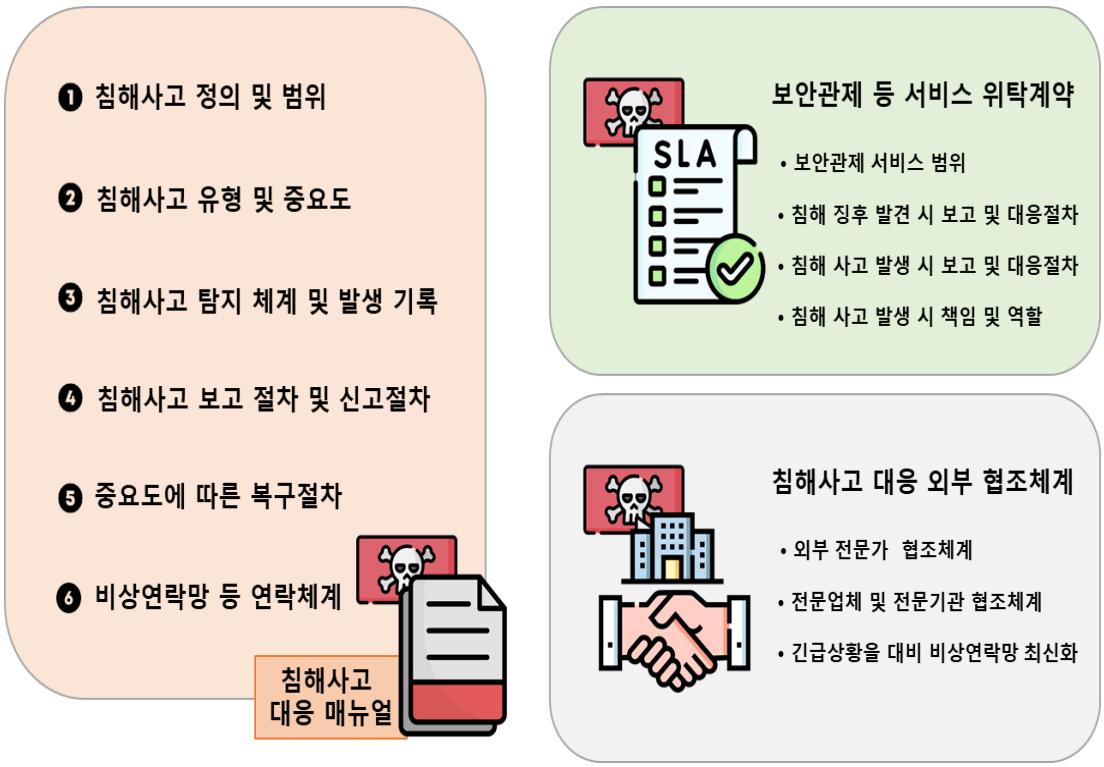
≫ 악성코드 분석 및 사고통보



※ 악성코드공격 대응요령(이해를 돕기 위한 예시)

2.11 사고 예방 및 대응

2.11.1 사고 예방 및 대응체계 구축

<table>
<tr><th>세부분야</th><th>2.11.1 사고 예방 및 대응체계 구축</th></tr>
<tr><td>인증
기준</td><td>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.</td></tr>
<tr><td>주요
확인사항</td><td>• 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 대응절차의 세부사항을 계약서에 반영하고 있는가?
• 침해사고의 모니터링, 대응 및 처리를 위하여 외부전문가, 전문업체, 전문기관 등과의 협조체계를 수립하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 침해사고 및 개인정보 유출사고를 예방하고 사고 발생 시 신속하고 효과적으로 대응하기 위한 체계와 절차를 마련하고 있는가?

→ 침해사고 대응 체계 및 절차 수립 (예시)
「침해사고 대응 매뉴얼」
① 침해사고의 정의 및 범위
≫ 정보자산의 손실·절도·파괴 등이 발생하여 정상적인 업무에 지장을 초래하는</td></tr>
</table>

사고

② 침해사고 유형 및 중요도

≫ IT침해사고 유형

(a) 정보시스템: 정보통신망에 대한 해킹, 악성코드 유포 등

(b) 정보자료: 비밀자료 유출·파괴·변조 및 노출 등

(c) 암호장비: 암호장비 키 운용체계 노출 등

③ 침해사고 선포절차 및 방법

④ 비상연락망 등의 연락체계

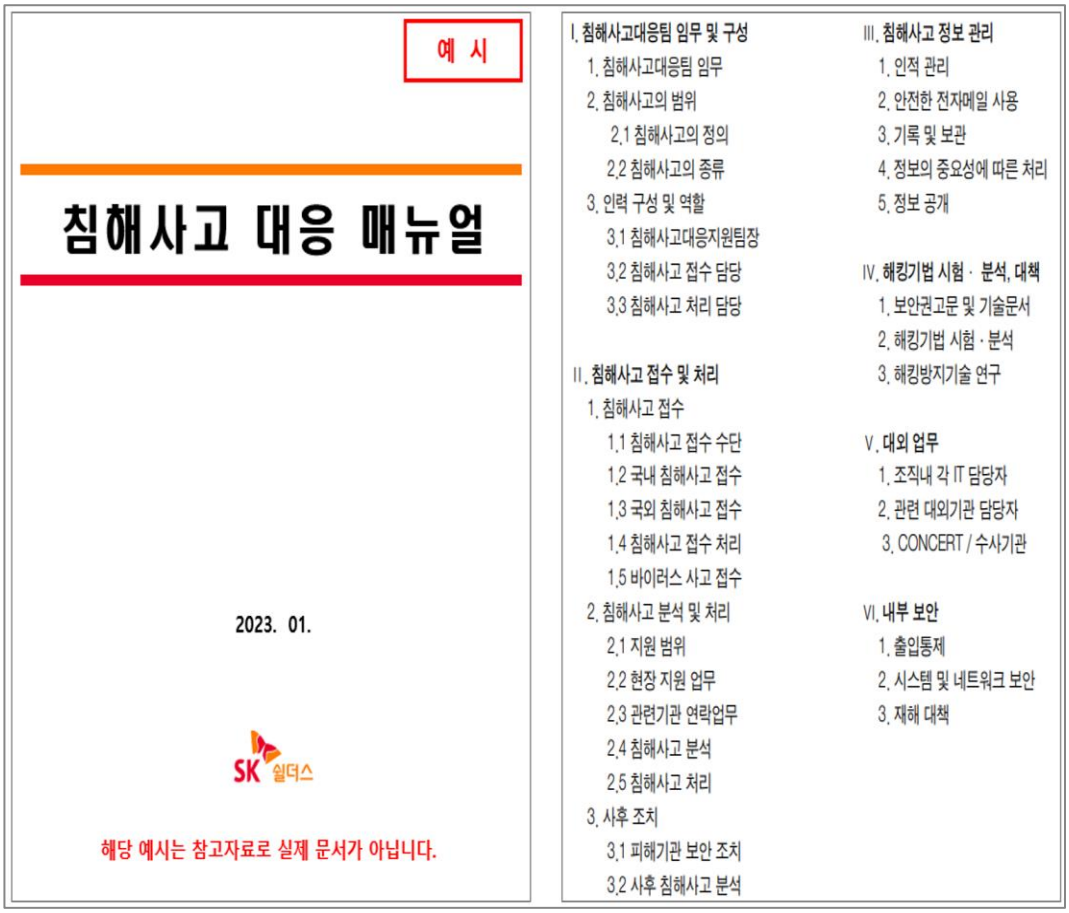
≫ IT침해사고 비상 연락망

(a) 침해사고대응팀 연락망: 침해사고팀장, 침해사고 분석담당자 등

(b) 관련 부서 연락망: 서비스보안팀, 부서별 보안담당자 등

(c) 관련 업체 연락망: 정보보호전문업체, 정보보호시스템 업체 등

⑤ 침해사고 탐지 체계



※ 침해사고 대응 매뉴얼(이해를 돕기 위한 예시)

◇ 보안관제서비스 등 외부 기관을 통하여 침해사고 대응체계를 구축·운영하는 경우 침해사고 대응절차의 세부사항을 계약서에 반영하고 있는가?

→ **외부 기관을 통한 침해사고 대응 절차 수립**

① 보안관제서비스의 범위

② 침해 징후 발견 시 보고 및 대응 절차

③ 침해사고 발생 시 보고 및 대응절차

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 비상연락망 현행화

침해사고 대비 비상 연락망

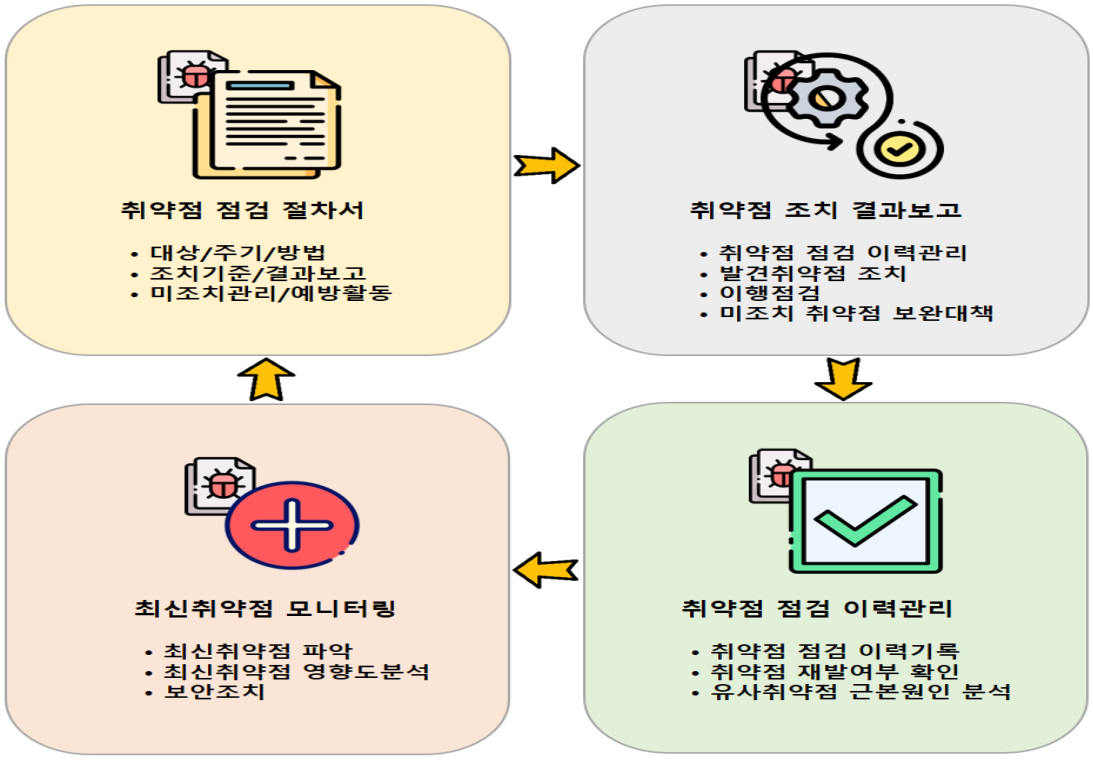
침해사고 대응팀 연락망			
부서	담당업무	담당자명	연락처
…	…	…	…

관련업체 연락망			
부서	담당업무	담당자명	연락처
…	…	…	…

관련기관 연락망			
부서	담당업무	담당자명	연락처
…	…	…	…

※ 협조체계 수립을 위한 비상연락망(이해를 돕기위한 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 기록관리하여 전년도에 도출된 취약점이 재발생하는 등의 문제점에 대하여 보호대책을 마련하고 있는가?
기준 요약도	
운영 방안	**◇ 정보시스템 취약점 점검 절차를 수립하고, 정기적으로 점검을 수행하고 있는가?** **→ 취약점 점검 절차 수립 (예시)** 「**침해사고 대응지침**」 제 ○○조 (취약점 점검계획) ① 정보보호책임자는 정보서비스 전체를 대상으로 주기적(년 1회 이상)으로 취약점 점검을 수행하여야 한다.

② 정보보호담당자는 취약점 점검 계획을 수립하고 정보보호책임자의 승인을 받은후에 수행하여야 한다. 취약점 점검 계획에는 다음의 사항이 포함되어야 한다.

≫ 취약점 점검대상

≫ 취약점 점검일정

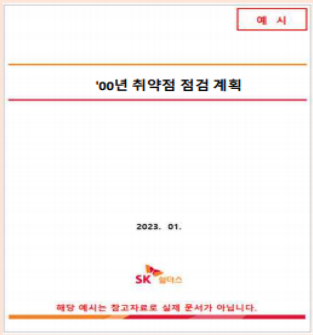
≫ 취약점 점검 담당자 및 책임자

≫ 취약점 점검 절차 및 방법

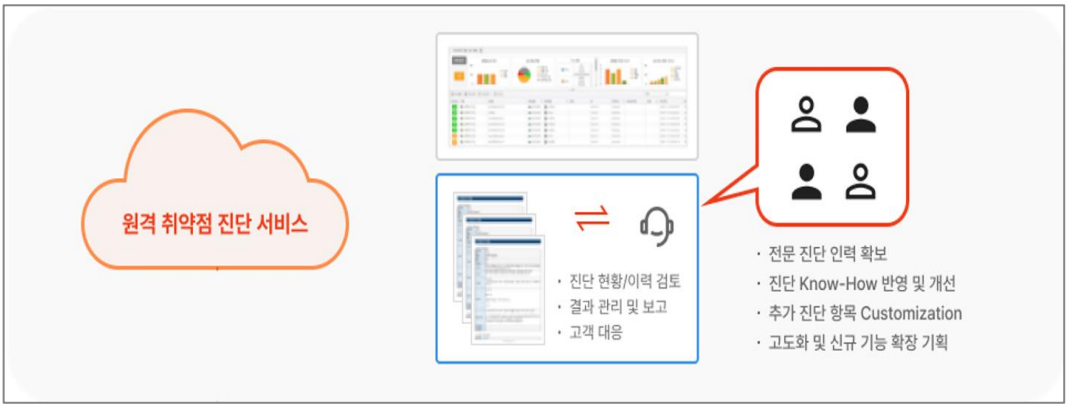
③ 취약점 점검결과 발견된 취약점별로 대응방안 및 조치결과를 문서화하여야 하며 조치결과서를 작성하여 정보보호최고책임자에게 보고하여야 한다

'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	승 인
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 이력관리가 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	승인
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 보안 취약점 지속 파악

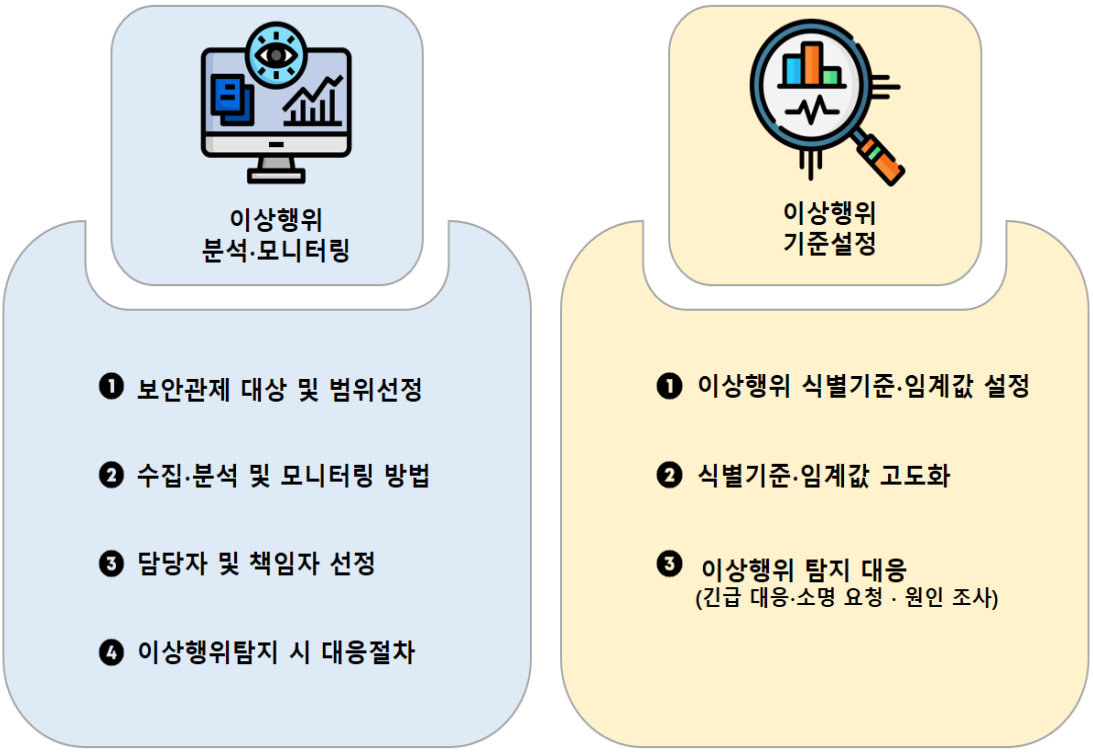
① 최신 보안취약점 파악 및 정보시스템 영향도 분석

※ 출처: SK쉴더스 최신동향 전파 (SK쉴더스)

◇ 취약점 점검 이력을 기록관리하여 전년도에 도출된 취약점이 재발생하는 등의 문제점에 대하여 보호대책을 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

<table>
<tr><th>세부분야</th><th>2.11.3 이상행위 분석 및 모니터링</th></tr>
<tr><td>인증
기준</td><td>내·외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등을 신속하게 탐지·대응할 수 있도록 네트워크 및 데이터 흐름 등을 수집하여 분석하며, 모니터링 및 점검 결과에 따른 사후조치는 적시에 이루어져야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 내·외부에 의한 침해시도, 개인정보유출 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, 개인정보유출시도, 부정행위 등의 여부를 판단하기 위한 기준 및 임계치를 정의하고 이에 따라 이상행위의 판단 및 조사 등 후속 조치가 적시에 이루어지고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 내·외부에 의한 침해시도, 개인정보유출 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 모니터링 절차 및 체계 구축

「정보시스템 운영관리지침」 제 ○○조 (침해사고 모니터링)</td></tr>
</table>

① 정보보호관리자는 보안사고를 예방하기 위해 사전 모니터링 및 탐지·대응 체계를 다음 각 호에 맞춰 운영관리 한다.

≫ 대상 및 범위

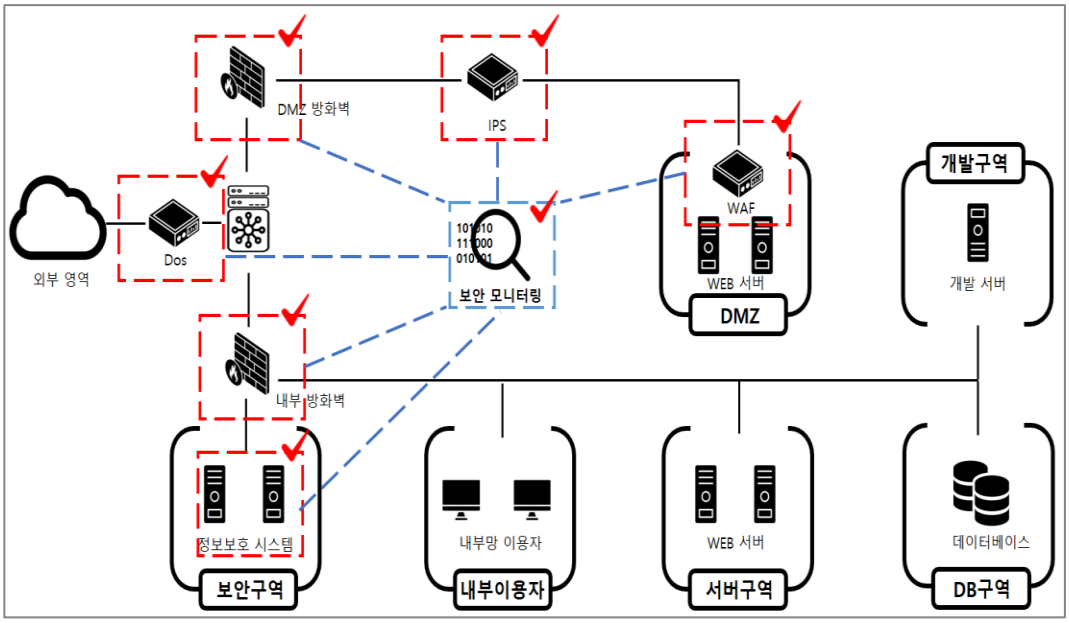
≫ 수집 및 분석, 모니터링 방법

- 자동으로 생성되는 정보를 각 호의 수집 이용하여 보안 모니터링을 실시한다.
  - 사이버공격 공격 의심 패킷
  - 공격지 및 피해의심지 IP주소, MAC주소, 전자우편, 계정정보 등 식별가능정보
  - 그밖에 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, 개인정보유출시도, 부정행위 등의 여부를 판단하기 위한 기준 및 임계치를 정의하고 이에 따라 이상행위의 판단 및 조사 등 후속 조치가 적시에 이루어지고 있는가?

→ 판단기준 정의 및 후속조치

① 침해시도, 개인정보유출 시도, 부정행위 등 임계값 설정

② 기준 및 임계치를 주기적으로 검토하여 최적화

③ 긴급 대응, 소명 요청, 원인 조사 등 사후조치 수행

→ 침입차단 시스템 로그 분석(기준 및 임계치)

① 포트 스캔 시도

≫ srcip=SRCIP, srcport=any, dstip=DSTIP, dstport=[PORTGROUP], actuon=any

샘플 로그(port scan)

- id=firewall time="2004-02-28 19:37:24" fw=firew4 pri=6 proto=21/TCP
  src=192.168.000.250 dst=158.216.666.1 sent=2592 msg="ALLOW SESSION"
- id=firewall time="2004-02-28 19:39:24" fw=firew4 pri=6 proto=23/TCP
  src=192.168.000.250 dst=158.216.666.1 sent=2592 msg="ALLOW SESSION"
- id=firewall time="2004-02-28 19:41:24" fw=firew4 pri=6 proto=135/UDP
  src=192.168.000.250 dst=158.216.666.1 sent=2592 msg="ALLOW SESSION"
- id=firewall time="2004-02-28 19:43:24" fw=firew4 pri=6 proto=161/UDP
  src=192.168.000.250 dst=158.216.666.1 sent=2592 msg="ALLOW SESSION"
- id=firewall time="2004-02-28 19:44:24" fw=firew4 pri=6 proto=513/TCP

※ 출처: 방화벽 관리 및 침해기록 분석방법(국가사비어안전센터)

2.11.4 사고 대응 훈련 및 개선

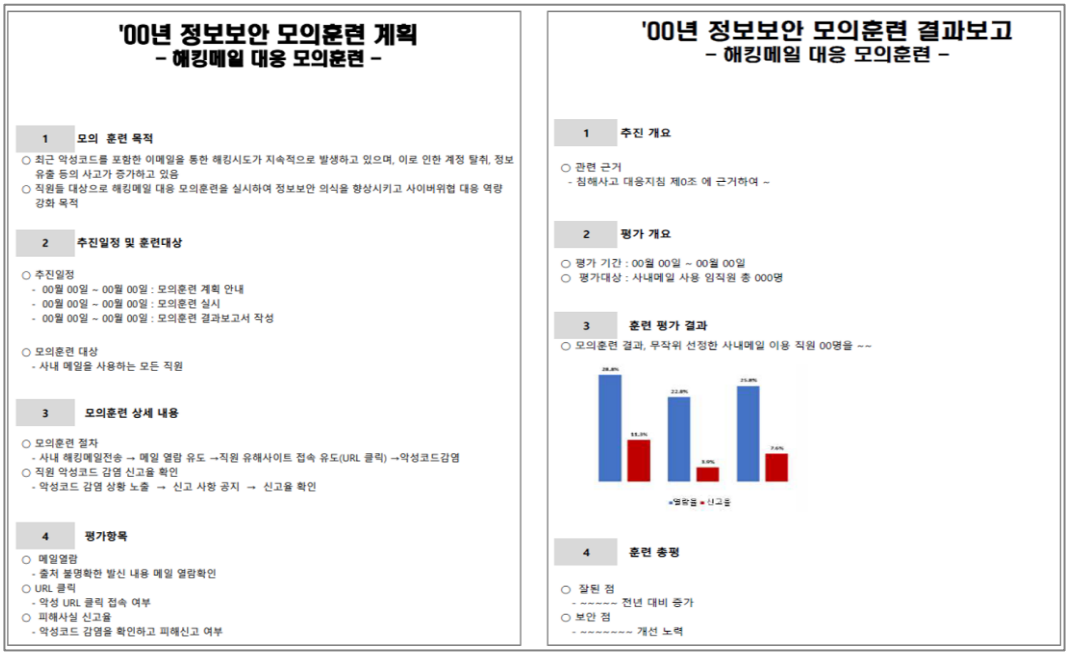
세부분야	2.11.4 사고 대응 훈련 및 개선
인증 기준	침해사고 및 개인정보 유출사고 대응 절차를 임직원과 이해관계자가 숙지하도록 시나리오에 따른 모의훈련을 연 1회 이상 실시하고 훈련결과를 반영하여 대응체계를 개선하여야 한다
주요 확인사항	• 침해사고 및 개인정보 유출사고 대응 절차에 관한 모의훈련계획을 수립하고 이에 따라 연 1회 이상 주기적으로 훈련을 실시하고 있는가? • 침해사고 및 개인정보 유출사고 훈련 결과를 반영하여 침해사고 및 개인정보 유출사고 대응체계를 개선하고 있는가?
기준 요약도	
운영 방안	**◇ 침해사고 및 개인정보 유출사고 대응 절차에 관한 모의훈련계획을 수립하고 이에 따라 연 1회 이상 주기적으로 훈련을 실시하고 있는가?** **→ 침해사고 대응 모의 훈련 계획 수립 (예시)** **「침해사고 대응지침」** 제 ○○조 (침해사고 대응 훈련) ① 침해사고 대응절차에 관한 연 1회 이상 모의훈련 계획을 수립하고 이에 따라 주기적으로 훈련 실시 및 적정성과 효과성을 평가해야한다. **→ 침해사고 대응 훈련 계획 (예시)**

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
– 해킹메일 대응 모의훈련 –

1 모의 훈련 목적

○ 최근 악성코드를 포함한 이메일을 통한 해킹시도가 지속적으로 발생하고 있으며, 이로 인한 계정 탈취, 정보 유출 등의 사고가 증가하고 있음
○ 직원들 대상으로 해킹메일 대응 모의훈련을 실시하여 정보보안 의식을 향상시키고 사이버위협 대응 역량 강화 목적

2 추진일정 및 훈련대상

○ 추진일정
- 00월 00일 ~ 00월 00일 : 모의훈련 계획 안내
- 00월 00일 ~ 00월 00일 : 모의훈련 실시
- 00월 00일 ~ 00월 00일 : 모의훈련 결과보고서 작성

○ 모의훈련 대상
- 사내 메일을 사용하는 모든 직원

3 모의훈련 상세 내용

○ 모의훈련 절차
- 사내 해킹메일전송 → 메일 열람 유도 →직원 유해사이트 접속 유도(URL 클릭) →악성코드감염
○ 직원 악성코드 감염 신고율 확인
- 악성코드 감염 상황 노출 → 신고 사항 공지 → 신고율 확인

4 평가항목

○ 메일열람
- 출처 불명확한 발신 내용 메일 열람확인
○ URL 클릭
- 악성 URL 클릭 접속 여부
○ 피해사실 신고율
- 악성코드 감염을 확인하고 피해신고 여부

'00년 정보보안 모의훈련 결과보고
– 해킹메일 대응 모의훈련 –

1 추진 개요

○ 관련 근거
- 침해사고 대응지침 제0조 에 근거하여 ~

2 평가 개요

○ 평가 기간 : 00월 00일 ~ 00월 00일
○ 평가대상 : 사내메일 사용 임직원 총 000명

3 훈련 평가 결과

○ 모의훈련 결과, 무작위 선정한 사내메일 이용 직원 00명을 ~~

4 훈련 총평

○ 잘된 점
- ~~~~~ 전년 대비 증가
○ 보안 점
- ~~~~~~~ 개선 노력

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 관계기관신고 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 대응절차 등을 변경하고 있는가?
기준 요약도	
운영 방안	**◇ 침해사고 및 개인정보 유출의 징후 또는 발생을 인지한 경우 정의된 침해사고 대응절차에 따라 신속하게 대응 및 보고가 이루어지고 있는가?** **→ 침해사고 대응절차 (예시)** **「침해사고 대응매뉴얼」** ① 정보시스템별 담당자는 침해사고 유형별 절차에 따라 대응한다.

≫ 서버의 네트워크 분리, 공격포트차단 등 응급조치

≫ 사내 업무 전체 영향을 미치는 경우 업무 시간 종료 후 서비스 중단

≫ 사내 일부 시스템에 영향을 미치는 경우 업무부서 협의 후 즉시 중단

≫ 응급조치 후 정보보호 침해사고 원인 분석 및 증거자료 확보

≫ 재발방지대책 수립 및 이행

→ 침해사고 보고서 작성 내역

「침해사고 대응매뉴얼」

① 정보시스템별 담당자는 접수된 신고에 대해 조치가 완료될때 까지의 모든 기록을 유지 및 관리해야하며, 침해사고 발생 및 처리 결과보고서를 작성하여 정보보호 최고책임자에게 보고한다. 보고 시 다음 각 호의 사항을 포함해야 한다.

≫ 침해사고 발생 유형 및 날짜

≫ 피해 범위 및 정도

≫ 침해사고 발생원인

≫ 대응조치 및 수립된 보안대책

침해사고 발생 결과보고서

정보보호 관리자	정보보호 책임자

발견 일자		발견자	
침해사고 시스템		IP	
침해사고 상세 내용			
1) 현상 : 2) 파급 영향 : 3) 협조 요청 사항: 4) 기타 상세 내역			
긴급 처리 여부			
긴급조치 일자		긴급조치 담당자	
긴급조치내용 요약			

침해사고 처리 결과보고서

정보보호 관리자	정보보호 책임자

작성 일자		작성 부서 / 작성자	/
침해사고 시스템		IP	
침해사고 발생 일자			
침해사고 발생 내용			
침해사고 발생 원인			
조치 시간		조 치 자	
조치 내용 및 결과			
향후 대책			

※ 침해사고 발생 결과보고서 (이해를 돕기 위한 예시)

◇ 개인정보 침해사고 발생 시 관련 법령에 따라 정보주체(이용자) 통지 및 관계기관 신고 절차를 이행하고 있는가?

→ 개인정보 유출 단계별 절차도

① 사고 인지 및 긴급조치

≫ 침해사고 대응팀 소집 및 유관기관 협조체계 구축

≫ 피해 최소화를 위한 긴급 조치

② 정보주체 유출통지

≫ 개인정보 유출 사실 5일 이내 정보주체 통지

③ 개인정보 유출신고

≫ 개인정보 유출 시 인터넷 진흥원 및 개인정보보호 위원회 유출 신고

④ 고객대응

≫ 개인정보 유출사고 규모에 따른 고객 대응팀 구성 2차 피해방지 대응

⑤ 피해구제 절차 안내

≫ 개인정보 유출에 대한 피해구제 절차

⑥ 보안기능강화

≫ 사고 원인 분석 및 보안강화

⑦ 결과보고

≫ 경영진에 사고에 대한 결과보고서 작성 및 보고

⑧ 재발방지대책

≫ 유출 사례 전파 교육 및 개선대책 시행

※ 출처: 해킹사고 신고접수(KISA)

→ 개인정보 유출 사실 신고 작성

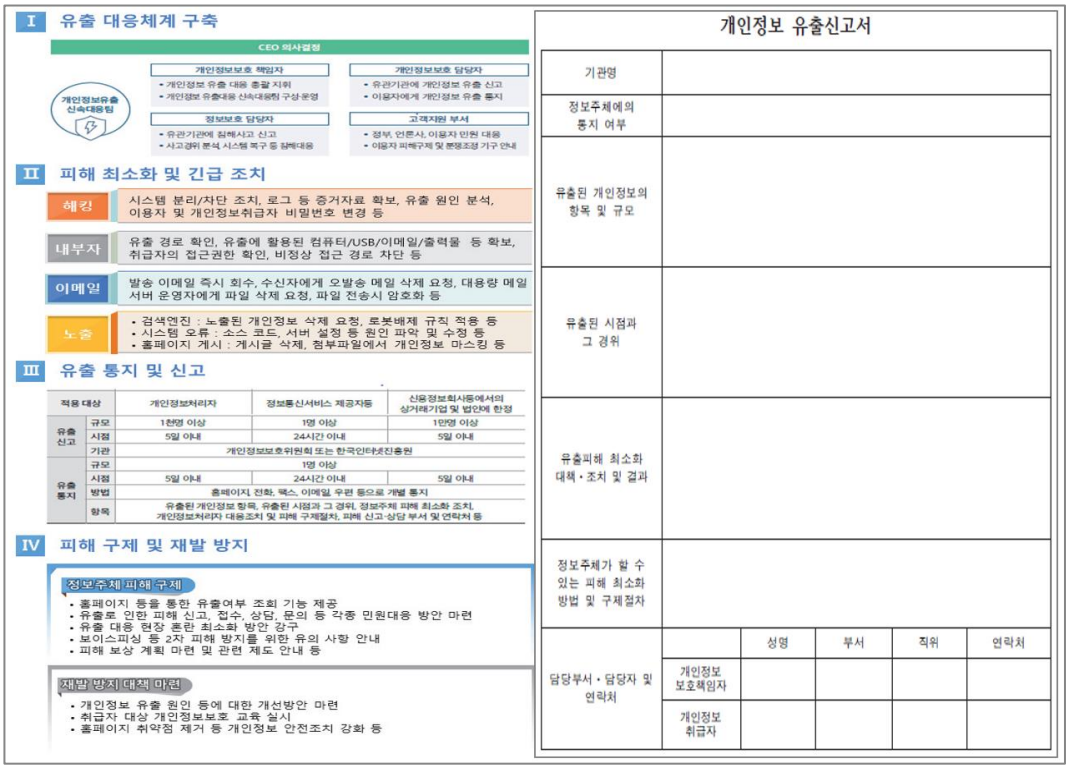
① 유출된 개인정보의 항목

② 유출된 시점과 그 경위

③ 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보

④ 개인정보처리자의 대응조치 및 피해 구제절차

⑤ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처



Ⅰ 유출 대응체계 구축

CEO 의사결정

개인정보유출 신속대응팀

개인정보보호 책임자
- 개인정보 유출 대응 총괄 지휘
- 개인정보 유출대응 신속대응팀 구성·운영

개인정보보호 담당자
- 유관기관에 개인정보 유출 신고
- 이용자에게 개인정보 유출 통지

정보보호 담당자
- 유관기관에 침해사고 신고
- 사고경위 분석 시스템 복구 등 침해대응

고객지원 부서
- 정부, 언론사, 이용자 민원 대응
- 이용자 피해구제 및 분쟁조정 기구 안내

Ⅱ 피해 최소화 및 긴급 조치

해킹	시스템 분리/차단 조치, 로그 등 증거자료 확보, 유출 원인 분석, 이용자 및 개인정보취급자 비밀번호 변경 등
내부자	유출 경로 확인, 유출에 활용된 컴퓨터/USB/이메일/출력물 등 확보, 취급자의 접근권한 확인, 비정상 접근 경로 차단 등
이메일	발송 이메일 즉시 회수, 수신자에게 오발송 메일 삭제 요청, 대용량 메일 서버 운영자에게 파일 삭제 요청, 파일 전송시 암호화 등
노출	• 검색엔진 : 노출된 개인정보 삭제 요청, 로봇배제 규칙 적용 등 • 시스템 오류 : 소스 코드, 서버 설정 등 원인 파악 및 수정 등 • 홈페이지 게시 : 게시글 삭제, 첨부파일에서 개인정보 마스킹 등

Ⅲ 유출 통지 및 신고

적용 대상		개인정보처리자	정보통신서비스 제공자등	신용정보회사등에서의 상거래기업 및 법인에 한정
유출 신고	규모	1천명 이상	1명 이상	1만명 이상
	시점	5일 이내	24시간 이내	5일 이내
	기관	개인정보보호위원회 또는 한국인터넷진흥원		
유출 통지	규모	1명 이상		
	시점	5일 이내	24시간 이내	5일 이내
	방법	홈페이지 전화, 팩스, 이메일, 우편 등으로 개별 통지		
	항목	유출된 개인정보 항목, 유출된 시점과 그 경위, 정보주체 피해 최소화 조치, 개인정보처리자 대응조치 및 피해 구제절차, 피해 신고·상담 부서 및 연락처 등		

Ⅳ 피해 구제 및 재발 방지

정보주체 피해 구제
- 홈페이지 등을 통한 유출여부 조회 기능 제공
- 유출로 인한 피해 신고, 접수, 상담, 문의 등 각종 민원대응 방안 마련
- 유출 대응 현장 혼란 최소화 방안 강구
- 보이스피싱 등 2차 피해 방지를 위한 유의 사항 안내
- 피해 보상 계획 마련 및 관련 제도 안내 등

재발 방지 대책 마련
- 개인정보 유출 원인 등에 대한 개선방안 마련
- 취급자 대상 개인정보보호 교육 실시
- 홈페이지 취약점 제거 등 개인정보 안전조치 강화 등

개인정보 유출신고서

기관명					
정보주체에의 통지 여부					
유출된 개인정보의 항목 및 규모					
유출된 시점과 그 경위					
유출피해 최소화 대책·조치 및 결과					
정보주체가 할 수 있는 피해 최소화 방법 및 구제절차					
담당부서·담당자 및 연락처		성명	부서	직위	연락처
	개인정보 보호책임자				
	개인정보 취급자				

※ 출처: 개인정보 유출 대응 매뉴얼(개인정보보호위원회·KISA)

◇ 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 공유하여야 한다.

② 침해사고가 처리되고 종결된 후 이에 대한 사고 원인에 대한 분석을 수행하고 결과보고서를 작성하여 책임자에게 보고

③ 침해사고 정보와 발견된 취약점 및 원인, 조치방안 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 대응절차 등을 변경하고 있는가?

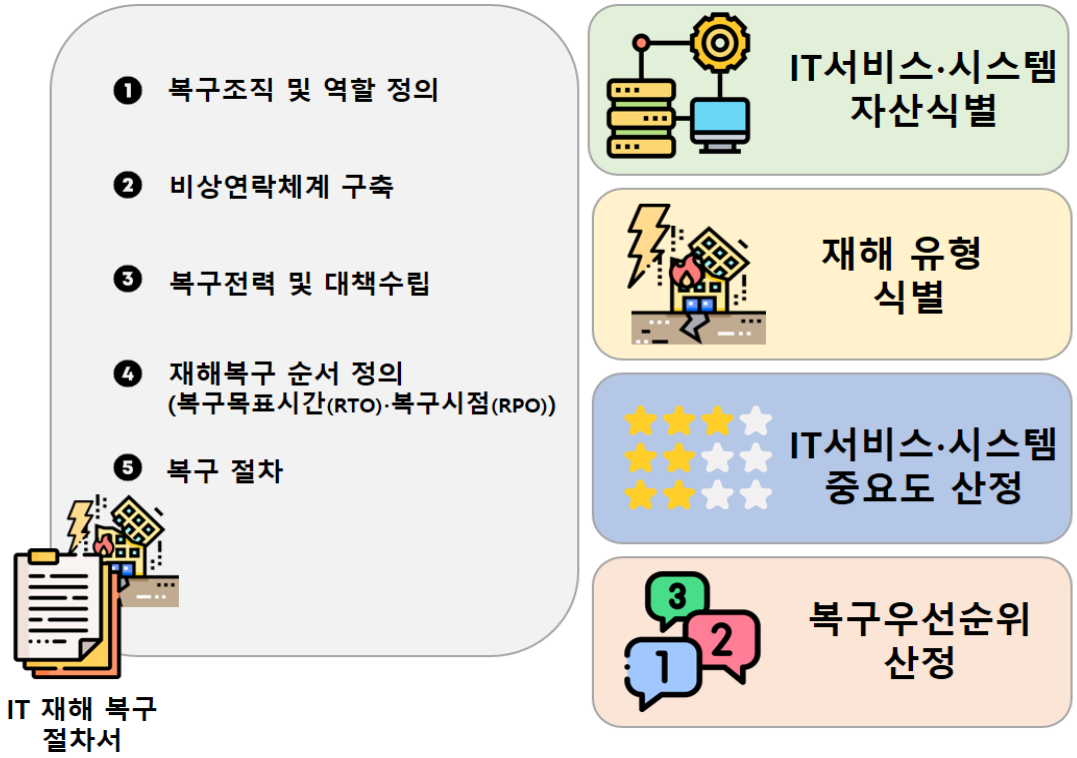
→ 침해사고 재발방지 대책 수립

① 침해사고 분석을 통하여 얻은 정보를 활용하여 유사 사고가 반복되지 않도록 하는 재발방지 대책 수립

② 분석된 결과에 따라 필요한 경우 침해사고 대응절차, 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 목표시점을 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?

→ **IT재해 유형 식별**

① 자연재해: 화재, 홍수, 지진, 태풍 등

② 외부요인: 해킹, 통신장애, 정전 등

③ 내부요인: 시스템 결함, 기계적 오류, 사용자 실수, 의도적·악의적 운영, 핵심 운영자 근무 이탈, 환경설정 오류 등

→ **피해규모 및 영향분석**

① 정량적 분석

≫ 화폐가치

≫ 업무처리 지연 시간

② 정성적 분석

≫ 유형영향: 고객이탈, 손해배상, 데이터유실 등

≫ 무형영향: 이미지실추, 감독기관 조사

◇ 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

≫ 조직의 핵심적 고객서비스

≫ 조직 전략 측면에서의 중요 업무

② 업무 프로세스간의 상호연관성 분석

≫ 선후관계: 후행 프로세스의 수행을 위해서는 선행 프로세스가 반드시 수행

≫ 참조관계: 수행 결과를 참조해야만 하는 두 프로세스

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
...	...	...		...	...

시스템 중요도 (우선순위)

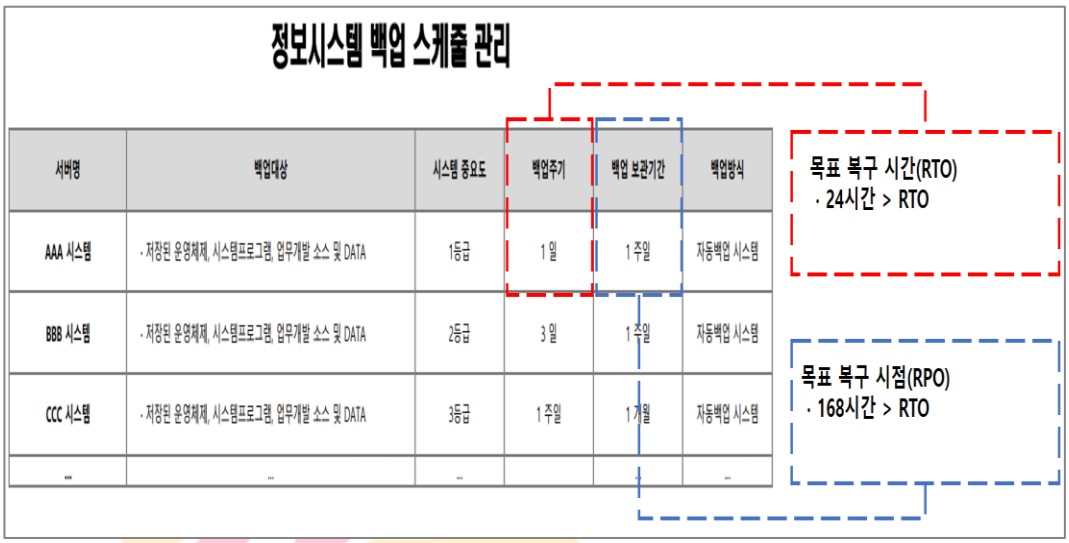
※ 시스템 중요도 산정(이해를 돕기 위한 예시)

→ **정보시스템 복구목표 시간결정**

① 정보시스템 업무 중요도에 따라 복구시간 지정

≫ RTO: 복구목표 시간

≫ RPO: 복구목표 시점



※ 출처: RTO·RPO 산정(이해를 돕기 위한 작성 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?

→ **개인정보처리시스템 위기대응 매뉴얼**

① 관련근거

② 적용범위 및 대상

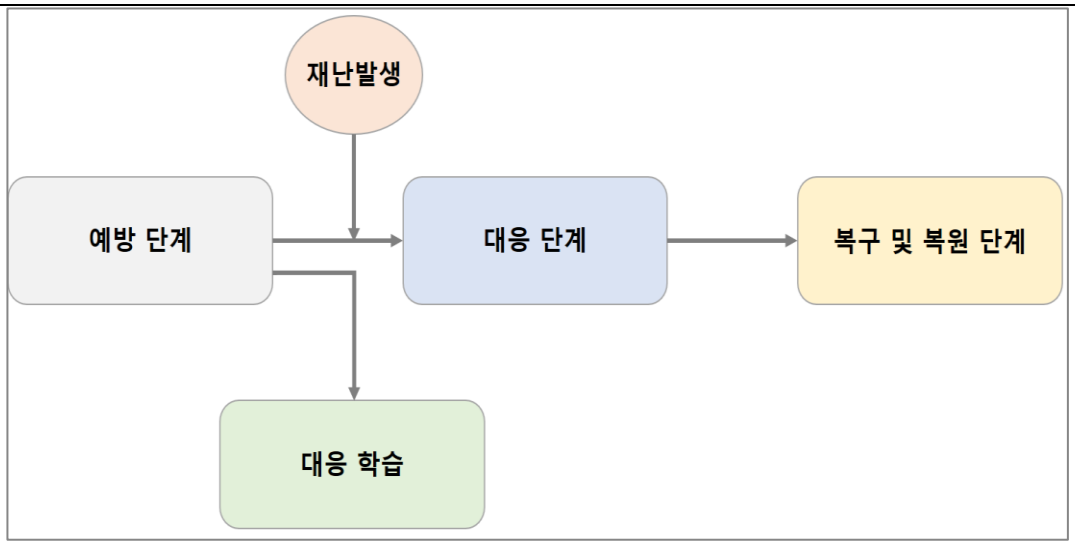
③ 재난·재해·위기 정의

≫ 재해·재난: 태풍, 홍수, 지진, 낙뢰 등 이상적인 자연현상 또는 붕괴, 폭발 등으로 사회적 혼란을 유발할 수 있는 사고

≫ 개인정보처리시스템 위기: 개인정보처리시스템이 장애로 인해 가동이 전면 중단되거나 중단 가능한 시간을 초과하는 경우 등

④ 개인정보처리시스템 구성요소

⑤ 재난·재해·위기 대응절차



※ 재난 대응 절차(이해를 돕기 위한 예시)

≫ 예방단계: 위기상황이 발생하기 전 예상되는 문제들을 미리 보완하고 대비 등

≫ 대응단계: 재해·재난으로 위기상황발생 위기대응 체계에 따라 대응 실시 등

≫ 복구 및 복원 단계: 복구목표에 따라 우선순위가 높은 업무부터 복구 및 복원

⑥ 개인정보처리시스템 백업 및 복구 우선순위, 목표시점·시간

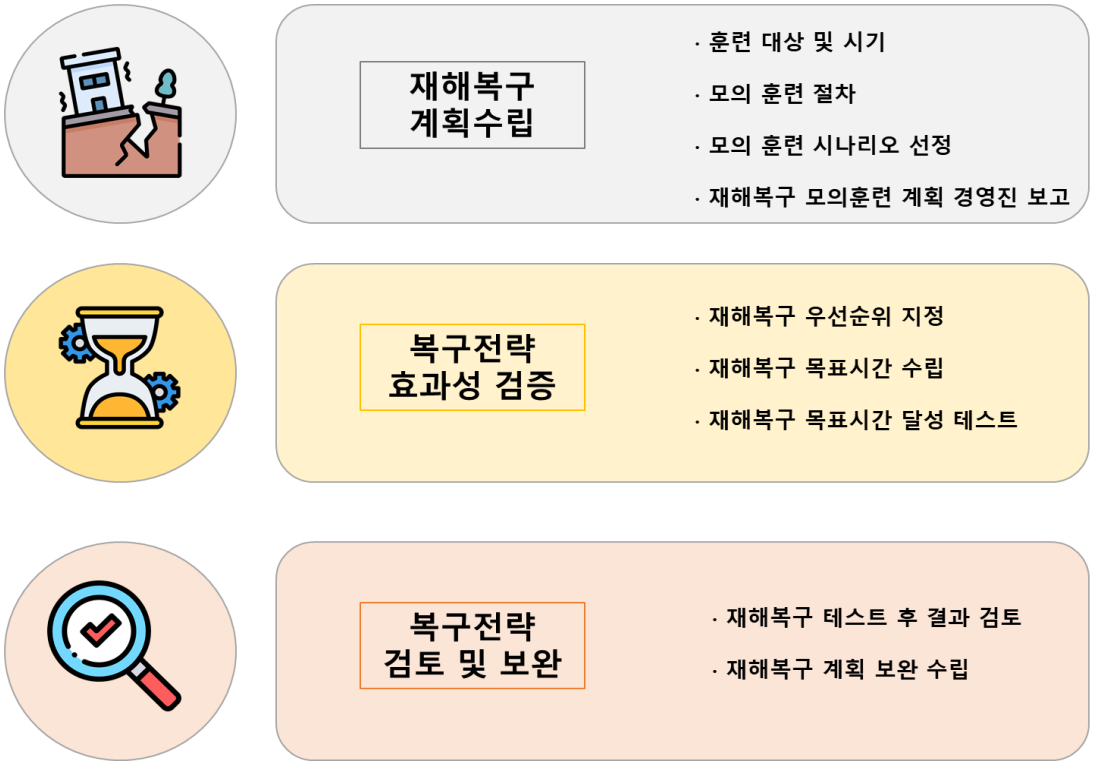
≫ "개인정보 처리시스템 구성현황"의 우선순위로 목표시간 설정

개인정보처리시스템 현황

서버명	백업대상	시스템 중요도	개인정보보유량	민감정보	백업주기	백업 보관기간	시스템 연계
AAA 시스템	· 저장된 운영체제, 시스템프로그램, 업무개발 소스 및 DATA	1등급	30,000 건	주민등록번호	1 일	1 주일	DB, WEB, 보안장비
BBB 시스템	· 저장된 운영체제, 시스템프로그램, 업무개발 소스 및 DATA	2등급	3,000 건	미포함	3 일	1 주일	DB, WEB, 보안장비
CCC 시스템	· 저장된 운영체제, 시스템프로그램, 업무개발 소스 및 DATA	3등급	300건	미포함	1 주일	1 개월	DB, WEB, 보안장비
...	...	...				...	...

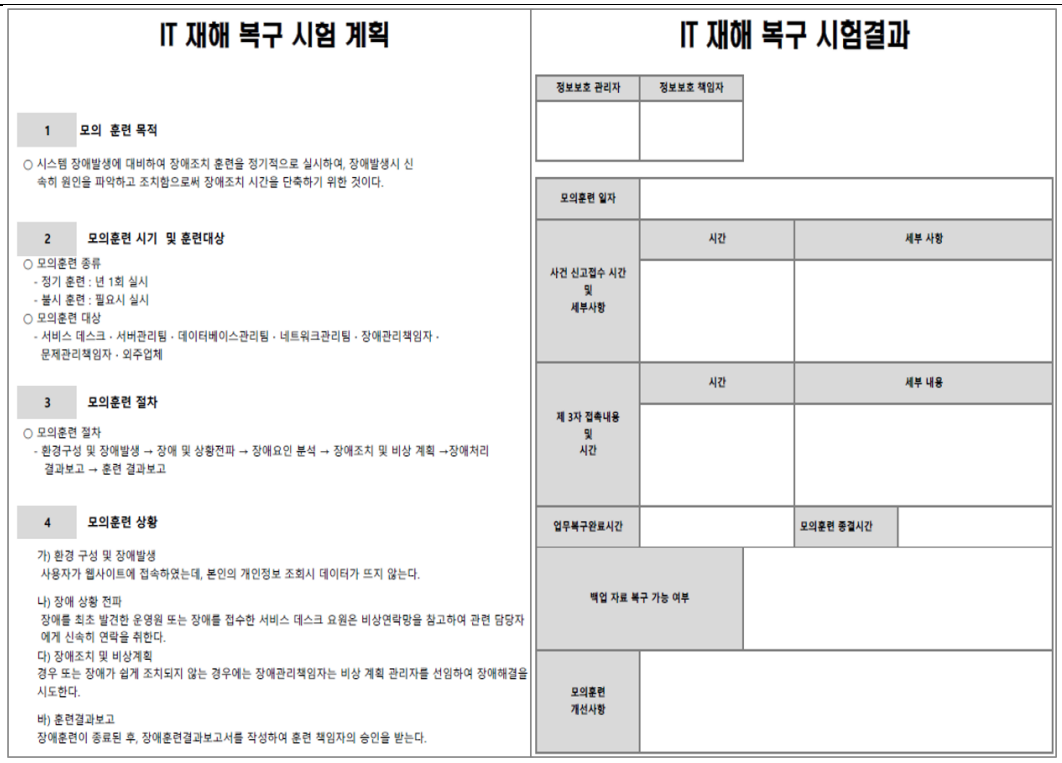
※ 개인정보처리시스템 현황(이해를 돕기 위한 예시)

2.12.2 재해 복구 시험 및 개선

<table>
<tr><th>세부분야</th><th>2.12.2 재해 복구 시험 및 개선</th></tr>
<tr><td>인증
기준</td><td>재해 복구 전략 및 대책의 적정성을 정기적으로 시험하여 시험결과, 정보시스템 환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완하여야 한다</td></tr>
<tr><td>주요
확인사항</td><td>• 수립된 IT 재해 복구체계의 실효성을 판단하기 위하여 재해 복구 시험계획을 수립·이행하고 있는가?
• 시험결과, 정보시스템 환경변화, 법률 등에 따른 변화를 반영할 수 있도록 복구전략 및 대책을 정기적으로 검토·보완하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 수립된 IT 재해 복구체계의 실효성을 판단하기 위하여 재해 복구 시험계획을 수립·이행하고 있는가?

→ 재해복구 시험 계획 수립·이행

「서비스 연속성관리지침」 제 ○○조 (재해복구 모의훈련)
① IT 재해복구 시험계획에 따라 모의훈련을 해야하며, 모의훈련은 문서에 의거 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.</td></tr>
</table>



IT 재해 복구 시험 계획

1 모의 훈련 목적

○ 시스템 장애발생에 대비하여 장애조치 훈련을 정기적으로 실시하여, 장애발생시 신속히 원인을 파악하고 조치함으로써 장애조치 시간을 단축하기 위한 것이다.

2 모의훈련 시기 및 훈련대상

○ 모의훈련 종류
- 정기 훈련 : 년 1회 실시
- 불시 훈련 : 필요시 실시

○ 모의훈련 대상
- 서비스 데스크 · 서버관리팀 · 데이터베이스관리팀 · 네트워크관리팀 · 장애관리책임자 · 문제관리책임자 · 외주업체

3 모의훈련 절차

○ 모의훈련 절차
- 환경구성 및 장애발생 → 장애 및 상황전파 → 장애요인 분석 → 장애조치 및 비상 계획 →장애처리 결과보고 → 훈련 결과보고

4 모의훈련 상황

가) 환경 구성 및 장애발생
사용자가 웹사이트에 접속하였는데, 본인의 개인정보 조회시 데이터가 뜨지 않는다.

나) 장애 상황 전파
장애를 최초 발견한 운영원 또는 장애를 접수한 서비스 데스크 요원은 비상연락망을 참고하여 관련 담당자에게 신속히 연락을 취한다.

다) 장애조치 및 비상계획
경우 또는 장애가 쉽게 조치되지 않는 경우에는 장애관리책임자는 비상 계획 관리자를 선임하여 장애해결을 시도한다.

바) 훈련결과보고
장애훈련이 종료된 후, 장애훈련결과보고서를 작성하여 훈련 책임자의 승인을 받는다.

IT 재해 복구 시험결과

정보보호 관리자	정보보호 책임자

모의훈련 일자		
사건 신고접수 시간 및 세부사항	시간	세부 사항
제 3자 접촉내용 및 시간	시간	세부 내용
업무복구완료시간		모의훈련 종결시간
백업 자료 복구 가능 여부		
모의훈련 개선사항		

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 시험계획(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(예시)

① 재해복구 우선순위 및 복구 목표시간 수립

② 재해복구 테스트 결과보고서 작성

≫ 재난상황 대비 정보시스템의 신속한 복구를 통한 업무 연속성 절차 확인 및 복구 목표시간 확인

≫ 훈련대상자: 정보시스템운영팀, 정보보안팀

≫ 테스트 복구절차: 1순위(AAA시스템) → 2순위(BBB시스템) → 3순위(CCC시스템)

≫ 테스트 결과: 복구테스트 실패(총 2시간 35분)

재해복구 테스트 계획(예시)

우선순위	복구 대상	복구 목표 시간
1순위	AAA 시스템	1시간
2순위	BBB 시스템	30분
3순위	CCC 시스템	1시간
합계		2시간 30분

재해복구 테스트 결과(예시)

우선순위	복구 대상	복구 목표 완료시간
1순위	AAA 시스템 ✓	1시간 15분
2순위	BBB 시스템 ✓	45분
3순위	CCC 시스템	50분
합계		2시간 35분

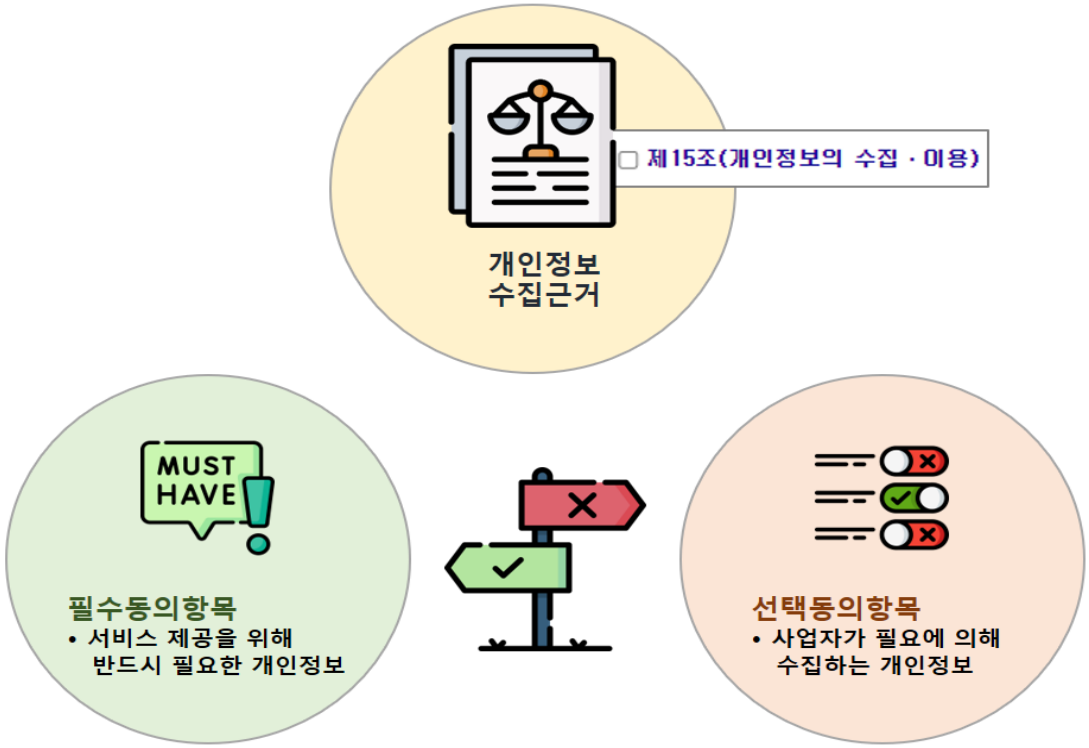
시스템 환경 및 법규 등의 변화에 따라 테스트 계획 재수립 필요

※ IT재해복구 시험계획 및 결과(이해를 돕기 위한 예시)

3. 개인정보 처리 단계별 요구사항

3.1 개인정보 수집 시 보호조치

3.1.1 개인정보 수집 제한

세부분야	3.1.1 개인정보 수집 제한
인증 기준	개인정보는 서비스 제공을 위하여 필요한 최소한의 정보를 적법하고 정당하게 수집하여야 하며, 필수정보 이외의 개인정보를 수집하는 경우에는 선택항목으로 구분하여 해당 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하지 않아야 한다
주요 확인사항	• 개인정보를 수집하는 경우 서비스 제공 또는 법령에 근거한 처리 등을 위하여 필요한 범위 내에서 최소한의 정보만을 수집하고 있는가? • 수집 목적에 필요한 최소한의 정보 외의 개인정보를 수집하는 경우 정보주체(이용자)가 해당 개인정보의 제공 여부를 선택할 수 있도록 하고 있는가? • 정보주체(이용자)가 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 서비스 제공 또는 법령에 근거한 처리 등을 위하여 필요한 범위 내에서 최소한의 정보만을 수집하고 있는가? → 개인정보 입증책임 부담 수집할 때에는 그 목적에 필요한 범위 내에서 최소한의 개인정보만을 수집하여야 한다.

최소한의 개인정보라는 입증책임은 개인정보처리자가 부담이며 그 목적 달성을 위해 필요한 최소한의 개인정보라는 것을 입증하지 못한다면 법적책임을 지게된다.

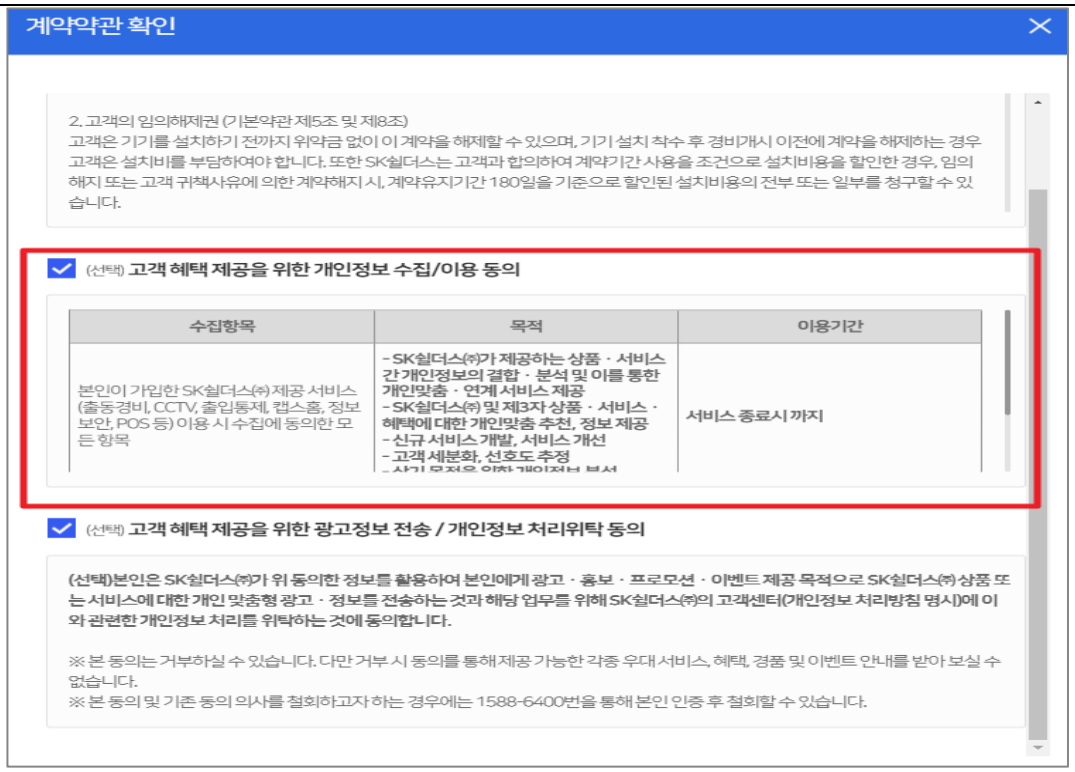
◇ 수집 목적에 필요한 최소한의 정보 외의 개인정보를 수집하는 경우 정보주체(이용자)가 해당 개인정보의 제공 여부를 선택할 수 있도록 하고 있는가?

→ 필수동의•선택동의 상세내용

① 필수 동의: 사업자가 해당 서비스 제공을 위해 반드시 필요한 개인정보에 대해서는 이용자로부터 수집 동의

※ 출처: SK쉴더스 홈페이지 캡스홈 도어 가이드 온라인가입 화면(SK쉴더스)

② 선택 동의: 사업자가 해당 서비스의 추가적 기능 또는 사업자의 필요에 의해 이용자에게 개인정보 수집 동의

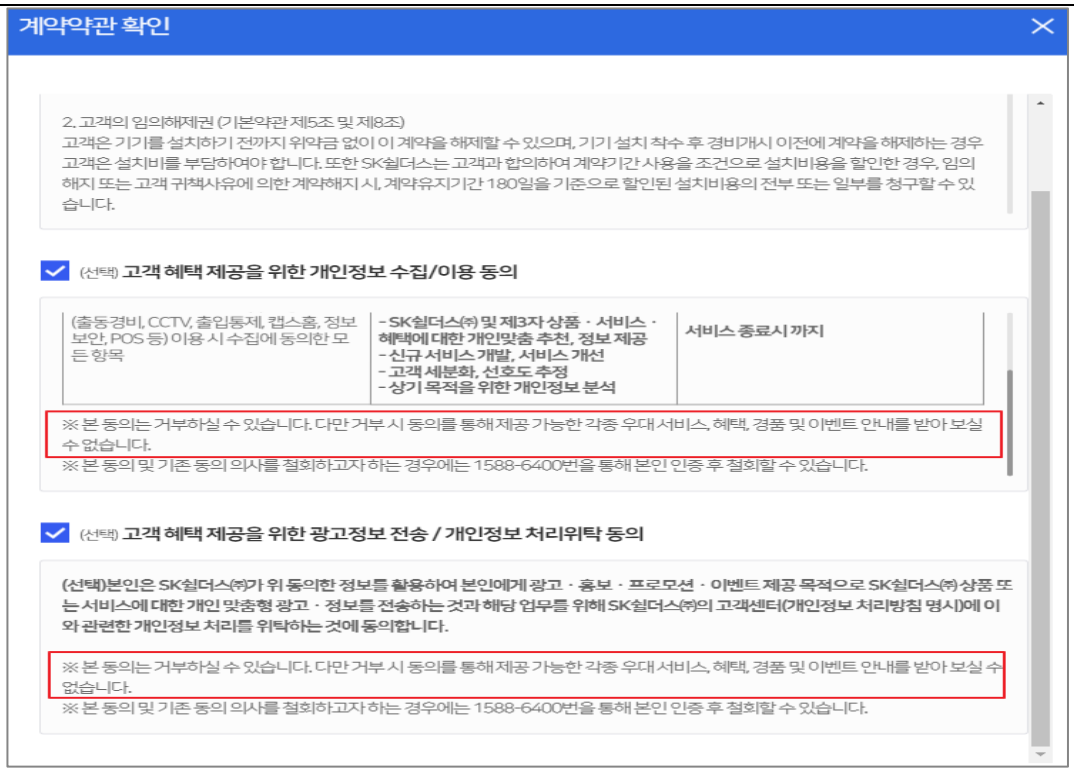


※ 출처: SK쉴더스 홈페이지 캡스홈 도어 가이드 온라인가입 화면(SK쉴더스)

◇ 정보주체(이용자)가 수집 목적에 필요한 최소한의 정보 이외의 개인정보 수집에 동의하지 않는다는 이유로 서비스 또는 재화의 제공을 거부하지 않도록 하고 있는가?

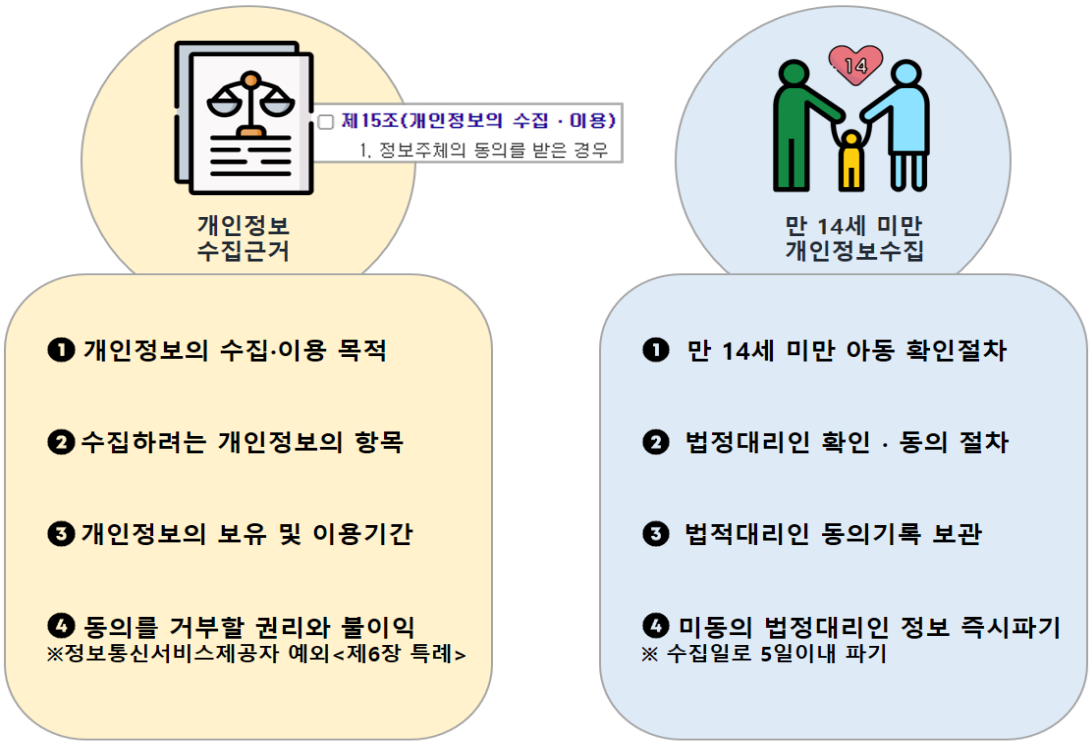
→ 선택동의 거부 시 고려 사항

① 선택 동의 거부 시 에도 정상 서비스 제공 안내



※ 출처: SK쉴더스 홈페이지 캡스홈 도어 가이드 온라인가입 화면(SK쉴더스)

3.1.2 개인정보의 수집 동의

<table>
<tr><th>세부분야</th><th>3.1.2 개인정보의 수집 동의</th></tr>
<tr><td>인증
기준</td><td>개인정보는 정보주체(이용자)의 동의를 받거나 관계 법령에 따라 적법하게 수집하여야 하며, 만 14세 미만 아동의 개인정보를 수집하려는 경우에는 법정대리인의 동의를 받아야 한다</td></tr>
<tr><td>주요
확인사항</td><td>• 개인정보 수집 시 법령에 특별한 규정이 있는 경우를 제외하고는 정보주체(이용자)에게 관련 내용을 명확하게 고지하고 동의를 받고 있는가?
• 정보주체(이용자)에게 동의를 받는 방법 및 시점은 적절하게 되어 있는가?
• 정보주체(이용자)에게 동의를 서면(전자문서 포함)으로 받는 경우 법령에서 정한 중요한 내용에 대하여 명확히 표시하여 알아보기 쉽게 하고 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?
• 정보주체(이용자) 및 법정대리인에게 동의를 받은 기록을 보관하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 개인정보 수집 시 법령에 특별한 규정이 있는 경우를 제외하고는 정보주체(이용자)에게 관련 내용을 명확하게 고지하고 동의를 받고 있는가?

→ 개인정보 수집 이용 가능 경우</td></tr>
</table>

① 개인정보처리자

≫ 정보주체의 동의를 받은 경우

≫ 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우

≫ 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우

≫ 정보주체와의 계약 체결 및 이행을 위하여 불가피한 경우

≫ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 사전동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우

≫ 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우

② 정보통신서비스 제공자

≫ 이용자의 동의를 받은 경우

≫ 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우

≫ 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우

≫ 다른 법률에 특별한 규정이 있는 경우

→ 개인정보의 수집·이용 동의 시 고지 사항

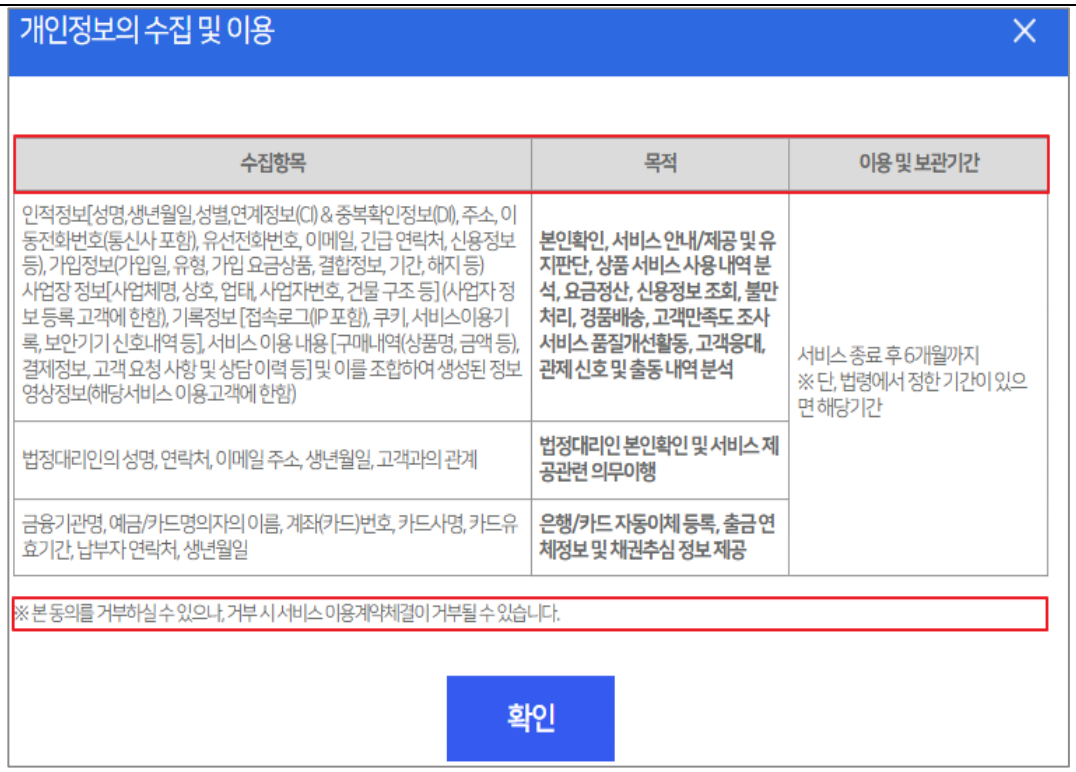
① 개인정보의 수집·이용 목적

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 (정보통신서비스 제공자 제외 근거: 제6장 정보통신서비스 제공자 등의 개인정보 처리 등 특례)

※ 출처: SK쉴더스 홈페이지 캡스홈 도어 가이드 온라인가입 화면(https://www.skshieldus.com)

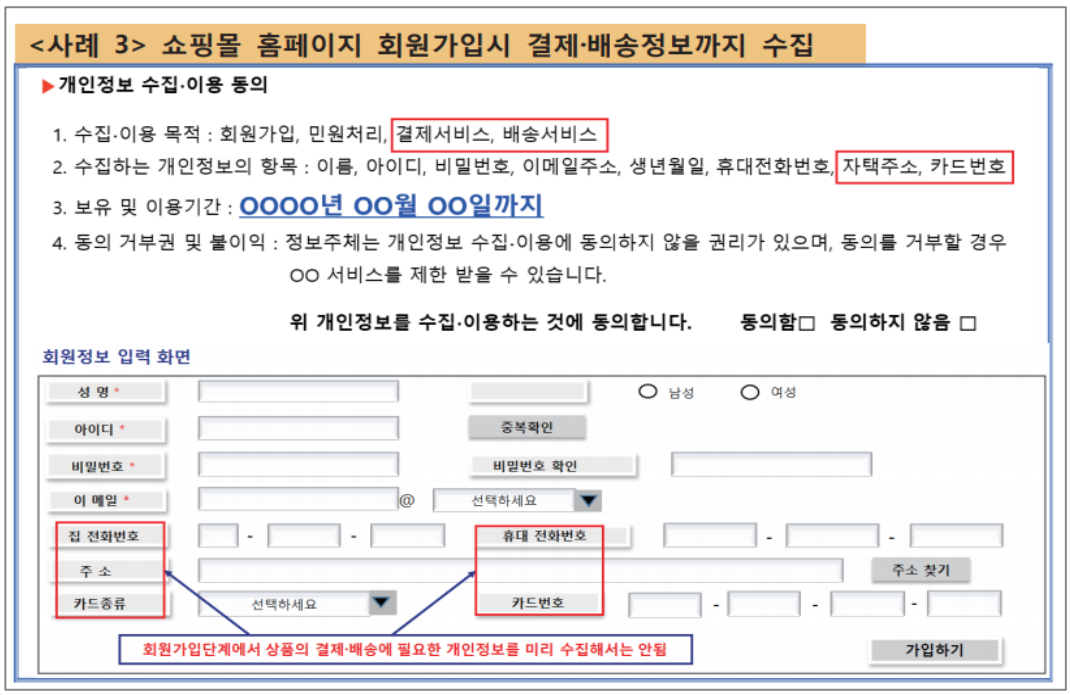


※ 출처: SK쉴더스 홈페이지 캡스홈 도어 가이드 온라인가입 화면(SK쉴더스)

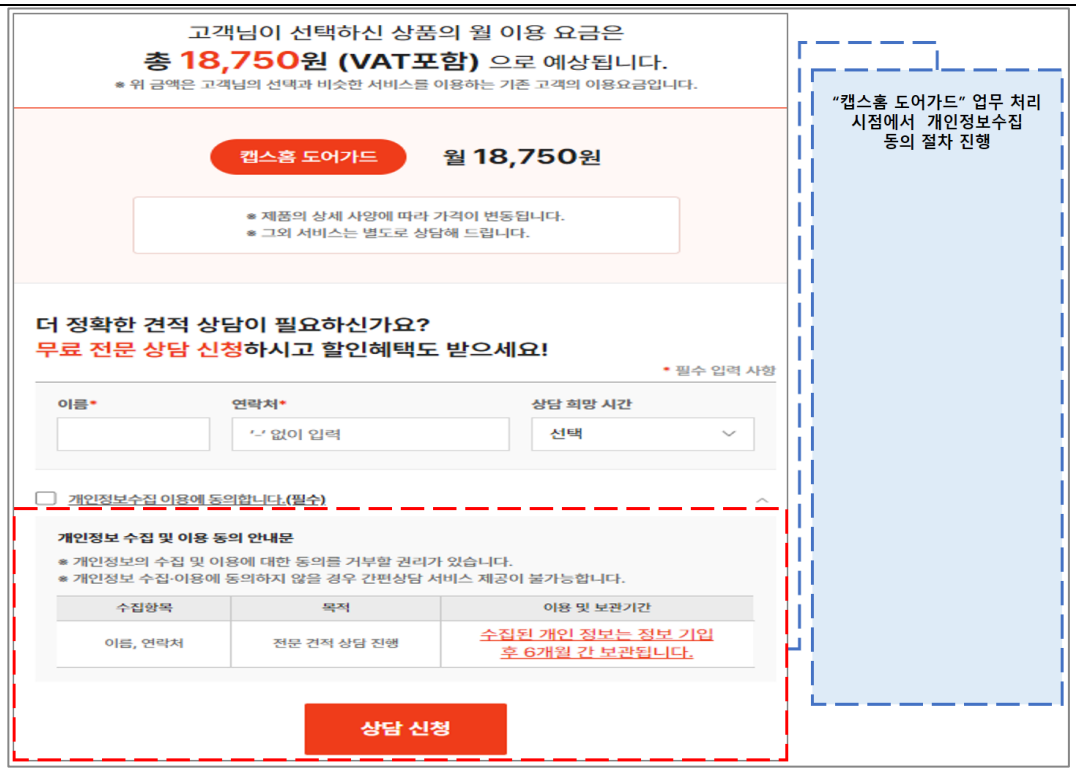
◇ 정보주체(이용자)에게 동의를 받는 방법 및 시점은 적절하게 되어 있는가?

→ 개인정보가 필요한 시점에 수집

① 각 업무 시점에 따라 수집 시점분류



※ 출처: 개인정보 수집 최소화 가이드(개인정보보호위원회·KISA)



※ 출처: SK쉴더스 홈페이지(SK쉴더스)

◇ 정보주체(이용자)에게 동의를 서면(전자문서 포함)으로 받는 경우 법령에서 정한 중요한 내용에 대하여 명확히 표시하여 알아보기 쉽게 하고 있는가?

→ 법령에 정해진 중요 내용만 알아보기 쉽도록 명확히 고지

① 명확한 고지 사항

≫ 글씨 크기 최소한 9포인트 이상

≫ 다른 내용보다 20% 이상 크게

≫ 글씨 색깔 굵기 또는 밑줄의 통한 내용 명확화

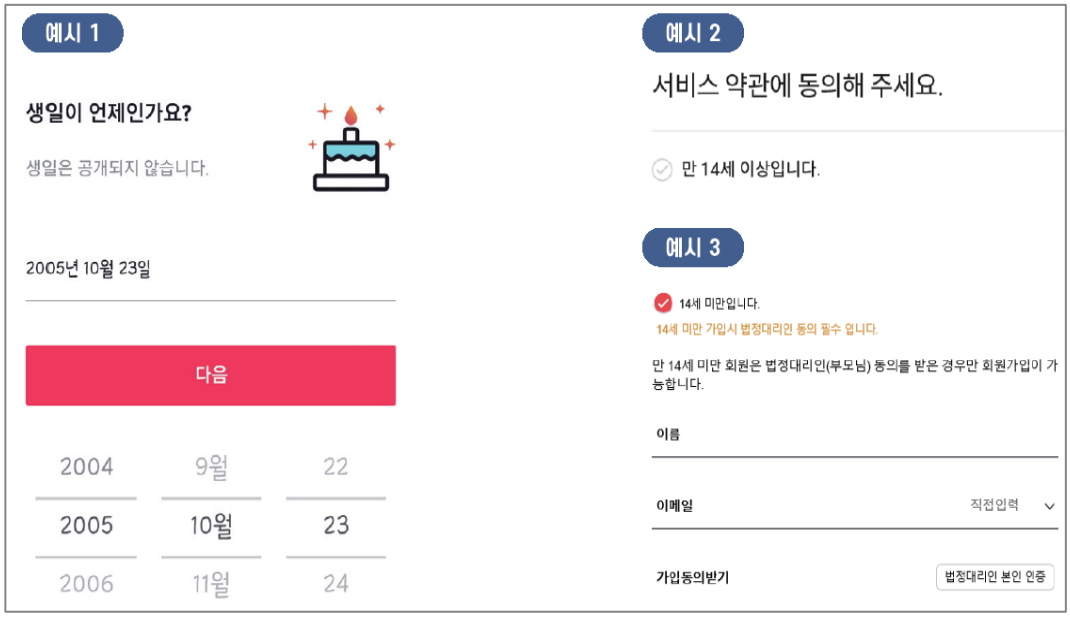
※ 출처: 알기쉬운 개인정보 처리 동의 안내서 (개인정보보호위원회)

◇ 만 14세 미만 아동의 개인정보에 대하여 수집·이용·제공 등의 동의를 받는 경우 법정대리인에게 필요한 사항에 대하여 고지하고 동의를 받고 있는가?

→ **비대면 개인정보 수집 시 만 14세 확인절차 필요**

① 인터넷 등 비대면 회원가입 시, 만14세 미만인지 여부는 정보주체가 "법정 생년월일"을 직접 입력하거나 "만 14세 이상" 항목에 스스로 체크하는 방법으로 확인하는 것이 바람직함

※ 출처: SK쉴더스 모바일가드 스마트폰 앱



※ 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?

→ **법정대리인 진의확인 및 수집·이용·제공 동의 절차**

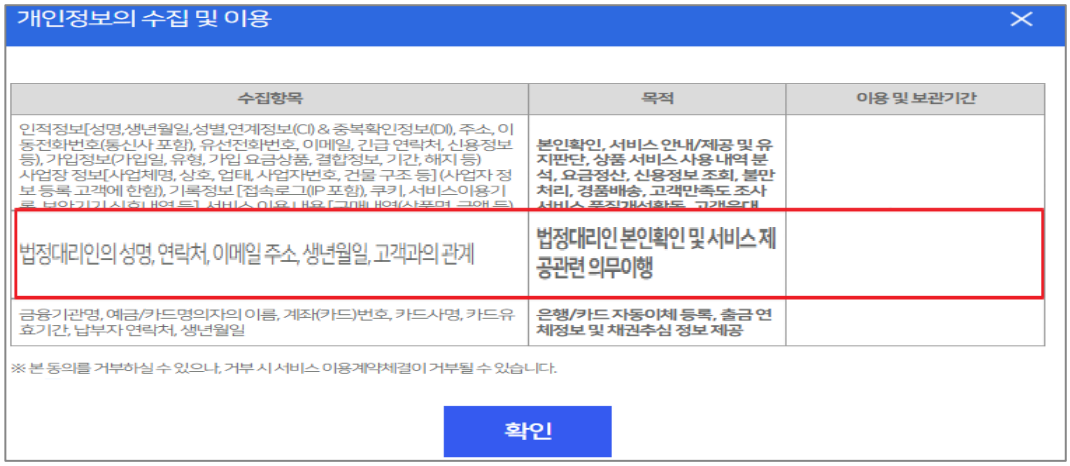
① 법정대리인 진위 확인: 가족관계증명서, 본인인증, 생년월일 등 확인

② 법정대리인 필요사항 고지 및 동의절차

③ 법정대리인 최소한의 개인정보수집

④ 법정대리인 동의의사 미확인 시 5일이내 파기

⑤ 법정대리인 동의기록 기록 및 개인정보 보관



※ 출처: SK쉴더스 홈페이지(SK쉴더스)

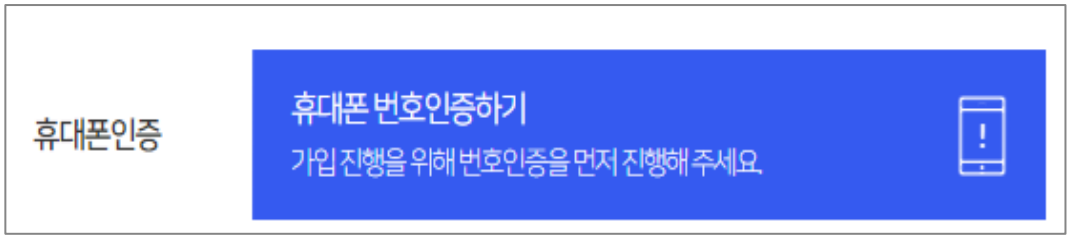
→ 법정대리인 동의 절차

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: SK쉴더스 홈페이지 캡스홈 도어 가이드 온라인가입 화면(SK쉴더스)

◇ 정보주체(이용자) 및 법정대리인에게 동의를 받은 기록을 보관하고 있는가?

→ 동의기록 보관

① 남겨야할 사항

≫ 동의 일시

≫ 동의 항목

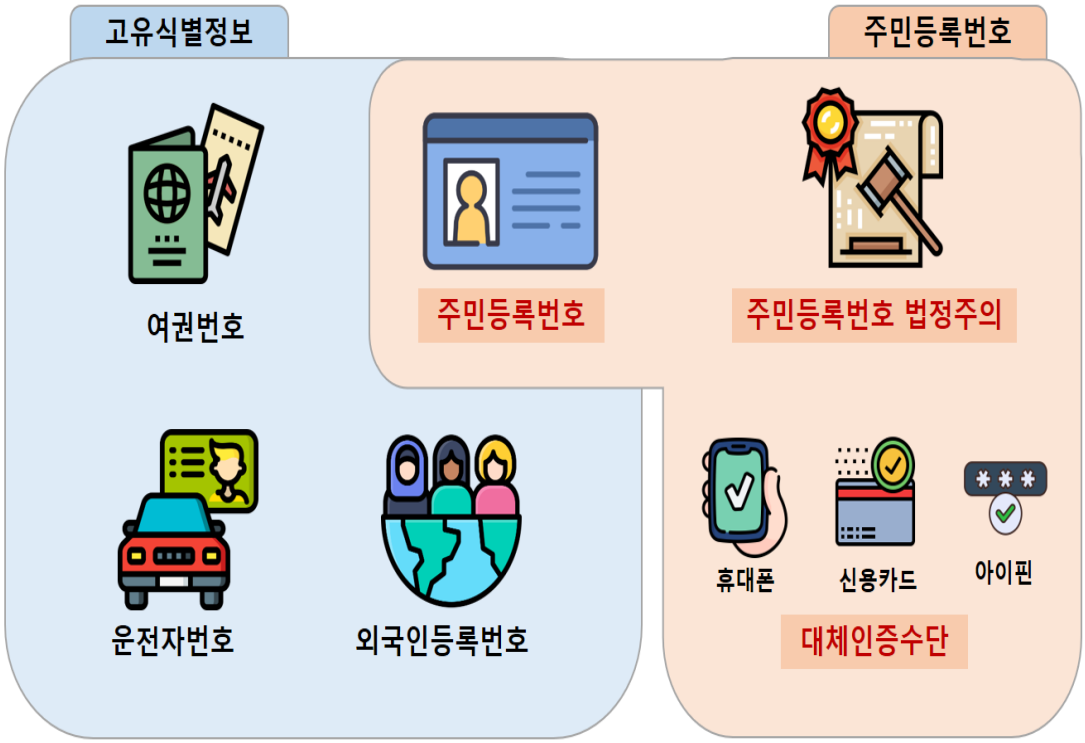
≫ 법정대리인 정보

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

※ 데이터베이스에 법정대리인 정보 함께 보유(이해를 돕기 위한 예시)

3.1.3 주민등록번호 처리 제한

<table>
<tr><th>세부분야</th><th>3.1.3 주민등록번호 처리 제한</th></tr>
<tr><td>인증
기준</td><td>주민등록번호는 법적 근거가 있는 경우를 제외하고는 수집·이용 등 처리할 수 없으며, 주민등록번호의 처리가 허용된 경우라 하더라도 인터넷 홈페이지 등에서 대체수단을 제공하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 주민등록번호는 명확한 법적 근거가 있는 경우에만 처리하고 있는가?
• 주민등록번호의 수집 근거가 되는 법조항을 구체적으로 식별하고 있는가?
• 법적 근거에 따라 정보주체(이용자)의 주민등록번호 수집이 가능한 경우에도 아이핀, 휴대폰 인증 등 주민등록번호를 대체하는 수단을 제공하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 주민등록번호는 명확한 법적 근거가 있는 경우에만 처리하고 있는가?

→ 주민등록번호를 처리는 법조항을 구체적으로 식별하여 입증필요
① (예시) <u>「부가가치세법」 제32조(세금계산서 등)</u>
≫ 사업자가 재화 또는 용역을 공급(부가가치세가 면제되는 재화 또는 용역의 공급은 제외한다)하는 경우에는 다음 각 호의 사항을 적은 계산서(이하 "세금계산서"라 한다)를 그 공급을 받는 자에게 발급하여야 한다.
공급받는 자의 등록번호. 다만, 공급받는 <u>자가 사업자가 아니거나 등록한 사업자가 아닌 경우에는 대통령령으로 정하는 고유번호 또는 공급받는 자의 주민등록번호</u></td></tr>
</table>

※ 출처: SK쉴더스 홈페이지 캡스홈 도어 가이드 온라인가입 화면(SK쉴더스)

◇ 주민등록번호의 수집 근거가 되는 법조항을 구체적으로 식별하고 있는가?

→ 주민등록번호를 처리는 법조항 근거사항

① "법령"은 법률, 시행령, 시행규칙을 의미함

② 행정규칙(고시, 훈령) 및 지방자치단체의 조례 등은 개인정보보호법 제24조의2에 따른 "법령"에 해당하지 않음

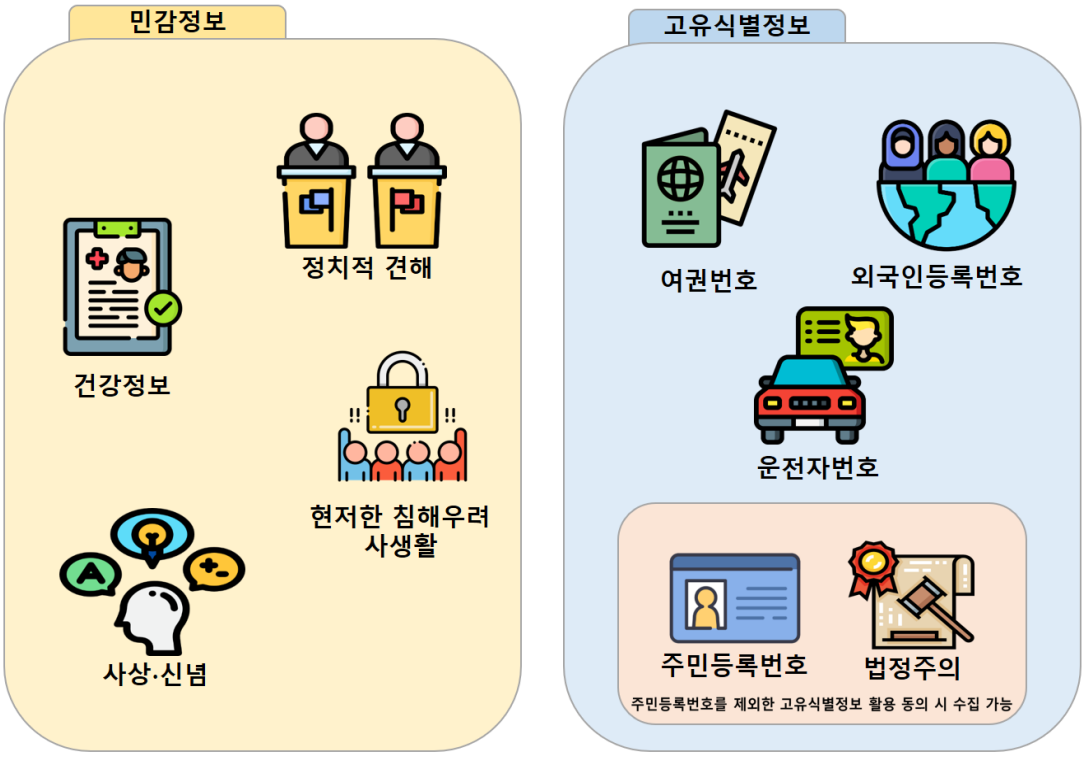
③ "법령"의 별지 서식에 "주민번호 기재항목"이 있거나, 주민번호가 기재된 서류의 제출•첨부 등을 규정한 경우에도 법령 근거가 있는 것으로 봄

④ "처리"란 수집•이용, 기록, 저장 등 제반 행위를 의미

◇ 법적 근거에 따라 정보주체(이용자)의 주민등록번호 수집이 가능한

	경우에도 아이핀, 휴대폰 인증 등 주민등록번호를 대체하는 수단을 제공하고 있는가? **→ 대체인증 수단 종류** ① 아이핀 ② 공동인증서 ③ 핸드폰 ④ 신용카드

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 정보주체(이용자)의 별도의 동의를 받아야 한다.
주요 확인사항	• 민감정보는 정보주체(이용자)로부터 별도의 동의를 받거나 관련 법령에 근거가 있는 경우에만 처리하고 있는가? • 고유식별정보(주민등록번호 제외)는 정보주체(이용자)로부터 별도의 동의를 받거나 관련 법령에 구체적인 근거가 있는 경우에만 처리하고 있는가?
기준 요약도	
운영 방안	**◇ 민감정보는 정보주체(이용자)로부터 별도의 동의를 받거나 관련 법령에 근거가 있는 경우에만 처리하고 있는가?** **→ 민감정보 처리 가능 경우** ① 정보주체로부터 민감정보 처리의 별도 동의를 받은 경우 ② 법령에서 민감정보의 처리를 요구하거나 허용하는 경우 **→ 민감정보의 종류** ① 사상. 신념, 노동조합. 정당의 가입탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 유전정보, 범죄경력자료, 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정

개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보, 인종이나 민족에 관한 정보

→ 민감정보 수집•활용동의 별도동의

① ★ 민감정보 수집•활용동의 [별도동의]

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 정보주체(이용자)로부터 별도의 동의를 받거나 관련 법령에 구체적인 근거가 있는 경우에만 처리하고 있는가?

→ 고유식별정보 처리 가능 경우

① 정보주체로부터 고유식별정보 처리의 별도 동의를 받은 경우

② 법령에서 고유식별정보 처리를 요구하거나 허용하는 경우

→ 고유식별번호의 종류

① 주민등록번호 (법정주의)

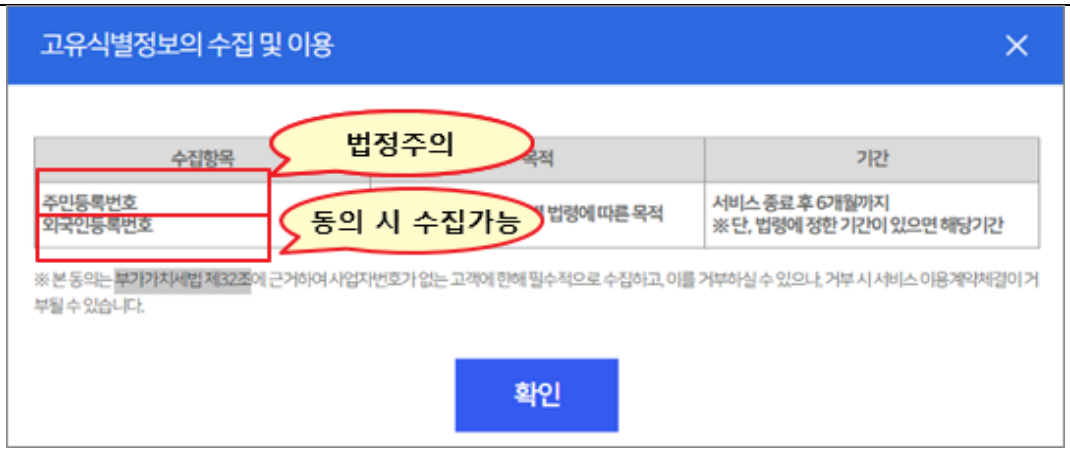
② 여권번호

③ 운전면허번호

④ 외국인등록번호

→ 고유식별정보 수집•활용동의 별도동의

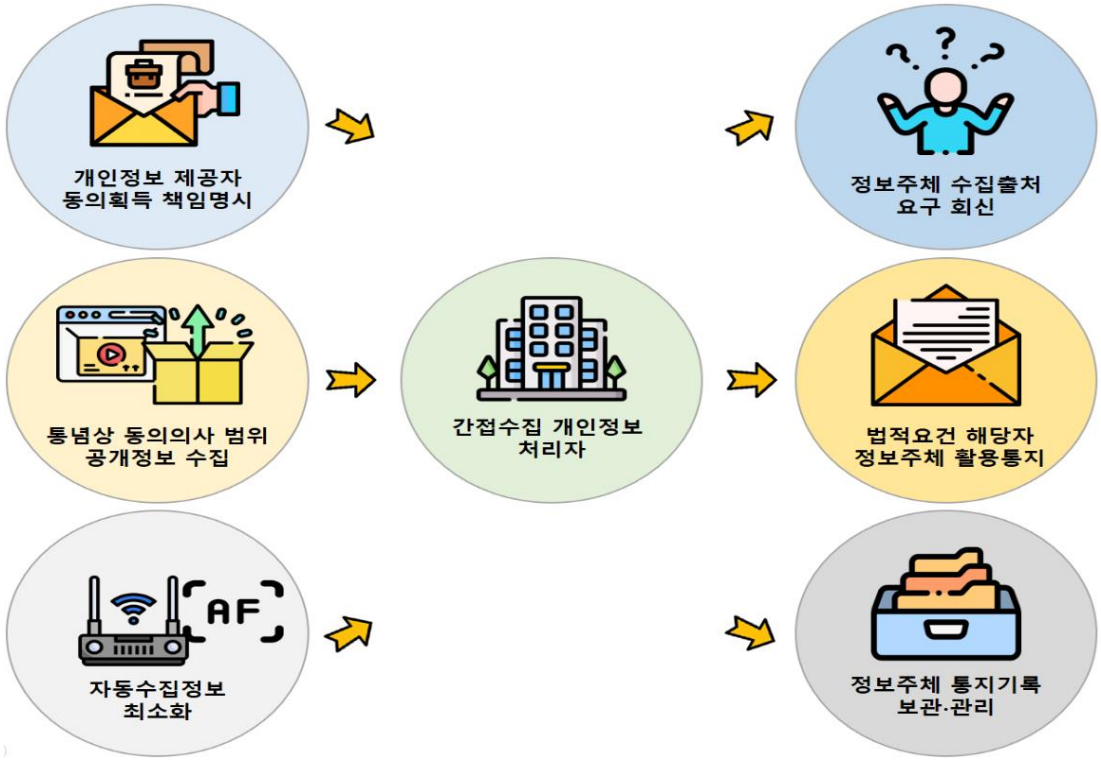
① 고유식별정보 수집•활용동의 [별도동의] (주민등록번호는 별도동의와 법정주의)



※ 출처: SK쉴더스 홈페이지 캡스홈 도어 가이드 온라인가입 화면(SK쉴더스)

※ 개인정보를 수집할 때는 필요한 최소한으로 수집하여야 하며, 수집 목적에 필요한 최소한의 개인정보 수집이라는 입증책임은 수집한 자의 부담

3.1.5 간접수집 보호조치

세부분야	3.1.5 간접수집 보호조치
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) 이외로부터 개인정보를 제공받는 경우 개인정보 수집에 대한 동의획득 책임이 개인정보를 제공하는 자에게 있음을 계약을 통하여 명시하고 있는가? • 공개된 매체 및 장소에서 개인정보를 수집하는 경우 정보주체(이용자)의 공개 목적·범위 및 사회 통념상 동의 의사가 있다고 인정되는 범위 내에서만 수집·이용하는가? • 서비스 계약 이행을 위하여 필요한 경우로서 사업자가 서비스 제공 과정에서 자동수집장치 등에 의하여 수집·생성하는 개인정보(이용내역 등)의 경우에도 최소수집 원칙을 적용하고 있는가? • 정보주체(이용자) 이외로부터 수집하는 개인정보에 대하여 정보주체(이용자)의 요구가 있는 경우 즉시 필요한 사항을 정보주체(이용자)에게 알리고 있는가? • 정보주체(이용자) 이외로부터 수집한 개인정보를 처리하는 경우 개인정보의 종류·규모 등이 법적 요건에 해당하는 경우 필요한 사항을 정보주체(이용자)에게 알리고 있는가? • 정보주체(이용자)에게 수집출처에 대하여 알린 기록을 해당 개인정보의 파기 시까지 보관·관리하고 있는가?
기준 요약도	
운영 방안	◇ 정보주체(이용자) 이외로부터 개인정보를 제공받는 경우 개인정보 수집에 대한 동의획득 책임이 개인정보를 제공하는 자에게 있음을 계약을 통하여

명시하고 있는가?

→ 개인정보를 제공받은 경우

① 개인정보를 제공하는 자에게 수집동의에 대한 입증책임이 있음을 계약에 명시

② 제공받은 개인정보를 목적에 맡게 사용하기 위해 문서에 제공받은 목적 구체화

≫ 개인정보를 제공받는 자의 성명(법인 또는 단체인 경우에는 그 명칭)

≫ 제공받는 자의 이용목적

≫ 제공하는 개인정보의 항목

≫ 제공받는 자의 개인정보 보유 및 이용기간

≫ 동의거부권이 있다는 사실 및 동의거부에 따른 불이익

◇ 공개된 매체 및 장소에서 개인정보를 수집하는 경우 정보주체(이용자)의 공개 목적·범위 및 사회 통념상 동의 의사가 있다고 인정되는 범위 내에서만 수집·이용하는가?

→ 공개된 매체를 통한 개인정보 수집 (예시)

① 상품거래 목적의 중고거래사이트 전화번호 기재

② 정보주체로 부터 직접 명함 또는 유사한 매체 제공

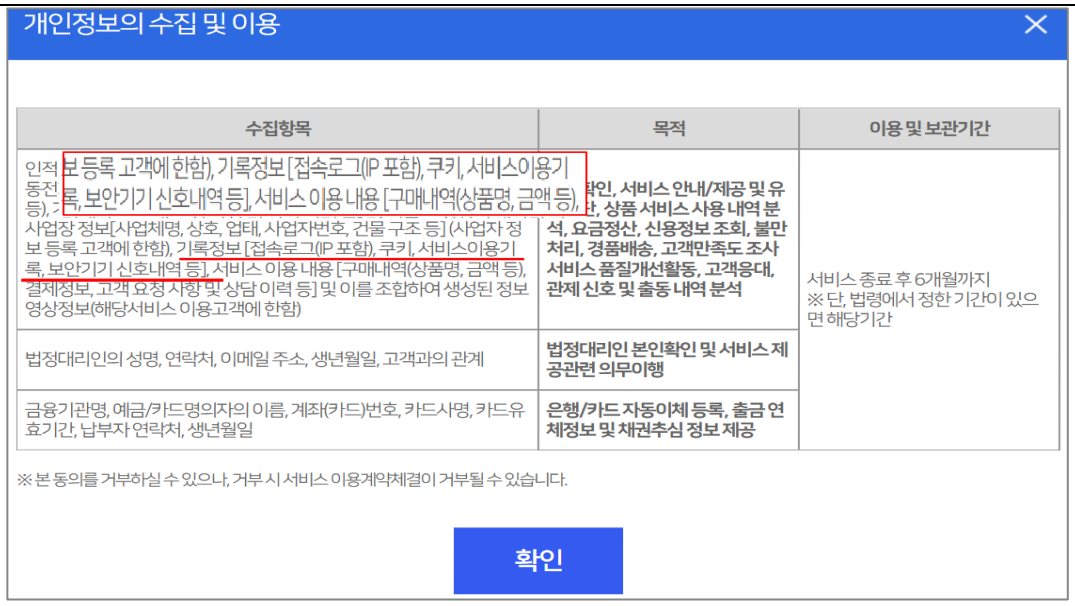
③ 업무처리를 위해 회사나 기관 공개 홈페이지등에 담당직원 회사번호나 이메일 등

※ 공개정보를 홍보나 마케팅등에 활용 목적으로 수집•가공•제공할 수 없음.

◇ 서비스 계약 이행을 위하여 필요한 경우로서 사업자가 서비스 제공 과정에서 자동 수집장치 등에 의하여 수집·생성하는 개인정보(이용내역 등)의 경우에도 최소수집원칙을 적용하고 있는가?

→ 자동수집 정보 동의사항

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(이용자) 이외로부터 수집하는 개인정보에 대하여 정보주체(이용자)의 요구가 있는 경우 즉시 필요한 사항을 정보주체(이용자)에게 알리고 있는가?

→ 수집 개인정보 정보주체 요구 시 알려야 할 사항

① 개인정보의 수집 출처

② 개인정보의 처리 목적

③ 개인정보 처리의 정지를 요구할 권리가 있다는 사실

◇ 정보주체(이용자) 이외로 부터 수집하는 개인정보에 대하여 정보주체의 필요한 사항을 정보주체에게 알리고 있는가?

→ 외부로 부터 수집을 정보주체의 알려야 할 경우

① 정보주체의 요구가 있는 경우

② 법적 요건에 해당하는 경우

≫ 5만 명 이상 정보주체에 관한 민감정보 또는 고유식별정보를 처리하는 자

≫ 100만 명 이상의 정보주체에 관한 개인정보를 처리하는 자

→ 정보주체의 알려야할 사항 및 시기

① 정보주체에게 알려야 할 사항

≫ 개인정보의 수집 출처

≫ 개인정보의 처리 목적

	≫ 개인정보 처리의 정지를 요구할 권리가 있다는 사실 ② 시기: 요구가 있은 날로부터 3일 이내 ≫ 고지로 인하여 다른 사람의 생명·신체를 해할 우려가 있는 등으로 인하여 정보주체의 요구를 거부하는 경우에는 정당한 사유가 없는 한 **◇ 정보주체(이용자)에게 수집출처에 대하여 알린 기록을 해당 개인정보의 파기 시까지 보관·관리하고 있는가?** **→ 수집출처 알린 기록 보관•관리 사항** ① 정보주체에게 알린 사실 ② 알린 시기 ③ 알린 방법

3.1.6 영상정보처리기기 설치·운영

세부분야	3.1.6 영상정보처리기기 설치·운영
인증 기준	영상정보처리기기를 공개된 장소에 설치·운영하는 경우 설치 목적 및 위치에 따라 법적 요구사항(안내판 설치 등)을 준수하고, 적절한 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 공개된 장소에 영상정보처리기기를 설치·운영할 경우 법적으로 허용한 장소 및 목적인지 검토하고 있는가? • 공공기관이 공개된 장소에 영상정보처리기기를 설치·운영하려는 경우 공청회·설명회 개최 등의 법령에 따른 절차를 거쳐 관계 전문가 및 이해관계자의 의견을 수렴하고 있는가? • 영상정보처리기기 설치·운영 시 정보주체가 쉽게 인식할 수 있도록 안내판 설치 등 필요한 조치를 하고 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 삭제하고 있는가? • 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우 관련 절차 및 요건에 따라 계약서에 반영하고 있는가?
기준 요약도	
운영 방안	◇ 공개된 장소에 영상정보처리기기를 설치·운영할 경우 법적으로 허용한 장소 및 목적인지 검토하고 있는가?

→ **공개된 장소**

공원, 도로, 지하철, 상가 내부, 주차장 등 불특정 다수가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소

→ **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 영상정보처리기기를 설치·운영하려는 경우 공청회·설명회 개최 등의 법령에 따른 절차를 거쳐 관계 전문가 및 이해관계자의 의견을 수렴하고 있는가?

→ **의견수렴 절차**

① 「행정절차법」에 따른 행정예고의 실시 또는 의견 청취

② 해당 영상정보처리기기의 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회. 설문조사

→ **의견수렴 방법**

① 일반인의 자유로운 출입이 제한되는 시설 및 장소: 해당시설을 이용하는 공무원 또는 임직원 등의 대표로 구성되는 위원회의 심의를 거쳐 설치

② 군사시설, 국가중요시설, 보안목표 시설 및 장소: 해당시설의 관리자 또는 관련 전문가의 의견수렴을 거쳐 설치

③ 이외 기타 일반 공공장소: 행정절차법에 따른 행정예고 또는 공청회 개최 및 CCTV 설치에 직접 영향을 받는 지역주민 등을 대상으로 하는 설명회, 설문조사, 여론조사 등을 통해 의견수렴을 거쳐 설치

→ **교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설에 영상정보처리기기를 설치하는 경우**

① 관계 전문가

② 해당 시설에 종사하는 사람, 해당 시설에 구금되어 있거나 보호받고 있는 사람 또는 그 사람의 보호자 등 이해관계인

→ **영상정보처리기기의 설치•목적 변경• 추가 설치하는 경우**

① 목적 변경에 따른 관계 전문가 및 이해관계인의 의견 수렴

② 안내판에 추가된 설치 목적 및 통합관리에 관한 내용을 기재

◇ 영상정보처리기기 설치·운영 시 정보주체가 쉽게 인식할 수 있도록 안내판 설치 등 필요한 조치를 하고 있는가?

→ 안내판 설치

① 안내판은 정보주체가 쉽게 알아볼 수 있는 출입구, 정문 등 눈에 잘 띄는 장소에 설치

② 건물 내, 공원 등 설치 장소에 따라 정보주체가 쉽게 판독할 수 있도록 안내판의 글자 크기와 높이를 조절하여 설치

→ 안내판 설치 예외

①「군사기지 및 군사시설 보호법」제2조제2호에 따른 군사시설

②「통합방위법」제2조제13호에 따른 국가중요시설

③「보안업무규정」제36조에 따른 보안목표시설

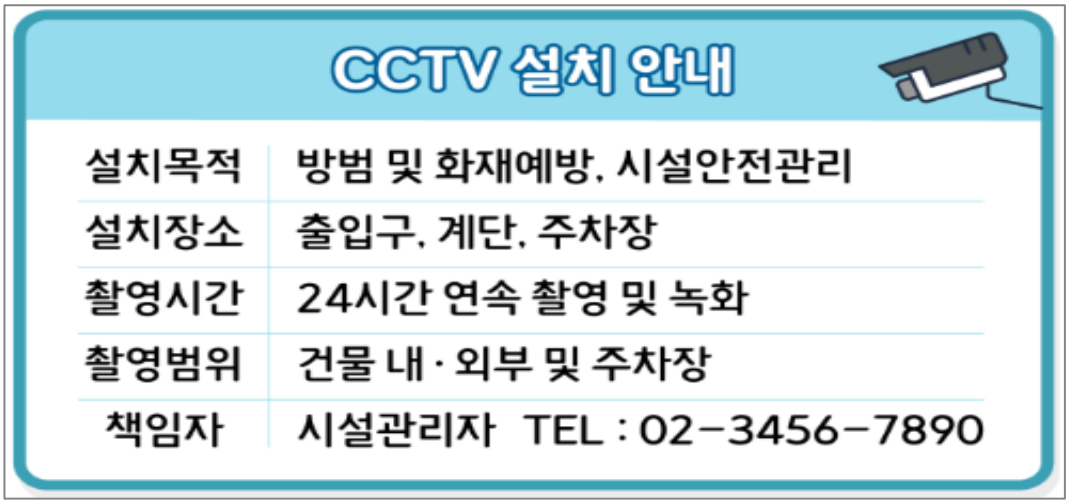
→ 안내판에 포함되어야 할 사항

① 설치 목적 및 장소

② 촬영 범위 및 시간

③ 관리책임자 이름 및 연락처

④ 위탁받은 자의 명칭 및 연락처(영상정보처리기기 설치·운영 사무 위탁)



※ 출처: 대한민국 개인정보 보호·활용 [개인정보보호위원회] 공식블로그

◇ 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 접근 권한이 있는 사람

④ 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법

⑤ 영상정보 확인 방법 및 장소

⑥ 정보주체의 영상정보 열람 등 요구에 대한 조치

⑦ 영상정보 보호를 위한 기술적. 관리적 및 물리적 조치

⑧ 그 밖에 영상정보처리기기의 설치. 운영 및 관리에 필요한 사항

→ 인터넷 홈페이지에 게재하여 정보주체에게 공개

※ 출처: SK쉴더스 홈페이지(SK쉴더스)

→ 영상정보처리기기가 설치된 목적외 사용 금지

① 영상정보처리기기의 녹음 기능 금지

② 영상정보처리기기의 임의 조작 기능 금지

◇ 영상정보의 보관 기간을 정하고 있으며, 보관 기간 만료 시 지체 없이 삭제하고 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

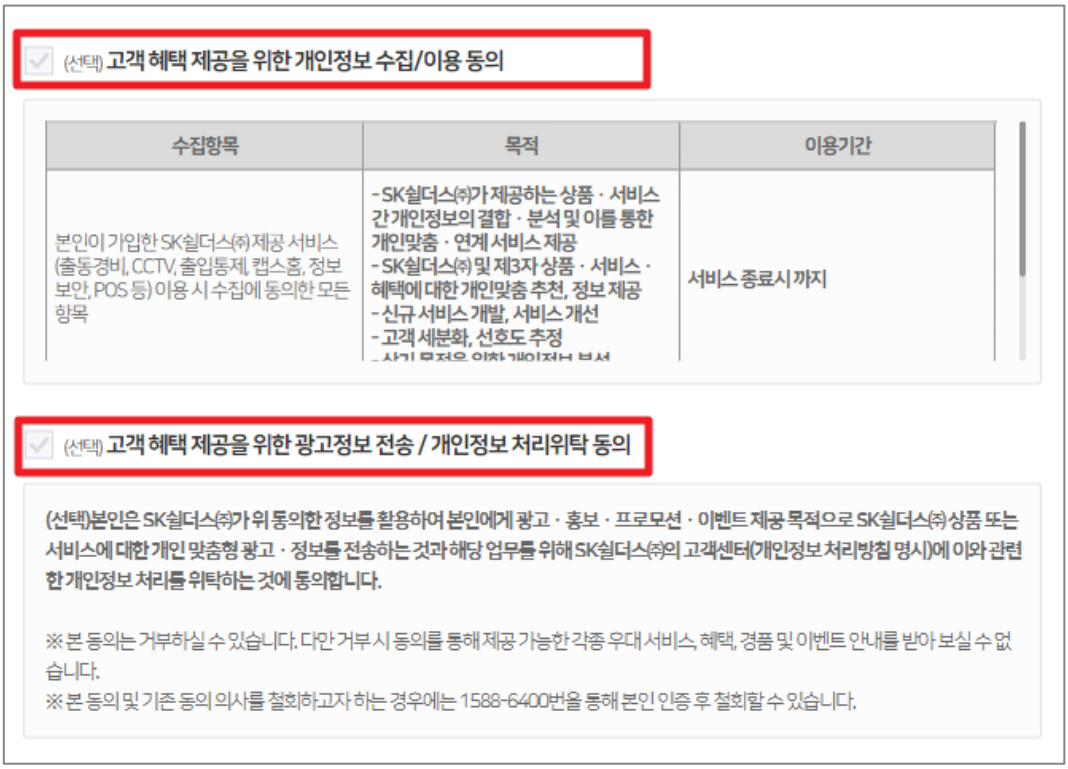
⑤ 위탁받는 자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

3.1.7 홍보 및 마케팅 목적 활용 시 조치

세부분야	3.1.7 홍보 및 마케팅 목적 활용 시 조치
인증 기준	재화나 서비스의 홍보, 판매 권유, 광고성 정보전송 등 마케팅 목적으로 개인정보를 수집·이용하는 경우에는 그 목적을 정보주체(이용자)가 명확하게 인지할 수 있도록 고지하고 동의를 받아야 한다.
주요 확인사항	• 정보주체(이용자)에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보 처리에 대한 동의를 받는 경우 정보주체(이용자)가 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	◇ 정보주체(이용자)에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보 처리에 대한 동의를 받는 경우 정보주체(이용자)가 이를 명확하게 인지할 수 있도록 알리고 별도의 동의를 받고 있는가?

→ **명확한 마케팅 목적활용 별도동의**

① 마케팅 활용동의 [별도동의]



(선택) 고객 혜택 제공을 위한 개인정보 수집/이용 동의

수집항목	목적	이용기간
본인이 가입한 SK쉴더스㈜ 제공 서비스(출동경비, CCTV, 출입통제, 캡스홈, 정보보안, POS 등) 이용 시 수집에 동의한 모든 항목	- SK쉴더스㈜가 제공하는 상품 · 서비스 간 개인정보의 결합 · 분석 및 이를 통한 개인맞춤 · 연계 서비스 제공 - SK쉴더스㈜ 및 제3자 상품 · 서비스 · 혜택에 대한 개인맞춤 추천, 정보 제공 - 신규 서비스 개발, 서비스 개선 - 고객 세분화, 선호도 추정	서비스 종료시 까지

(선택) 고객 혜택 제공을 위한 광고정보 전송 / 개인정보 처리위탁 동의

(선택)본인은 SK쉴더스㈜가 위 동의한 정보를 활용하여 본인에게 광고 · 홍보 · 프로모션 · 이벤트 제공 목적으로 SK쉴더스㈜ 상품 또는 서비스에 대한 개인 맞춤형 광고 · 정보를 전송하는 것과 해당 업무를 위해 SK쉴더스㈜의 고객센터(개인정보 처리방침 명시)에 이와 관련한 개인정보 처리를 위탁하는 것에 동의합니다.

※ 본 동의는 거부하실 수 있습니다. 다만 거부 시 동의를 통해 제공 가능한 각종 우대 서비스, 혜택, 경품 및 이벤트 안내를 받아 보실 수 없습니다.
※ 본 동의 및 기존 동의 의사를 철회하고자 하는 경우에는 1588-6400번을 통해 본인 인증 후 철회할 수 있습니다.

※ 출처: SK쉴더스 공식 홈페이지(SK쉴더스)

※ 개인정보를 수집할 때는 필요한 최소한으로 수집하여야 하며, 수집 목적에 필요한 최소한의 개인정보 수집이라는 입증책임은 수집한 자의 부담

→ **개인정보 수집동의와 마케팅 목적활용동의 구별**

①「개인정보보호법」 제39조의3 제1항에서의 동의

≫ 필수 동의

≫ 선택동의 (마케팅 활용목적을 위한 동의)

②「정보통신망법」 제50조의 영리적 목적의 광고성 정보 전송 제한

≫ 영리목적의 광고성 정보를 전송하려면 명시적인 사전 동의를 받아야 한다

→ **정보주체가 알아보기 쉽도록 명확한 동의서 양식 구현**

① 글씨의 크기는 최소한 9포인트 이상으로 다른 내용보다 20퍼센트 이상 크게 하고, 글씨의 색깔, 굵기 또는 밑줄 등 명확한 구현

◇ 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 경우 수신자의 명시적인 사전 동의를 받고 있으며, 2년마다 정기적으로 수신자의 수신동의 여부를 확인하고 있는가?

→ **수신동의 여부를 확인하려는 자 명시사항**

① 전송자의 명칭

② 수신자의 수신동의 사실과 수신에 동의한 날짜

③ 수신동의에 대한 유지 또는 철회의 의사를 표시하는 방법

※ 출처: 불법스팸방지 안내서(개인정보보호위원회•KISA)

→ **정기적 수신동의 여부**

① 매 2년이 되는 해의 수신동의를 받은 날과 같은 날

② 수신자가 수신동의 여부 안내를 받은 후 아무런 의사표시를 하지 않는 경우 수신동의 의사가 그대로 유지

◇ 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 수신거부 의사 표시 대상자

≫ 수신거부 의사 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

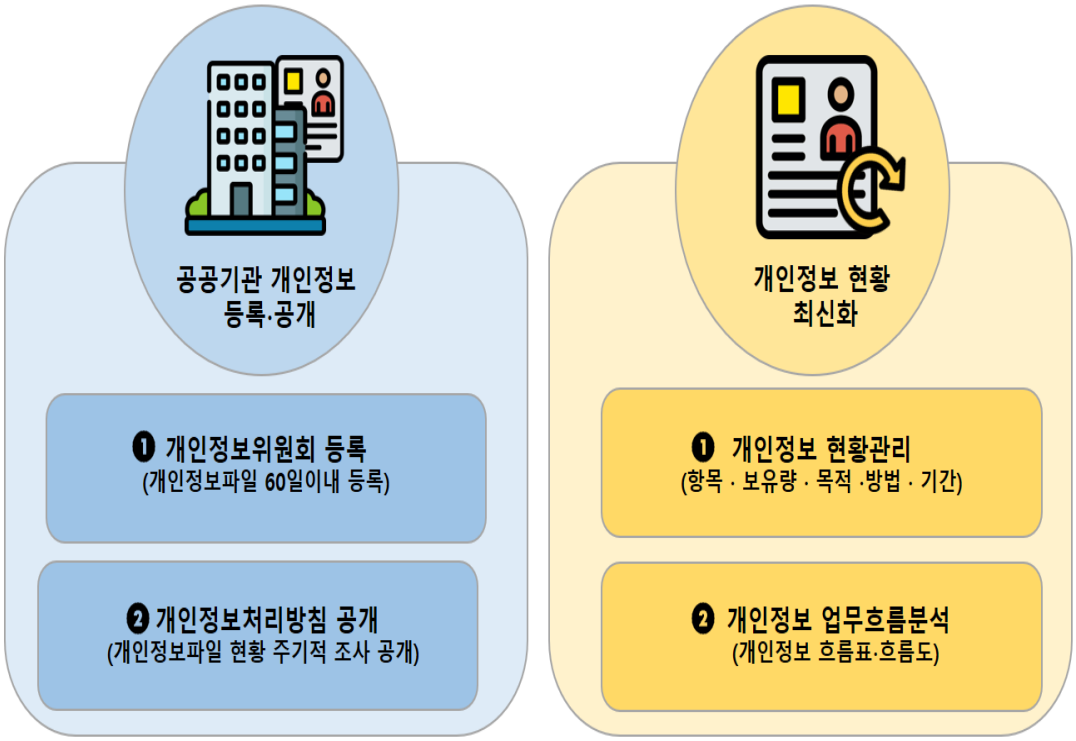
③ 통합회원으로 사전 동의를 받은 경우 수신거부시 통합회원에 대한 모든 동의 철회

◇ 영리목적의 광고성 정보를 전송하는 경우 전송자의 명칭, 수신거부 방법

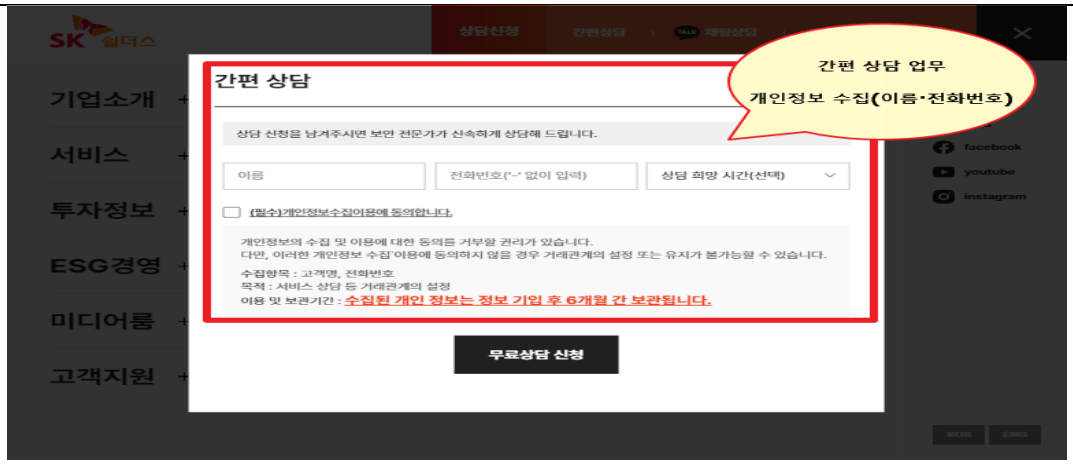
	등을 구체적으로 밝히고 있으며, 야간시간에는 전송하지 않도록 하고 있는가? **→ 광고성 정보 전송 시 명시사항** ① 전송자의 명칭 및 연락처 ② 수신의 거부 또는 수신동의의 철회 의사표시를 쉽게 할 수 있는 조치 및 방법에 관한 사항 **→ 야간광고 전송 제한 및 예외** ① 야간광고 제한: 오후 9시부터 그 다음 날 오전 8시까지 ② 예외사항: 전자우편 야간광고 가능

3.2 개인정보 보유 및 이용 시 보호조치

3.2.1 개인정보 현황관리

<table>
<tr><th>세부분야</th><th>3.2.1 개인정보 현황관리</th></tr>
<tr><td>인증
기준</td><td>수집·보유하는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하여야 하며, 공공기관의 경우 이를 법률에서 정한 관계기관의 장에게 등록하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 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 개인정보 처리방침에 공개하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 수집·보유하고 있는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하고 있는가?

→ 개인정보 생명주기(Life-Cycle) 흐름 파악
① 개인정보 수집 (예시)
≫ "간편 상담" 업무를 위해 "이름", "전화번호" 개인정보 수집</td></tr>
</table>



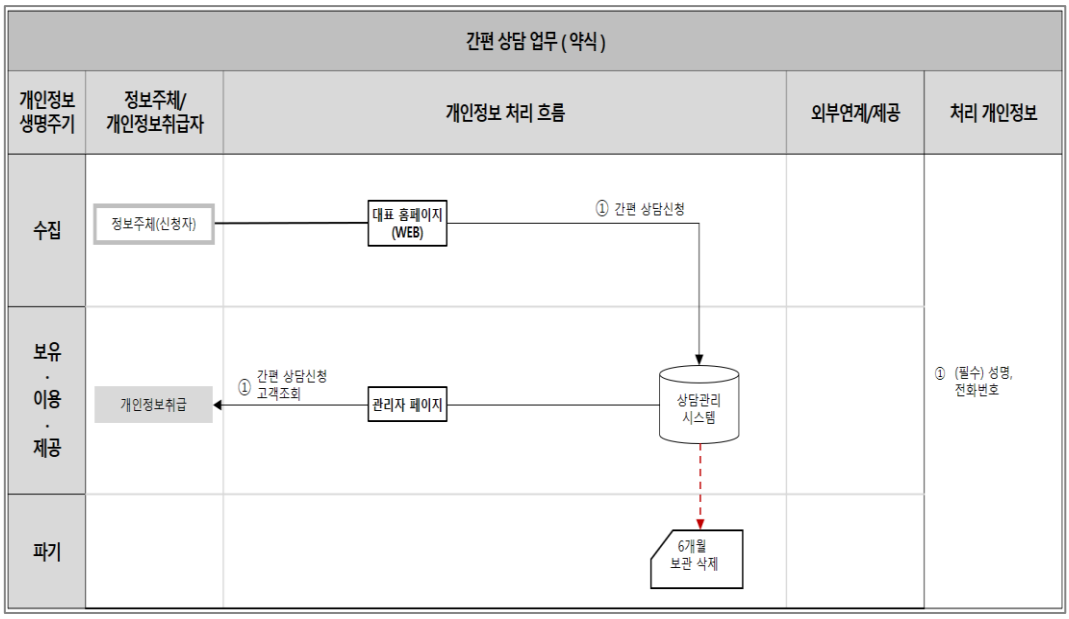
※ 출처: SK쉴더스 대표 홈페이지(SK쉴더스)

≫ "간편 상담"업무 개인정보 흐름표 약식

개인정보 흐름표 (약식 예시)

번호	업무	수집항목	수집경로	수집주기	수집부서	보관기간
1	간편상담	이름 / 전화번호	대표 홈페이지	상시	고객상담팀	6개월보관
2	…	…	…	…	…	…

≫ "간편 상담" 업무 개인정보 흐름도



② 개인정보 현황정리 관리

개인정보 처리 업무표 예시

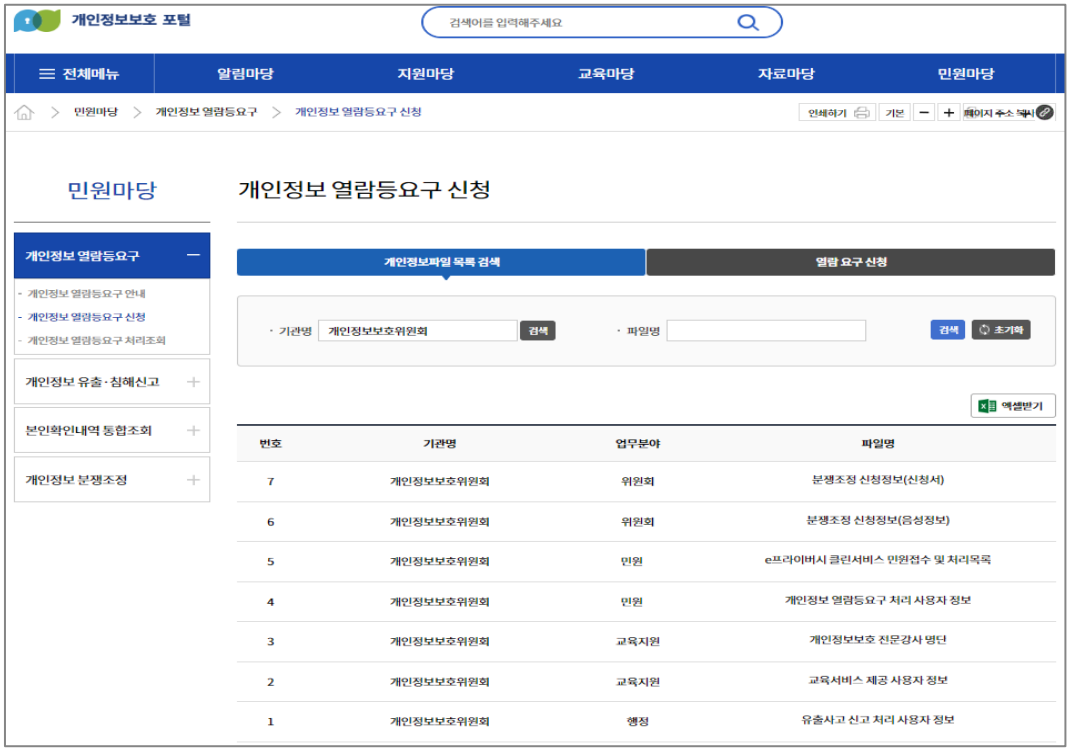
평가 업무명	처리 목적	처리 개인정보	주관 부서	개인정보 건수 (고유식별정보수)	개인정보 영향도
회원관리	홈페이지 회원가입, 본인확인, 정보제공 등 회원 서비스 제공	**필수** : 성명, 생년월일, 전화번호, 이메일주소, ID, 비밀번호 **선택** : 집주소, 집전화번호	민원팀	10만건 (0건)	5
상담업무	고객 문의 및 민원 응대	**필수** : 성명, 전화번호, 상담내용	민원팀	5천건 (0건)	3
실업급여 관리	실업급여 지급확인 및 관련 절차 알림, 확인	**필수** : 성명, 주민등록번호, 계좌번호, 전화번호 **선택** : 이메일주소	민원팀	3만건 (3만건)	5
…	…	…	…	…	…

※ 출처: 개인정보 영향평가 수행 안내서(개인정보보호위원회•KISA)

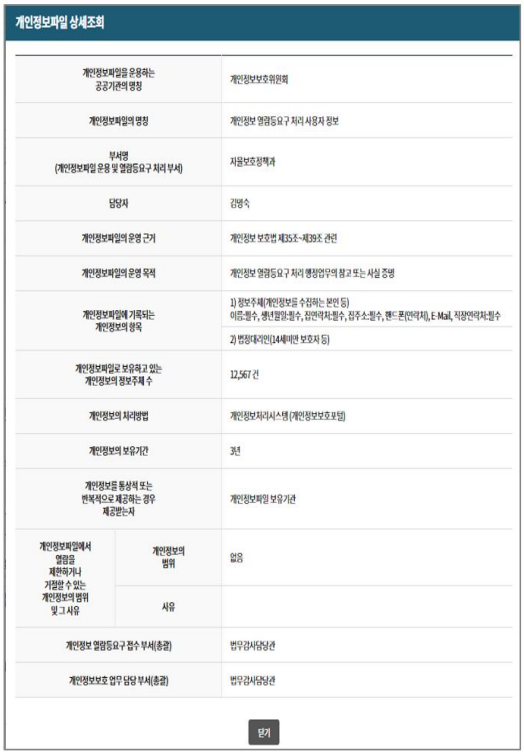
◇ 공공기관이 개인정보파일을 운용하거나 변경하는 경우 관련된 사항을 법률에서 정한 관계기관의 장에게 등록하고 있는가?

→ 공공기관 개인정보파일 운용 현황 등록

① 개인정보파일 등록 또는 변경 신청을 받은 개인정보 보호책임자는 등록·변경 사항을 검토하고 그 적정성을 판단한 후 개인정보보호위원회에 60일 이내에 등록



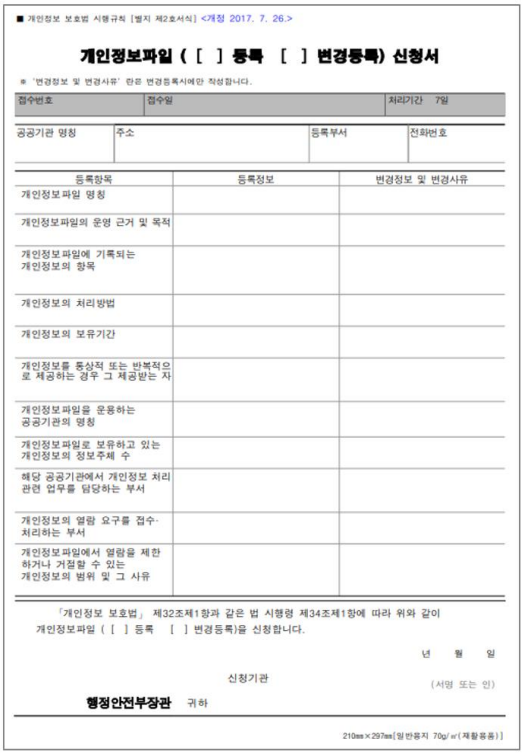
※ 출처: 개인정보보호포털(https://www.privacy.go.kr)



개인정보파일 상세조회

개인정보파일을 운용하는 공공기관의 명칭		개인정보보호위원회
개인정보파일의 명칭		개인정보 열람등요구 처리 사용자 정보
부서명 (개인정보파일 운용 및 열람등요구 처리 부서)		자율보호정책과
담당자		김영식
개인정보파일의 운영 근거		개인정보 보호법 제35조~제39조 관련
개인정보파일의 운영 목적		개인정보 열람등요구 처리 행정업무의 참고 또는 사실 증명
개인정보파일에 기록되는 개인정보의 항목		1) 정보주체(개인정보를 수집하는 본인 등) 이름-필수, 생년월일-필수, 집전화-필수, 집주소-필수, 핸드폰(연락처), E-Mail, 직장연락처-필수 2) 법정대리인(14세미만 보호자 등)
개인정보파일로 보유하고 있는 개인정보의 정보주체 수		12,567 건
개인정보의 처리방법		개인정보처리시스템 (개인정보보호포털)
개인정보의 보유기간		3년
개인정보를 통상적 또는 반복적으로 제공하는 경우 제공받는자		개인정보파일 보유기관
개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유	개인정보의 범위	없음
	사유	
개인정보 열람등요구 접수 부서(총괄)		법무감사담당관
개인정보보호 업무 담당 부서(총괄)		법무감사담당관

닫기



■ 개인정보 보호법 시행규칙 [별지 제2호서식] <개정 2017. 7. 26.>

개인정보파일 ([ ] 등록 [ ] 변경등록) 신청서

※ '변경정보 및 변경사유' 란은 변경등록시에만 작성합니다.

접수번호	접수일	처리기간 7일

공공기관 명칭	주소	등록부서	전화번호

등록항목	등록정보	변경정보 및 변경사유
개인정보파일 명칭		
개인정보파일의 운영 근거 및 목적		
개인정보파일에 기록되는 개인정보의 항목		
개인정보의 처리방법		
개인정보의 보유기간		
개인정보를 통상적 또는 반복적으로 제공하는 경우 그 제공받는 자		
개인정보파일을 운용하는 공공기관의 명칭		
개인정보파일로 보유하고 있는 개인정보의 정보주체 수		
해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서		
개인정보의 열람 요구를 접수·처리하는 부서		
개인정보파일에서 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 그 사유		

「개인정보 보호법」 제32조제1항과 같은 법 시행령 제34조제1항에 따라 위와 같이 개인정보파일 ([ ] 등록 [ ] 변경등록)을 신청합니다.

년 월 일

신청기관 (서명 또는 인)

행정안전부장관 귀하

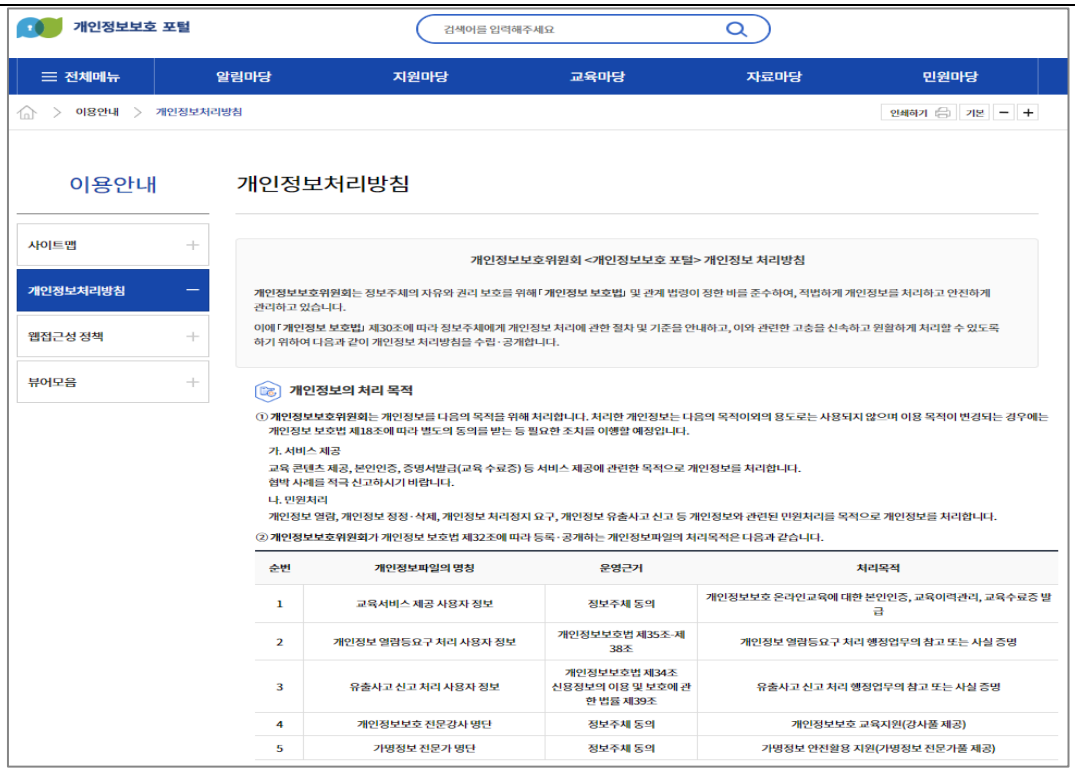
210mm×297mm[일반용지 70g/㎡(재활용품)]

※ 출처: 개인정보보호포털(https://www.privacy.go.kr)

◇ 공공기관은 개인정보파일의 보유 현황을 개인정보 처리방침에 공개하고 있는가?

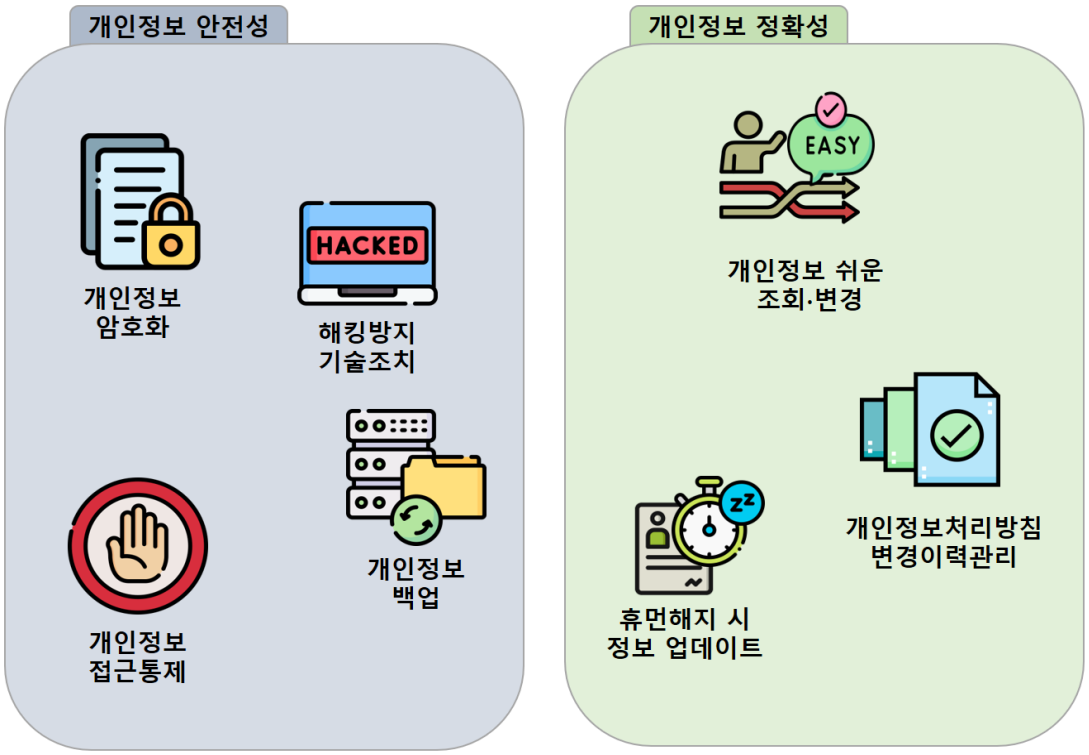
→ 공공기관의 개인정보파일 공개

① 공공기관의 개인정보 보호책임자는 개인정보파일의 보유·파기현황을 주기적으로 조사하여 그 결과를 해당 공공기관의 개인정보 처리방침에 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 정보주체(이용자)에게 관리절차를 제공하여야 한다.
주요 확인사항	• 수집된 개인정보는 내부 절차에 따라 안전하게 처리하도록 관리하며, 최신의 상태로 정확하게 유지하고 있는가? • 정보주체(이용자)가 개인정보의 정확성, 완전성 및 최신성을 유지할 수 있는 방법을 제공하고 있는가?
기준 요약도	
운영 방안	**◇ 수집된 개인정보는 내부 절차에 따라 안전하게 처리하도록 관리하며, 최신의 상태로 정확하게 유지하고 있는가?** **→ 개인정보 안전성 확보를 위한 보안조치** ① 개인정보 안정성 확보: 접근통제, 개인정보 암호화, 악성프로그램 방지, 물리적 접근방지 등 ② 개인정보 백업: 개인정보의 정확성·완전성을 확보할 수 있도록 백업·복구 등의 체계 구축 및 이행 **◇ 정보주체(이용자)가 개인정보의 정확성, 완전성 및 최신성을 유지할 수 있는**

방법을 제공하고 있는가?

→ 개인정보의 정확성·완전성 및 최신성을 유지할 수 있는 방법

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-2020.12(개인정보보호위원회•KISA)

④ 휴면 회원인 경우 휴면회원 해제 시 회원정보 업데이트 절차 마련

⑤ 정보주체가 수집 및 처리되는 개인정보의 현황을 쉽게 알 수 있도록 개인정보 처리방침의 변경과 이력관련 내용을 쉽게 인지할 수 있도록 게시

3.2.3 개인정보 표시제한 및 이용시 보호조치

세부분야	3.2.3 개인정보 표시제한 및 이용 시 보호조치
인증 기준	개인정보의 조회 및 출력(인쇄, 화면표시, 파일생성 등) 시 용도를 특정하고 용도에 따라 출력 항목 최소화, 개인정보 표시제한, 출력물 보호조치 등을 수행하여야 한다. 또한 빅데이터 분석, 테스트 등 데이터 처리 과정에서 개인정보가 과도하게 이용되지 않도록 업무상 반드시 필요하지 않은 개인정보는 삭제하거나 또는 식별할 수 없도록 조치하여야 한다
주요 확인사항	• 개인정보의 조회 및 출력(인쇄, 화면표시, 파일생성 등) 시 용도를 특정하고 용도에 따라 출력항목을 최소화하고 있는가? • 개인정보 표시제한 보호조치의 일관성을 확보할 수 있도록 관련 기준을 수립하여 적용하고 있는가? • 개인정보가 포함된 종이 인쇄물 등 개인정보의 출력·복사물을 안전하게 관리하기 위하여 필요한 보호조치를 하고 있는가? • 개인정보 검색 시 불필요하거나 과도한 정보가 조회되지 않도록 일치검색 또는 두 가지 항목 이상의 검색조건을 요구하고 있는가? • 개인정보를 가명처리하여 이용·제공 시 추가 정보의 사용·결합 없이 개인을 알아볼 수 없도록 적절한 방법으로 가명처리를 수행하고 있으며, 이에 대한 적정성을 평가하고 있는가? 또한, 다른 개인정보처리자 간의 가명정보 결합은 국가에서 지정한 전문기관을 통하고 있는가? • 가명정보를 처리하는 경우 추가 정보를 삭제 또는 별도로 분리하여 보관·관리하는 등 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하고 있는가? 또한, 가명정보의 처리내용을 관리하기 위하여 관련 기록을 작성·보관하고 있는가?
기준 요약도	

운영 방안

◇ 개인정보의 조회 및 출력(인쇄, 화면표시, 파일생성 등) 시 용도를 특정하고 용도에 따라 출력항목을 최소화하고 있는가?

→ 개인정보 조회 업무 권한 최소화

① 개인정보 조회 및 출력의 권한을 최소화하고 불가피하게 사용할 경우 마스킹 해지기능 적용

≫ 정보통신서비스 제공자등이 이용자의 개인정보 보호를 위해 개인정보를 마스킹하여 표시하는 조치를 취할 때 마스킹 방식에관한 일관된 기준을 따를 수 있도록 권고하는 사항으로서 의무적 적용사항은 아님

→ 설개개발오류 및 개인정보 취급 부주의

① 기능적오류: 개인정보 소스코드 노출 금지

※ 출처: 홈페이지 개인정보 노출방지 안내서(개인정보보호위원회•KISA)

② 개인정보 취급자 부주의: 엑셀 숨겨진 필드 처리, 공개된 게시판 개인정보 고지 등

③ 정보주체 부주의: 공개게시판 개인정보 작성 등

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

→ 일관성 있는 마스킹 처리

① 마스킹 표시제한 기준수립과 일관성 있는 적용

표시 제한 조치 (예시)

☞ 성명: 홍*동
☞ 연락처: 010-****-1234
☞ 주소: 서울시 송파구 중대로 **
☞ 접속지 IP: 123.123.***.123

구분	㉠시스템	㉡시스템
성명	홍길동	홍길동
연락처	010-****-5678	010-1234-****
주소	송파구 중대로 1	송파구 중대로 1

☞ 위와 같이 연락처를 다른 방식으로 마스킹 할 때 개인정보취급자가 ㉠,㉡시스템을 통하여 홍길동의 연락처가 02-1234-5678 이라는 것을 확인할 수 있으므로 동일한 방식의 표시제한 조치를 권고한다.

※ 출처: 개인정보 기술적 관리적 보호조치 기준(개인정보보호위원회•KISA)

◇ 개인정보가 포함된 종이 인쇄물 등 개인정보의 출력·복사물을 안전하게 관리하기 위하여 필요한 보호조치를 하고 있는가?

→ 출력 복사물 보호조치 정책(예시)

① 개인정보 다운로드 시 표시제한 조치의 일관성 확보

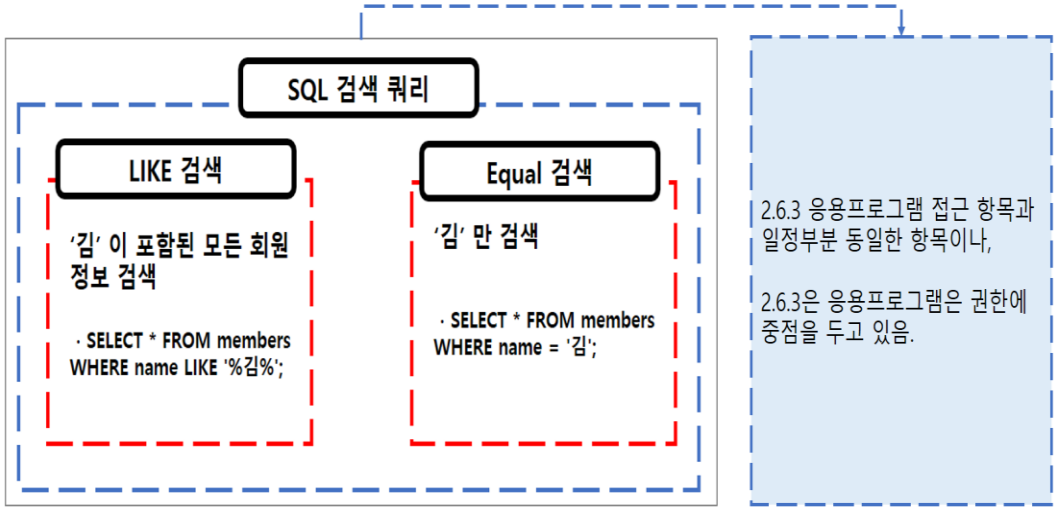
※ 파일 다운로드 시 개인정보 표시 일관성 유지(이해를 돕기 위한 예시)

◇ 개인정보 검색 시 불필요하거나 과도한 정보가 조회되지 않도록 일치검색 또는 두 가지 항목 이상의 검색조건을 요구하고 있는가?

→ LIKE검색 설정 제한

① LIKE 검색: 특정 문자로 해당 내역 전체 검색 "%"

② equal 검색: 2가지 항목 이상의 검색조건 사용



※ 라이크 검색(이해를 돕기 위한 예시)

◇ 개인정보를 가명처리하여 이용·제공 시 추가 정보의 사용·결합 없이 개인을 알아볼 수 없도록 적절한 방법으로 가명처리를 수행하고 있으며, 이에 대한 적정성을 평가하고 있는가? 또한, 다른 개인정보처리자 간의 가명정보 결합은 국가에서 지정한 전문기관을 통하고 있는가?

→ 가명정보 처리 법적근거

① 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 이용, 제공, 결합 등 처리

> **제28조의2(가명정보의 처리 등)** ① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.
>
> **제28조의3(가명정보의 결합 제한)** ① 제28조의2에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.

※ 출처: 가명정보처리가이드라인(개인정보보호위원회)

◇ 가명정보를 처리하는 경우 추가 정보를 삭제 또는 별도로 분리하여 보관·관리하는 등 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하고 있는가? 또한, 가명정보의 처리내용을 관리하기 위하여 관련 기록을 작성·보관하고 있는가?

→ 가명정보 관리적 보호조치

① 내부 관리계획의 수립, 수탁자 관리·감독 등의 관리적 보호조치

제29조의5(가명정보에 대한 안전성 확보 조치) ① 개인정보처리자는 법 제28조의4 제1항에 따라 가명정보 및 가명정보를 원래의 상태로 복원하기 위한 추가 정보(이하 이 조에서 "추가정보"라 한다)에 대하여 다음 각 호의 안전성 확보 조치를 해야 한다.

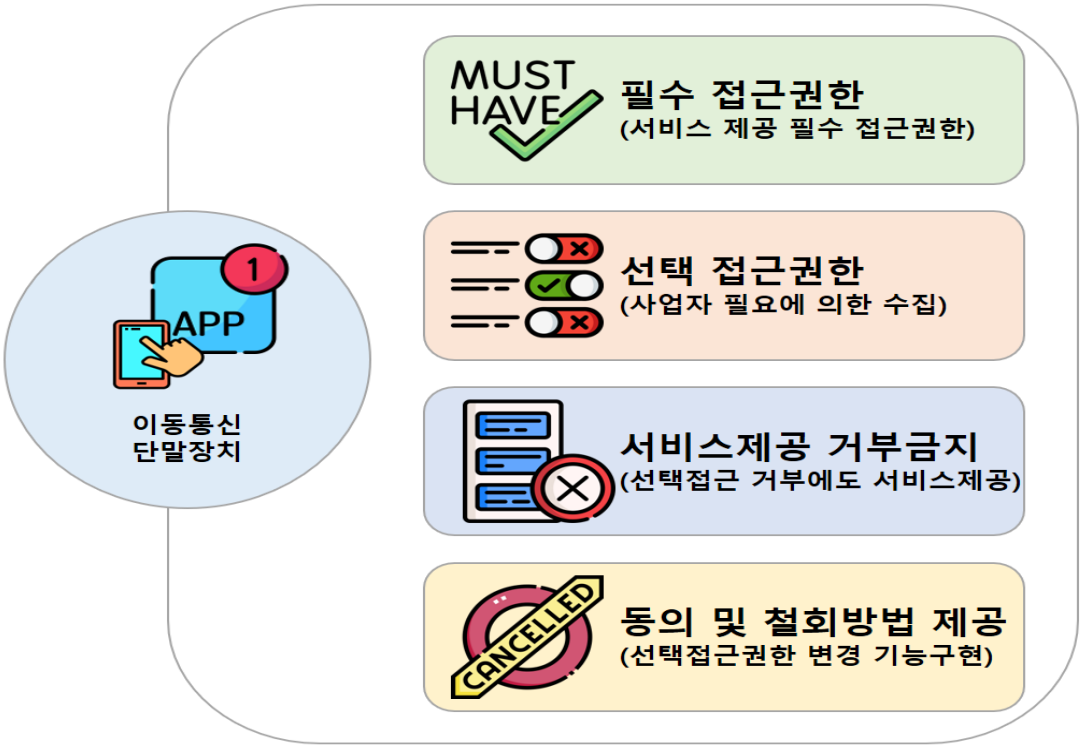
1. 제30조 또는 제48조의2에 따른 안전성 확보조치
2. 가명정보와 추가정보의 분리 보관. 다만, 추가정보가 불필요한 경우에는 추가정보를 파기해야 한다.
3. 가명정보와 추가정보에 대한 접근 권한의 분리. 다만, 「소상공인 보호 및 지원에 관한 법률」 제2조에 따른 소상공인으로서 가명정보를 취급할 자를 추가로 둘 여력이 없는 경우 등 접근 권한의 분리가 어려운 정당한 사유가 있는 경우에는 업무 수행에 필요한 최소한의 접근 권한만 부여하고 접근 권한의 보유 현황을 기록으로 보관하는 등 접근 권한을 관리·통제해야 한다.

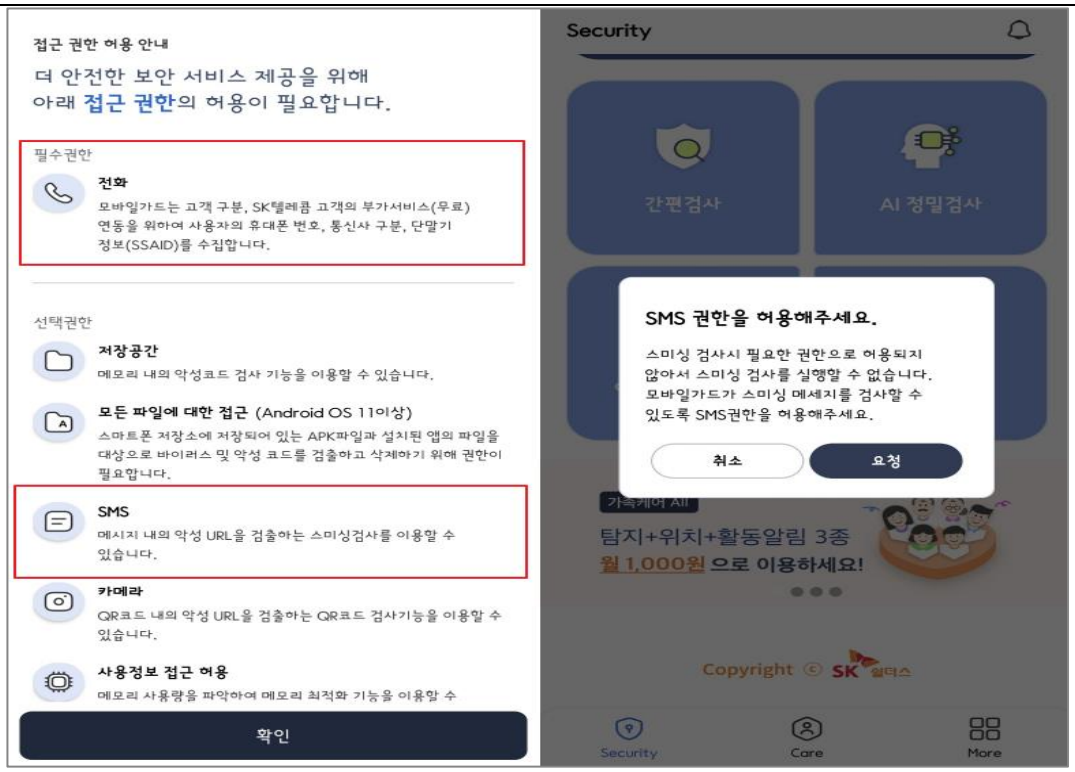
② 법 제28조의4제2항에서 "대통령령으로 정하는 사항"이란 다음 각 호의 사항을 말한다.

1. 가명정보 처리의 목적
2. 가명처리한 개인정보의 항목
3. 가명정보의 이용내역
4. 제3자 제공 시 제공받는 자
5. 그 밖에 가명정보의 처리 내용을 관리하기 위하여 보호위원회가 필요하다고 인정하여 고시하는 사항

※ 출처: 가명정보처리가이드라인(개인정보보호위원회)

3.2.4 이용자 단말기 접근 보호

세부분야	3.2.4 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?** **→ 필수•선택권한 동의** ① 스마트폰 필수적 접근권한과 선택적 접근권한을 각각 동의필요



※ 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?

→ 선택권한의 미동의

① 서비스에 필요한 최소한의 접근권한만을 허용하고 선택접근권한 거부 시에도 서비스 제공

※ 출처: SK쉴더스 모바일가드 스마트폰 앱 (SK쉴더스)

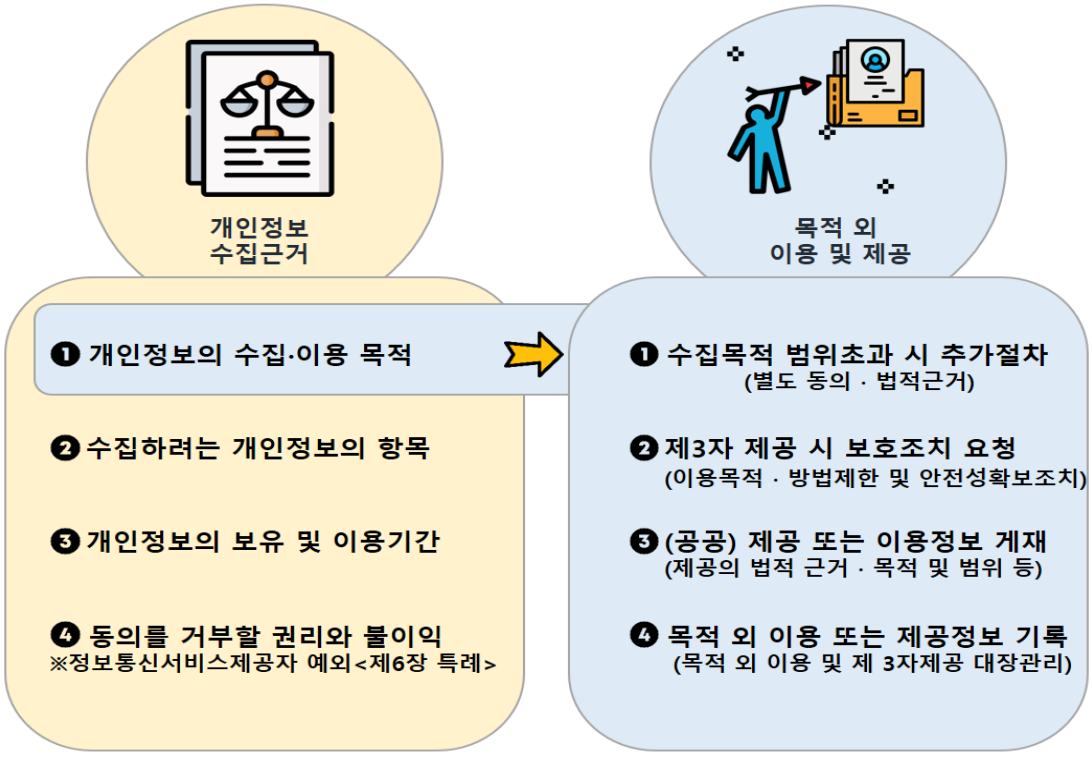
◇ 이동통신단말장치 내에서 해당 접근권한에 대한 정보주체(이용자)의 동의 및 철회방법을 마련하고 있는가?

→ 운영체제 공급자 동의철회 기능제공

① 운영체제(IOS, Android 등)별 동의 철회 기능 구현

※ 출처: 스마트폰 앱 접근권한 안내서 리플렛(방송통신위원회•KISA)

3.2.5 개인정보 목적 외 이용 및 제공

세부분야	3.2.5 개인정보 목적 외 이용 및 제공
인증 기준	개인정보는 수집 시의 정보주체(이용자)에게 고지·동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용·제공하려는 때에는 정보주체(이용자)의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 개인정보는 최초 수집 시 정보주체(이용자)로부터 동의받은 목적 또는 법령에 근거한 범위 내에서만 이용·제공하고 있는가? • 개인정보를 수집 목적 또는 범위를 초과하여 이용하거나 제공하는 경우 정보주체로부터 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? • 공공기관이 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하는 경우 목적 외 이용 및 제3자 제공대장에 기록·관리하고 있는가?
기준 요약도	
운영 방안	◇ 개인정보는 최초 수집 시 정보주체(이용자)로부터 동의받은 목적 또는 법령에 근거한 범위 내에서만 이용·제공하고 있는가?

→ **이용•제공 목적의 동의 받은 범위나 법령에 의해 이용**

① 개인정보 수집 시 동의나 다른법령 명시등의 목적 범위를 벗어나서 개인정보를 이용하거나 제공해서는 안 된다.

※ 출처: SK쉴더스 문의사항(SK쉴더스)

◇ 개인정보를 수집 목적 또는 범위를 초과하여 이용하거나 제공하는 경우 정보주체(이용자)로부터 별도의 동의를 받거나 법적 근거가 있는 경우로 제한하고 있는가?

→ **목적 외 이용 및 제공 동의사항**

① 목적 외 이용 시

≫ 개인정보의 이용목적

≫ 이용하는 개인정보의 항목

≫ 개인정보 보유 및 이용기간

≫ 동의거부권이 있다는 사실 및 동의거부에 따른 불이익이 있을 시 그 내용

② 목적 외 제3자 제공 시

≫ 개인정보를 제공받는 자

≫ 개인정보를 제공받는 자의 이용 목적

≫ 제공하는 개인정보의 항목

≫ 제공받는 자의 개인정보 보유 및 이용기간

≫ 동의거부권이 있다는 사실 및 동의거부에 따른 불이익이 있을 시 그 내용

→ **다른 법령에 의한 규정**

'법률'로 한정되어 있으므로 법률에 위임근거가 없고 시행령. 시행규칙에만 관련 규정이 있는 경우에는 허용되지 않음. '특별한 규정'에 한하므로 '법령상 의무이행과 같이 포괄적으로 규정된 경우에도 허용되지 않음.

◇ 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 전성 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?

→ **공개방법**

① 목적 외 이용 등을 한날부터 30일 이내

② 관보 또는 홈페이지 게재(홈페이지의 경우 10일 이상)

→ **공개의 예외**

① 정보주체로부터 별도의 동의를 받은 경우

② 범죄의 수사와 공소의 제기 및 유지를 목적

→ **필수 공개사항**

① 이용 또는 제공의 일자

② 이용 또는 제공의 법적 근거

③ 이용 또는 제공의 목적

④ 이용 또는 제공하는 개인정보의 항목

○○ 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 (개인정보보호 위원회)

◇ 공공기관이 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공하는 경우 목적 외 이용 및 제3자 제공대장에 기록·관리하고 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: 개인정보 보호법 시행규칙 [별지 제1호서식]

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 정보주체(이용자)의 동의를 받아야 하며, 제3자에게 개인정보의 접근을 허용하는 등 제공 과정에서 개인정보를 안전하게 보호하기 위한 보호대책을 수립·이행하여야 한다.
주요 확인사항	• 개인정보를 제3자에게 제공하는 경우 법령에 규정이 있는 경우를 제외하고는 정보주체에게 관련 내용을 명확하게 고지하고 동의를 받고 있는가? • 개인정보의 제3자 제공 동의는 수집·이용에 대한 동의와 구분하여 받고 이에 동의하지 않는다는 이유로 해당 서비스의 제공을 거부하지 않도록 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?
기준 요약도	
운영 방안	◇ 개인정보를 제3자에게 제공하는 경우 법령에 규정이 있는 경우를 제외하고는 정보주체(이용자)에게 관련 내용을 명확하게 고지하고 동의를 받고 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

→ **정보주체의 동의를 받은 경우 동의 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)

◇ 개인정보의 제3자 제공 동의는 수집·이용에 대한 동의와 구분하여 받고 이에 동의하지 않는다는 이유로 해당 서비스의 제공을 거부하지 않도록 하고 있는가?

→ **개인정보의 제3자 제공 동의는 수집·이용에 동의사항**

① 제3자 제공 동의는 수집·이용에 대한 동의와 구분

※ 출처: SK쉴더스 홈페이지 캡스홈 도어 가이드 온라인가입 화면(SK쉴더스)

② 제3자 제공에서 "선택 제공동의" 거부 시에도 서비스 제공

≫ 필수 제공동의: 서비스 제공을 위해 필수적인 제공동의

≫ 선택 제공동의: 사업자의 편의에 의한 제공동의

◇ 개인정보를 제3자에게 제공하는 경우 제공 목적에 맞는 최소한의 개인정보 항목으로 제한하고 있는가?

→ **목적에 맞는 최소한의 개인정보 제공**

① 동의에 근거한 제3자 제공 시: 동의 시 고지한 제공 목적을 달성하기 위하여 필요한 최소한의 개인정보 항목만 제공하여야 함.

② 법령에 근거한 제3자 제공 시: 법률에서 구체적으로 명시하거나 해당 법령상 의무를 준수하기 위하여필요한 범위 내에서 최소한의 개인정보 항목만 제공하여야 함

◇ 개인정보를 제3자에게 제공하는 경우 안전한 절차와 방법을 통하여 제공하고 제공 내역을 기록하여 보관하고 있는가?

→ **개인정보 제3자 제공 시 안전한 절차**

① 개인정보에 대한 파기 의무, 기술적·관리적 보호조치 의무(고객 정보에 대한 접근범위 설정, 암호화 보관 등) 등

② 제3자 제공 기록 보관

≫ 제공받는 자

≫ 제공 일시

≫ 제공된 개인정보

	≫ 제공 목적 또는 근거 ≫ 제공자(담당자) 및 승인자 ≫ 제공 방법: 시스템 연계, 이메일 전송 등 ≫ 기타 필요한 정보 **◇ 제3자에게 개인정보의 접근을 허용하는 경우 개인정보를 안전하게 보호하기 위한 보호절차에 따라 통제하고 있는가?** **→ 제3자 제공 개인정보 보호절차** ① 권한이 있는 자만 접근할 수 있도록 안전한 인증 및 접근통제 조치 ② 전송구간에서의 도청을 방지하기 위한 암호화 조치 ③ 책임추적성을 확보할 수 있도록 접속기록 보존 등

3.3.2 업무 위탁에 따른 정보주체 고지

<table>
<tr><th>세부분야</th><th>3.3.2 업무 위탁에 따른 정보주체 고지</th></tr>
<tr><td>인증
기준</td><td>개인정보 처리업무를 제3자에게 위탁하는 경우 위탁하는 업무의 내용과 수탁자 등 관련사항을 정보주체(이용자)에게 알려야 하며, 필요한 경우 동의를 받아야 한다..</td></tr>
<tr><td>주요
확인사항</td><td>• 개인정보 처리업무를 제3자에게 위탁하는 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?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 개인정보 처리업무를 제3자에게 위탁하는 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</td></tr>
</table>

※ 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?

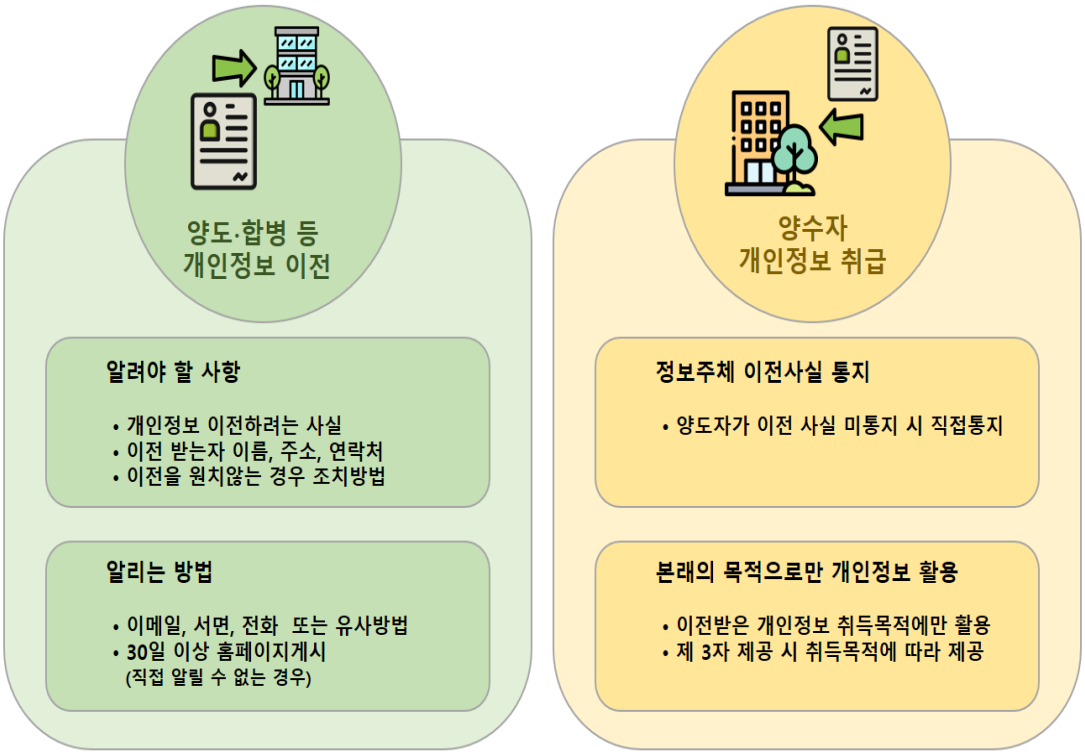
→ 재화 또는 홍보 위탁 시 정보주체 고지 법적근거

「**개인정보보호법**」 제26조(업무위탁에 따른 개인정보의 처리 제한)

≫ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다.

≫ 법 제26조 3항 전단에서 "대통령령으로 정하는 방법"이란 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(이하 "서면등의 방법"이라 한다)을 말한다

3.3.3 영업의 양수 등에 따른 개인정보의 이전

세부분야	3.3.3 영업의 양수 등에 따른 개인정보의 이전
인증 기준	영업의 양도·합병 등으로 개인정보를 이전하거나 이전받는 경우 정보주체(이용자) 통지 등 적절한 보호조치를 수립·이행하여야 한다.
주요 확인사항	• 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우 필요한 사항을 사전에 정보주체(이용자)에게 알리고 있는가? • 영업양수자 등은 법적 통지 요건에 해당될 경우 개인정보를 이전받은 사실을 정보주체(이용자)에게 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 정보주체(이용자)에게 알리고 있는가?** **→ 양도·합병 등으로 정보주체(이용자)에게 알려야하는 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)

◇ 영업양수자 등은 법적 통지 요건에 해당될 경우 개인정보를 이전받은 사실을 정보주체(이용자)에게 지체 없이 알리고 있는가?

→ 개인정보 이전 사실 통보

① 양도자가 이전 사실을 정보주체에게 알린 경우 양수자는 추가로 알리지 않아도 됨.

② 영업 양수 등에 따라 개인정보를 이전받았으나 개인정보를 이전하는 자가 이전한 사실을 알리지 않은 경우, 이전 사실을 정보주체(이용자)에게 알려야 함.

→ 알리는 방법

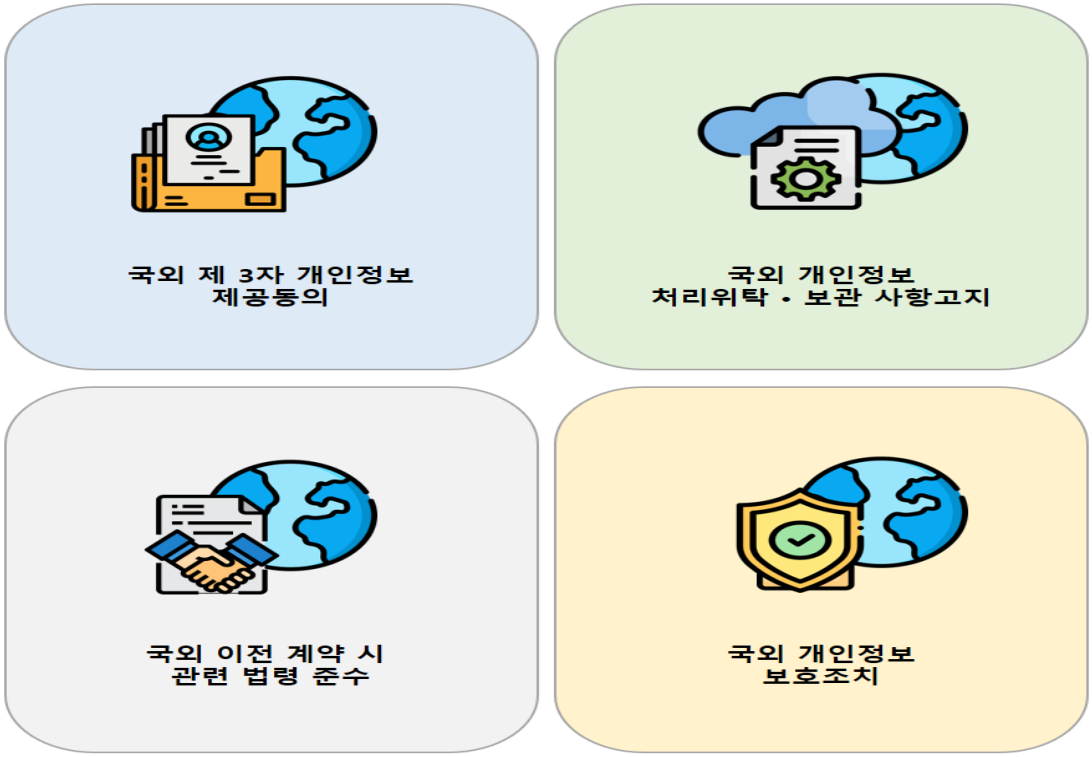
① 전자우편·서면·모사전송·전화 또는 이와 유사한 방법 중 어느 하나의 방법

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? → 양도·합병 등으로 정보주체(이용자)에게 알려야하는 사항 ① 개인정보를 이전받은 자가 당초의 목적 범위 외로 개인정보를 이용하거나 제공하고자 하는 경우에는 별도로 정보주체(이용자)의 동의를 받아야 함.

3.3.4 개인정보의 국외 이전

세부분야	3.3.4 개인정보의 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 국외의 제3자에게 제공하는 경우 정보주체(이용자)에게 필요한 사항을 모두 알리고 동의를 받고 있는가? • 정보통신서비스 제공자 등이 국외에 개인정보를 처리위탁 또는 보관 시 이전되는 개인정보의 항목, 이전되는 국가 등 필요한 사항을 모두 이용자에게 알리고 있는가? • 개인정보 보호 관련 법령 준수 및 개인정보 보호 등에 관한 사항을 포함하여 국외 이전에 관한 계약을 체결하고 있는가? • 개인정보를 국외로 이전하는 경우 개인정보 보호를 위하여 필요한 조치를 취하고 있는가?
기준 요약도	
운영 방안	**◇ 개인정보를 국외의 제3자에게 제공하는 경우 정보주체(이용자)에게 필요한 사항을 모두 알리고 동의를 받고 있는가?** **→ 개인정보 국외의 제3자 제공동의 고지사항** ① 개인정보를 제공받는 자 ② 개인정보를 제공받는 자의 개인정보 이용목적

③ 제공하는 개인정보의 항목

④ 개인정보를 제공받는 자의 개인정보 보유 및 이용기간

⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용

(예시) 여행계약 이행을 위한 제3자 제공

[개인정보 제3자제공 동의 획득 시 필수 안내 항목]
① 개인정보를 제공받는 자
(예 : ㅇㅇ렌터카, ㅇㅇ호텔)
② 개인정보를 제공받는 자의 개인정보 이용 목적
(예 : 숙박예약, 운송업체 탑승예약, 서비스 제공)
③ 제공하는 개인정보의 항목
(예 : 성명, 연락처)
④ 개인정보를 제공받는 자의 개인정보 보유 및 이용기간
(예 : 서비스 이용 종료 시 까지)
⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용
(예 : 동의를 거부하시면 렌터카 및 호텔 예약 서비스를 받을 수 없습니다.)

2	항공사/선박회사 등	항공예약/크루즈 예약	이름(한글, 영문), 성별, 생년월일, 여권(여권번호, 유효일자)	「출입국관리법」 제73조의2	불필요
3	대사관	비자발급	이름(한글, 영문), 성별, 생년월일, 여권(여권번호, 유효일자)	제3자 제공 동의(국외이전)	필요
4	숙박업체	숙소예약	이름(영문)	제3자 제공 동의(국외이전)	필요
5	현지여행사	현지여행가이드	이름(한글, 영문), 연락처	제3자 제공 동의(국외이전)	필요
6	렌터카업체	차량렌트	이름(한글, 영문), 연락처	제3자 제공 동의(국외이전)	필요
7	비자발급 대행사	비자발급 대행	이름(한글, 영문), 성별, 생년월일, 여권(여권번호, 유효일자)	제3자 제공 동의	필요

※ 출처: 자율규제단체 참여사를 위한 업종별 개인정보 처리가이드 여행업 (개인정보보호위원회·KISA)

◇ 정보통신서비스 제공자 등이 국외에 개인정보를 처리위탁 또는 보관 시 이전되는 개인정보의 항목, 이전되는 국가 등 필요한 사항을 모두 이용자에게 알리고 있는가?

→ 이용자에게 알려야 할 사항

개인정보의 국외 이전(제공, 위탁, 보관)은 개인정보 관련 보호 체계가 다른 제3의

국가로개인정보가 옮겨지는 것으로, 정보주체의 권리를 침해할 위험성이 높으므로, 개인정보의 제3자 제공, 위탁과 구분하여 처리방침에 기재하는 것이 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)

◇ 개인정보 보호 관련 법령 준수 및 개인정보 보호 등에 관한 사항을 포함하여 국외 이전에 관한 계약을 체결하고 있는가?

→ 국외 이전 시 보호조치 법령

「**개인정보보호법 시행령**」 제48조 10(개인정보 국외이전 보호조치)

개인정보를 국외에 이전하려는 경우에는 제1항 각 호의 사항에 관하여 이전받는 자와 미리 협의하고 이를 계약내용 등에 반영해야 한다.

① 개인정보 보호를 위한 안전성 확보 조치

② 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 조치

③ 그 밖에 이용자의 개인정보 보호를 위하여 필요한 조치

「**개인정보보호법** 」 제39조 12(국외 이전 개인정보의 보호)

정보통신서비스 제공자등은 제2항 본문에 따른 동의를 받아 개인정보를 국외로 이전하는 경우 대통령령으로 정하는 바에 따라 보호조치를 하여야 한다

① 개인정보 보호를 위한 안전성 확보 조치

② 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 조치

③ 그 밖에 이용자의 개인정보 보호를 위하여 필요한 조치

◇ 개인정보를 국외로 이전하는 경우 개인정보 보호를 위하여 필요한 조치를 취하고 있는가?

	→ 개인정보 국외 이전 시 적용하여야 하는 보호조치 ① 개인정보 보호를 위한 안전성 확보 조치 ② 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 조치 ③ 그 밖에 이용자의 개인정보 보호를 위하여 필요한 조치

3.4 개인정보 파기 시 보호조치

3.4.1 개인정보의 파기

세부분야	3.4.1 개인정보의 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 수집항목별, 수집목적별, 수집경로별로 보관장소(데이터베이스, 백업데이터 등), 파기방법, 파기시점 법령근거 등 현황 관리

수집 항목

평가 업무명[1]	수집					
	수집 항목[2]	수집 경로[3]	수집 대상[4]	수집 주기[5]	수집담당자[6]	수집 근거[7]
민원 처리	(필수) 성명, 주민등록번호, 전화번호, 이메일 주소, 민원 내용 (선택) 집전화번호	온라인 (홈페이지)	민원인	상시	-	이용자 동의/ 00법제0조0항 (주민등록번호)
		오프라인 (민원신청서 작성)	민원인	상시	안내창구 담당자	이용자 동의/ 00법제0조0항 (주민등록번호)

파기 절차

파기			
보관 기간[10]	파기 담당자[11]	파기 절차[12]	분리 보관 여부[13]
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 - 2020.12(개인정보보호위원회•KISA)

◇ 개인정보의 처리목적이 달성되거나 보유기간이 경과한 경우 지체 없이 해당 개인정보를 파기하고 있는가?

→ 개인정보 기한경과 및 목적달성

① 정보주체 동의 시 개인정보 목적 및 보유기간

≫ (예시) 간편 상담 업무 목적 개인정보 "이름","전화번호" 수집 6개월 보관 삭제

※ 출처: SK쉴더스 대표홈페이지 간편상담 신청(SK쉴더스)

개인정보처리방침

ADT캡스 | infosec

에스케이 쉴더스 주식회사(이하 "SK쉴더스"라고 한다)는 고객의 개인정보를 철저히 보호하고 있으며, "개인정보 보호법"과 "정보통신망 이용촉진 및 정보보호에 관한 법률"(이하 "정보통신망법") 등 개인정보보호관련 법률을 성실히 준수하고 있습니다. SK쉴더스는 개인정보처리방침을 홈페이지에 공개하여 고객이 언제나 쉽게 열람 할 수 있도록 하고 있습니다.

SK쉴더스의 개인정보처리방침은 관련 법률 및 지침의 변경 또는 내부 운영 방침의 변경에 따라 변경될 수 있으며, 변경이 있을 경우 회사 홈페이지 (www.skshieldus.com)를 통하여 공지하여 드립니다.

대상	필수 수집 항목	목적	이용 및 보관기간
사이버가드	인적정보(성명,생년월일,주소, 이동전화번호(통신사 포함), 유선전화번호, 이메일,긴급 연락처,신용정보 등),가입정보 (가입일, 기간, 해지 등)사업장 정보[사업체명,상호,업태, 사업자번호등]기록정보[접속로그(IP 포함), 쿠키, 서비스이용기록,보안기기 신호내역 등], 서비스 이용 내용 [구매내역(상품명,금액 등), 결제정보, 고객 요청 사항 및 상담 이력 등] 및 이를 조합하여 생성된 정보	본인확인, 서비스안내/제공및유지판단, 상품 서비스 사용 내역 분석,요금정산, 신용정보조회, 불만처리	서비스종료후 6개월까지 ※단, 법령에서 정한기간이있으면해당기간
	법정대리인의성명, 연락처, 이메일주소, 생년월일, 고객과의관계	법정대리인 본인확인 및 서비스 제공관련 의무이행	
	금융기관명, 예금/카드명의자의이름, 계좌(카드)번호, 카드사명,카드유효기간, 납부자연락처, 생년월일	은행/카드 자동이체 등록, 출금 연체정보 및 채권추심 정보 제공	

대상	필수 수집 항목	목적	이용 및 보관기간
대표 홈페이지	성명, 연락처	'상담신청', '간편AS접수', '고객소개제도' 등을 위한 본인확인	기입 후 6개월까지
	서비스 구분, 이름, 연락처, 고객의 소리(칭찬, 불만, 제안) 내용, 주소(선택 동의 항목에 동의한 경우에만 수집)	고객의 소리(칭찬, 불만, 제안) 접수 처리를 위한 본인확인, 통계 분석 데이터 활용을 통한 서비스 개선	기입 후 1년까지
	세금계산서, 청구서 재발행 요청 시 요청자 정보(계약번호, 상호명, 요청자 이름, 휴대폰 번호, 이메일 주소), 세금계산서 정보 변경 시 요청자 정보(계약번호, 상호명, 요청자 이름, 휴대폰 번호) 및 변경 요청 항목(대표자 이름, 상호, 업태, 종목, 주소, 사업자등록증)	서비스 계약자의 세금계산서 정보 변경 요청 및 세금계산서, 청구서 재발행 요청 처리	요청 업무 처리 완료 시 파기 (변경을 요청한 정보는 서비스 종료 후 6개월까지 보관)

※ 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

≫ 하드디스크, USB 메모리의 경우 '로우레벨포멧(Low level format)' 방법으로 파기

② 물리적인 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

③ 고객 서비스에 이용 중인 DB서버에 저장된 일부 데이터를 파기하는 경우

≫ 서비스 중인 DB의 해당 개인정보 위에 임의의 값(Null값 등)을 덮어쓰기한 후 삭제

≫ DB의 특정부분에 덮어쓰기가 곤란한 경우에는 테이블 데이터에 대한 논리적인 삭제(delete)도 허용되나, 신속하게 다른 데이터로 덮어쓰기될 수 있도록 운영

◇ 개인정보 파기에 대한 기록을 남기고 관리하고 있는가?

→ 개인정보 파기 기록

① 개인정보 파기 시행 및 파기결과 확인 개인정보 보호책임자 책임 하에 수행

② 파기관리대장 및 기록 증적기록물 보관

③ 공공기관은 파기관리대장 필수

≫ 구분(이용·제공·열람·파기)

≫ 일시

≫ 파일명/형태

≫ 담당자

≫ 목적/사유

≫ 이용·제공받은 제3자/열람 등 요구자

≫ 이용·제공 형태

≫ 기간

개인정보 파기 관리대장

번호	개인정보파일명	자료의 종류	생성일	폐기일	폐기사유	처리담당자	처리부서장

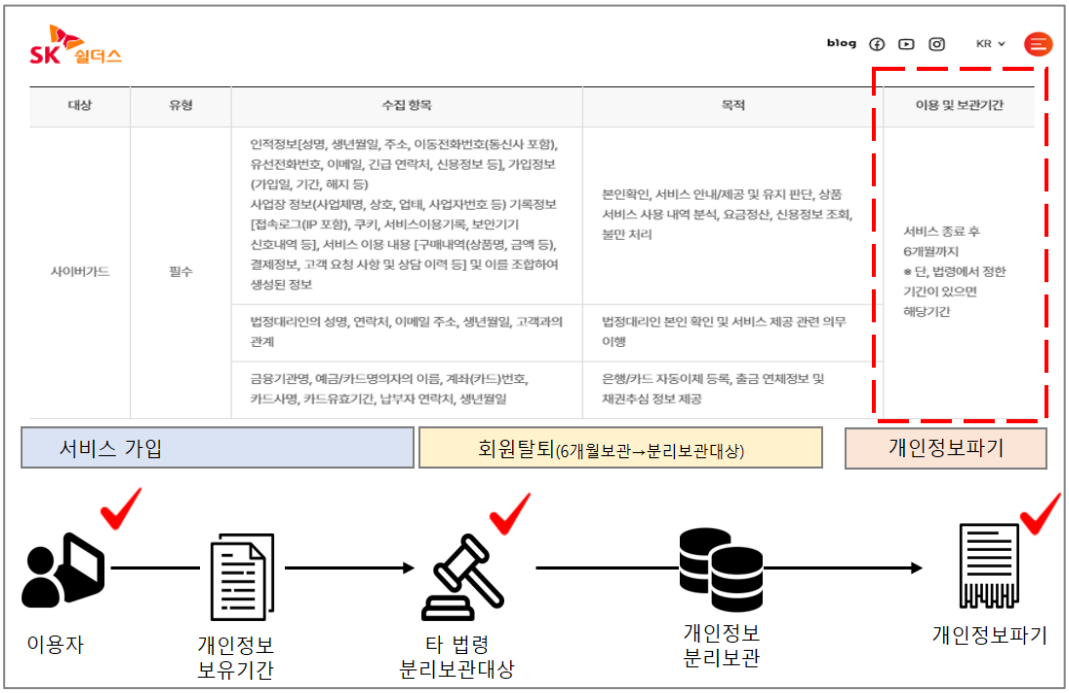
※ 개인정보파기관리대장(이해를 돕기 위한 예시)

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?

→ 타 법령에 따른 보유기간

① "사이버가드" 서비스 (예시)



※ 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?

→ 분리 보관 개인정보 관리

① 법령에서 정한 목적 범위 내에서만 처리

② 접근권한을 최소한의 인원으로 제한

③ 분리 데이터베이스에 대한 접속기록을 남기고 정기적으로 검토

◇ 분리 보관하고 있는 개인정보에 대하여 법령에서 정한 목적 범위 내에서만

처리 가능하도록 관리하고 있는가?

→ 개인정보의 항목을 보유목적에 맞는 최소한의 항목으로 제한

① 전자상거래 등에서 소비자 보호에 관한 법률

≫ 표시·광고에 관한 기록: 6개월

≫ 계약 또는 청약철회 등에 관한 기록: 5년

≫ 대금결제 및 재화 등의 공급에 관한 기록: 5년

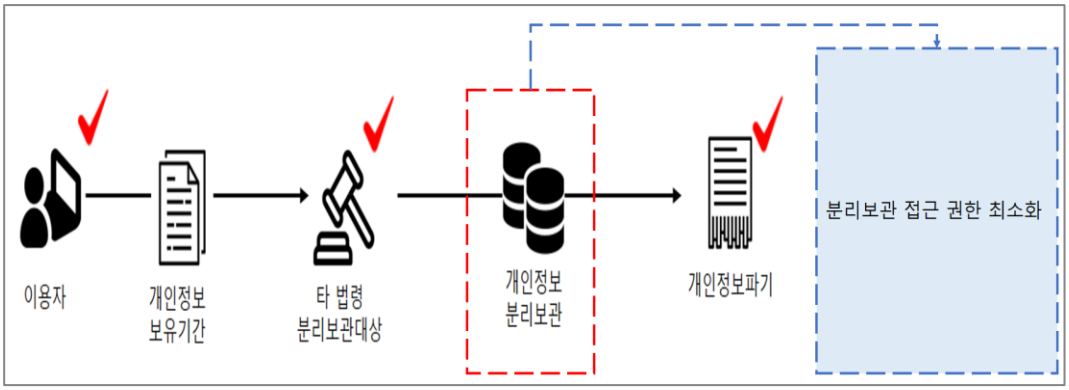
≫ 소비자의 불만 또는 분쟁처리에 관한 기록: 3년 법령에서 정한 목적 범위 내에서만 처리

◇ 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)

3.4.3 휴면 이용자 관리

<table>
<tr><th>세부분야</th><th>3.4.3 휴면 이용자 관리</th></tr>
<tr><td>인증
기준</td><td>서비스를 일정기간 동안 이용하지 않는 휴면 이용자의 개인정보를 보호하기 위하여 관련 사항의 통지, 개인정보의 파기 또는 분리보관 등 적절한 보호조치를 이행하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 정보통신서비스 제공자 등은 법령에서 정한 기간 동안 이용하지 않는 휴면 이용자의 개인정보를 파기 또는 분리 보관하고 있는가?
• 휴면 이용자의 개인정보를 파기하거나 분리하여 저장·관리하려는 경우 이용자에게 알리고 있는가?
• 분리되어 저장·관리하는 휴면 이용자의 개인정보는 법령에 따른 보관 목적 또는 이용자의 요청에 대해서만 이용 및 제공하고 있는가?
• 분리되어 저장·관리하는 휴면 이용자의 개인정보에 대하여 접근권한을 최소한의 인원으로 제한하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 정보통신서비스 제공자 등은 법령에서 정한 기간 동안 이용하지 않는 휴면 이용자의 개인정보를 파기 또는 분리 보관하고 있는가?

→ 유효기간제 대상자
「개인정보보호법」 제39조 6(개인정보 파기에 대한 특례)
≫ 정보통신서비스 제공자등은 정보통신서비스를 1년의 기간 동안 이용하지</td></tr>
</table>

아니하는 이용자

≫ 다만, 그 기간에 대하여 다른 법령 또는 이용자의 요청에 따라 달리 정한 경우에는 그에 따른다.

< 서비스 미이용 기간 선택 기능 제공 예시 >

(예시①) 개인정보를 파기 또는 분리 저장·관리하여야 하는 서비스 미이용 기간을 ☐년으로 요청합니다.

※ 다만, 별도의 요청이 없을 경우 서비스 미이용 기간은 1년으로 합니다.

(예시②) 개인정보를 파기 또는 분리 저장·관리하여야 하는 서비스 미이용 기간을

2년 ☐ 3년 ☐ 회원 탈퇴 시까지 ☐ 으로 요청합니다.

※ 다만, 별도의 요청이 없을 경우 서비스 미이용 기간은 1년으로 합니다.

※ 출처: 개인정보 보호 법령 및 지침, 고시해설서 (개인정보보호 위원회)

→ 개인정보 분리•파기

① 개인정보 분리보관: 물리적분리 또는 논리적분리(테이블분리)

≫ 물리적•논리적 분리 시 엄격한 접근통제 및 외부해킹방지 등 보호조치

≫ 분리된 개인정보 4년간 보관 후 지체 없이 파기

② 개인정보 파기: 전체데이터파기 또는 일부데이터파기

≫ 전체데이터 파기: 복구 불가능 형태로 파기(백업 데이터 누락없이 파기)

≫ 일부데이터 파기: 개인정보 덮어쓰기(Null) 또는 삭제(delete)

◇ 휴면 이용자의 개인정보를 파기하거나 분리하여 저장·관리하려는 경우 이용자에게 알리고 있는가?

→ 휴면 이용자 개인정보 분리보관•파기 통지

① 통지 시기: 서비스 미이용 기간 만료 30일 전까지

② 통지 방법: 전자우편, 서면, 모사전송(팩스), 전화 등의 방법 중 하나를 선택

③ 통지 항목

≫ 개인정보를 파기하는 경우: 개인정보가 파기되는 사실, 기간 만료일 및 파기되는 개인정보의 항목

≫ 개인정보를 분리하여 저장·관리하는 경우: 개인정보가 분리되어 저장·관리되는 사실, 기간 만료일 및 분리·저장되어 관리되는 개인정보의 항목

※ 정보통신서비스 제공자등이 이용자의 연락처를 보유하고 있지 않거나, 이용자의 연락처가 변경 또는 오류 등으로 통지가 불가능한 신규 회원 가입시 서비스 이용약관 및 개인정보 처리방침 등에 제도의 주요 내용을 공지 등 통지의 오배송에 대한 고의 · 과실이 없음을 입증할 수 있어야 한다.

◇ 분리되어 저장·관리하는 휴면 이용자의 개인정보는 법령에 따른 보관 목적 또는 이용자의 요청에 대해서만 이용 및 제공하고 있는가?

→ 분리•보관 정보 재이용 방법

① 이용자 정보통신서비스의 재이용(계정 활성화)을 요구

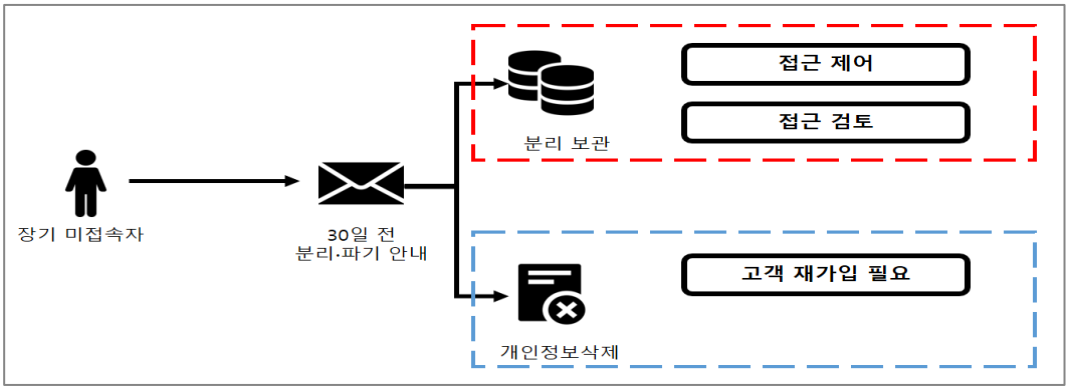
② 법률에 특별한 규정이 있는 경우에 예외가 인정되는 경우

◇ 분리되어 저장·관리하는 휴면 이용자의 개인정보는 법령에 따른 보관 목적 또는 이용자의 요청에 대해서만 이용 및 제공하고 있는가?

→ 분리되어 저장·관리하는 휴면 이용자의 개인정보에 대하여 접근권한

① 분리 데이터베이스의 접속 권한을 최소인원으로 제한하는 등 접근권한 최소화

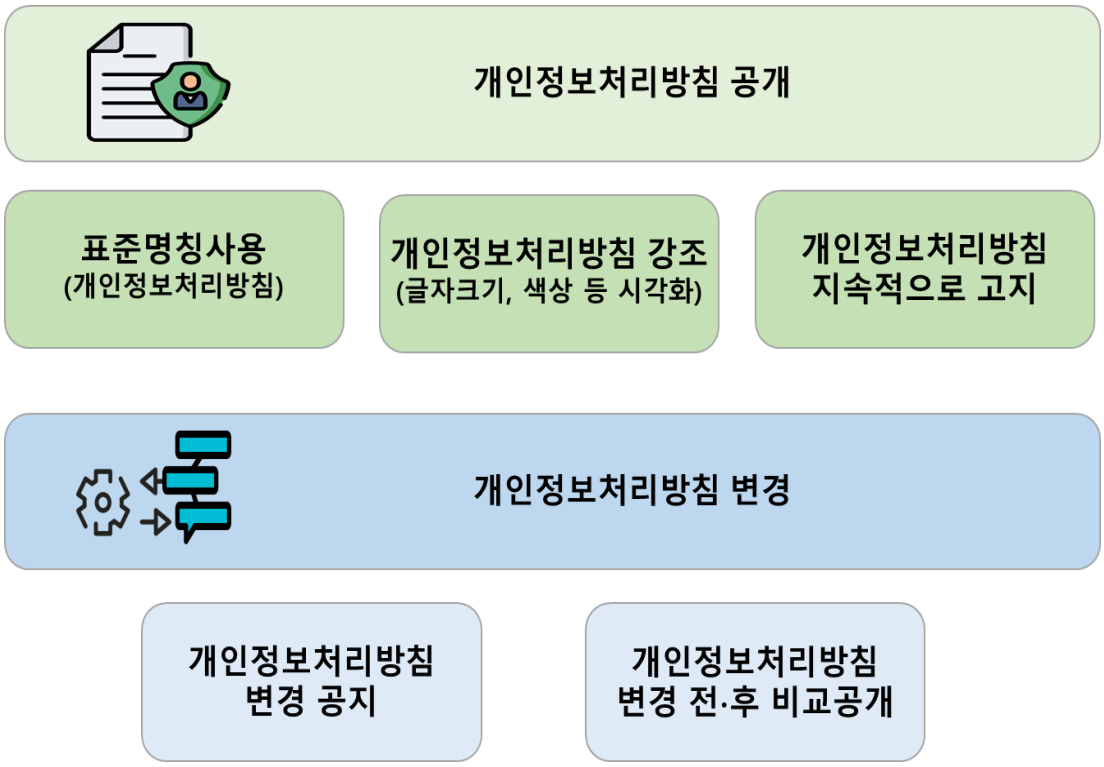
② 분리 데이터베이스에 대한 접속기록을 남기고 정기적으로 검토 등



※ 개인정보 분리보관시 보호조치(이해를 돕기 위한 예시)

3.5 정보주체 권리보호

3.5.1 개인정보처리방침 공개

<table>
<tr><th>세부분야</th><th>3.5.1 개인정보처리방침 공개</th></tr>
<tr><td>인증
기준</td><td>개인정보의 처리 목적 등 필요한 사항을 모두 포함하여 개인정보처리방침을 수립하고, 이를 정보주체(이용자)가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하고 지속적으로 현행화하여야 한다.</td></tr>
<tr><td>주요
확인사항</td><td>• 개인정보 처리방침을 정보주체(이용자)가 쉽게 확인할 수 있도록 인터넷 홈페이지 등에 지속적으로 현행화하여 공개하고 있는가?
• 개인정보 처리방침에는 법령에서 요구하는 내용을 모두 포함하고 있는가?
• 개인정보 처리방침이 변경되는 경우 사유 및 변경 내용을 지체 없이 공지하고 정보주체(이용자)가 언제든지 변경된 사항을 쉽게 알아볼 수 있도록 조치하고 있는가?</td></tr>
<tr><td>기준
요약도</td><td> 
</td></tr>
<tr><td>운영
방안</td><td>◇ 개인정보 처리방침을 정보주체(이용자)가 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 "개인정보 처리방침"이라는 표준화된 명칭을 사용</td></tr>
</table>

※ 출처: SK쉴더스 홈페이지(SK쉴더스)

◇ 개인정보 처리방침에는 법령에서 요구하는 내용을 모두 포함하고 있는가?

→ 개인정보 처리방침에 포함하여야 할 필수 사항

① 개인정보의 처리 목적

② 개인정보의 처리 및 보유 기간

③ 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다.)

④ 개인정보의 파기절차 및 파기방법(제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다.)

⑤ 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다.)

⑥ 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항

⑦ 제31조에 따른 개인정보 보호책임자의 이름 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처

⑧ 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당되는 경우에만 정한다.)

⑨ 처리하는 개인정보의 항목

⑩ 시행령 제30조 또는 제48조의2에 따른 개인정보의 안전성 확보 조치에 관한 사항

◇ 개인정보 처리방침이 변경되는 경우 사유 및 변경 내용을 지체 없이 공지하고 정보주체(이용자)가 언제든지 변경된 사항을 쉽게 알아볼 수 있도록 조치하고 있는가?

→ 개인정보 변경 내용공지

① 개인정보 처리방침이 변경되는 경우 사유 및 변경 내용 공지

※ 출처: SK쉴더스 홈페이지(SK쉴더스)

→ 개인정보 변경 사항 확인

① 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	정보주체(이용자)가 개인정보의 열람, 정정·삭제, 처리정지, 이의제기, 동의철회 요구를 수집 방법·절차보다 쉽게 할 수 있도록 권리행사 방법 및 절차를 수립·이행하고, 정보주체(이용자)의 요구를 받은 경우 지체 없이 처리하고 관련 기록을 남겨야 한다. 또한 정보주체(이용자)의 사생활 침해, 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 삭제 요청, 임시조치 등의 기준을 수립·이행하여야 한다
주요 확인사항	• 정보주체(이용자) 또는 그 대리인이 개인정보에 대한 열람, 정정·삭제, 처리정지, 이의제기, 동의 철회(이하 '열람 등'이라 함.) 요구를 개인정보 수집방법·절차보다 쉽게 할 수 있도록 권리 행사 방법 및 절차를 마련하고 있는가? • 정보주체(이용자) 또는 그 대리인이 개인정보 열람 요구를 하는 경우 규정된 기간 내에 열람 가능하도록 필요한 조치를 하고 있는가? • 정보주체(이용자) 또는 그 대리인이 개인정보 정정·삭제 요구를 하는 경우 규정된 기간 내에 정정·삭제 등 필요한 조치를 하고 있는가? • 정보주체(이용자) 또는 그 대리인이 개인정보 처리정지 요구를 하는 경우 규정된 기간 내에 처리정지 등 필요한 조치를 하고 있는가? • 정보주체(이용자)의 요구에 대한 조치에 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하여 안내하고 있는가? • 정보주체(이용자) 또는 그 대리인이 개인정보 수집·이용·제공 등의 동의를 철회하는 경우 지체 없이 수집된 개인정보를 파기하는 등 필요한 조치를 취하고 있는가? • 개인정보 열람 등의 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	

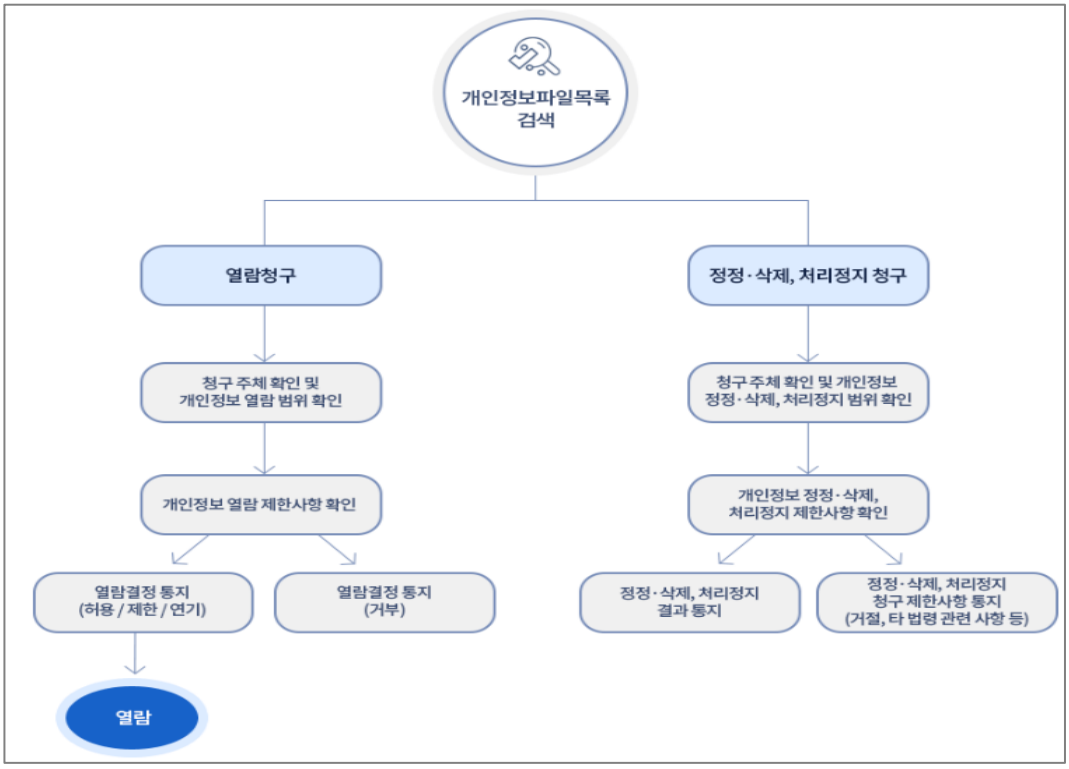
운영 방안	◇ 정보주체(이용자) 또는 그 대리인이 개인정보에 대한 열람, 정정·삭제, 처리정지, 이의제기, 동의 철회 요구를 개인정보 수집방법·절차보다 쉽게 할 수 있도록 권리 행사 방법 및 절차를 마련하고 있는가? → 열람, 정정, 삭제, 처리정지, 이의제기, 동의철회 등의 방법 공개 ① 정보주체에게 구체적인 방법과 절차를 공개 ② 다양한 권리 행사 방법을 마련하여 제공 ③ 열람 등을 요구한 자가 본인이거나 정당한 대리인인지 확인수단 적용 제6조(고객의 권리와 그 행사방법) ① 고객은 SK쉴더스가 처리하는 정보들에 대하여 자신 및 14세 미만 아동(법정대리인만 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(이용자) 또는 그 대리인이 개인정보 열람 요구를 하는 경우 규정된 기간 내에 열람 가능하도록 필요한 조치를 하고 있는가? → 권리 행사 방법 ① 개인정보 열람요구 ② 오류 등이 있을 경우 정정요구 ③ 삭제요구 ④ 처리정지요구 ◇ 정보주체(이용자) 또는 그 대리인이 개인정보 정정·삭제 요구를 하는 경우 규정된 기간 내에 정정·삭제 등 필요한 조치를 하고 있는가? → 열람 요구 · 정정 · 삭제 조치

① 10일 이내 개인정보 열람 요구 · 정정 · 삭제 알림

② 열람요구 연기 · 제한 · 거절 시 그 사유를 알리고 열람 거절

③ 불복 시 이의제기 절차 마련

④ 동의 철회 시 즉시 파기 · 위탁 · 제 3자 제공 자에게 조치요청

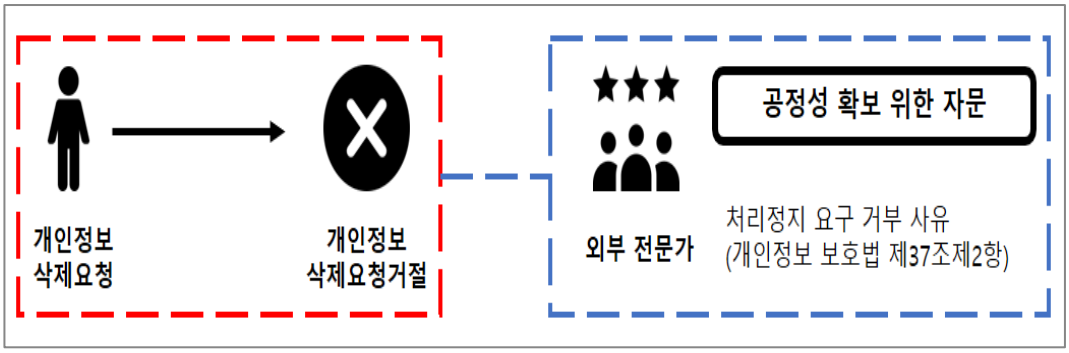


※ 출처: 개인정보보호 포털 공식홈페이지(민원마당 → 개인정보 열람등요구 안내)

◇ 정보주체(이용자)의 요구에 대한 조치에 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하여 안내하고 있는가?

→ 이의 제기에 대한 공적성 확보

① 공정하게 운영될 수 있도록 외부전문가를 참여시키거나 내부의 견제장치 마련 필요



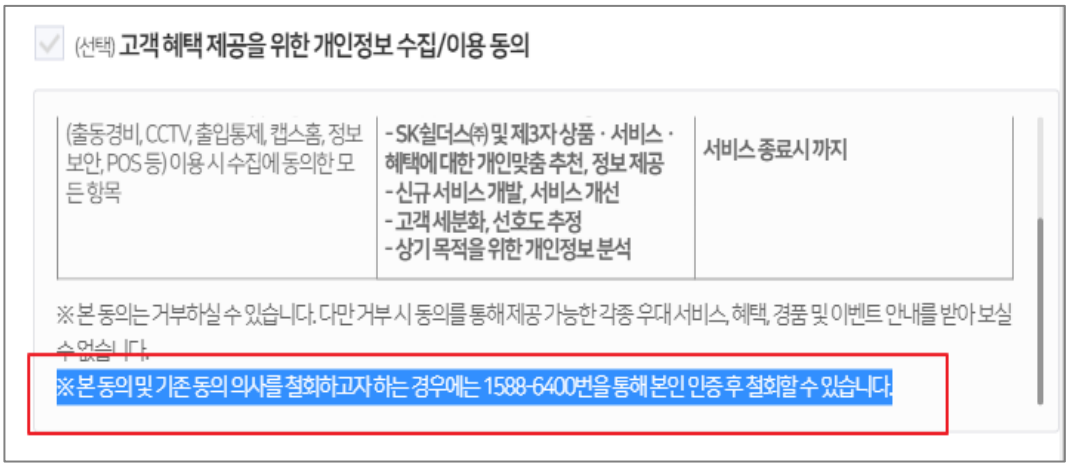
※ 정보주체 요청거절에 대한 정당성 확인(이해를 돕기 위한 예시)

◇ 정보주체(이용자) 또는 그 대리인이 개인정보 수집·이용·제공 등의 동의를 철회하는 경우 지체 없이 수집된 개인정보를 파기하는 등 필요한 조치를 취하고 있는가?

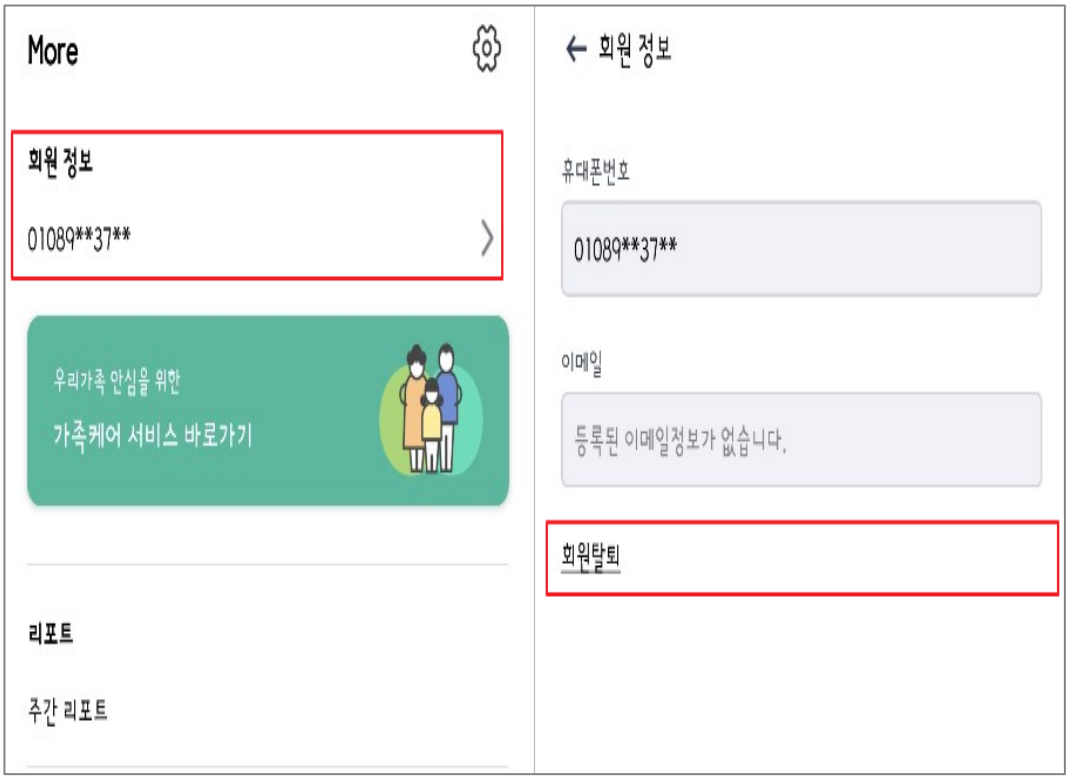
→ 동의 철회 시 조치

① 동의 철회 방법 제공

≫ 동의 철회 시 홍보 마케팅•제 3자 제공 등 개인정보가 활용되지 않도록 조치



※ 출처: SK쉴더스 홈페이지 캡스홈 도어 가이드 온라인가입 화면(SK쉴더스)



※ 출처: SK쉴더스 모바일가드 스마트폰 앱(SK쉴더스)

◇ 개인정보 열람 등의 요구 및 처리 결과에 대하여 기록을 남기고 있는가?

→ 개인정보 열람 조치 및 기록

① 열람이네 제공을 요구할 수 있는 정보

≫ 개인정보의 항목 및 내용

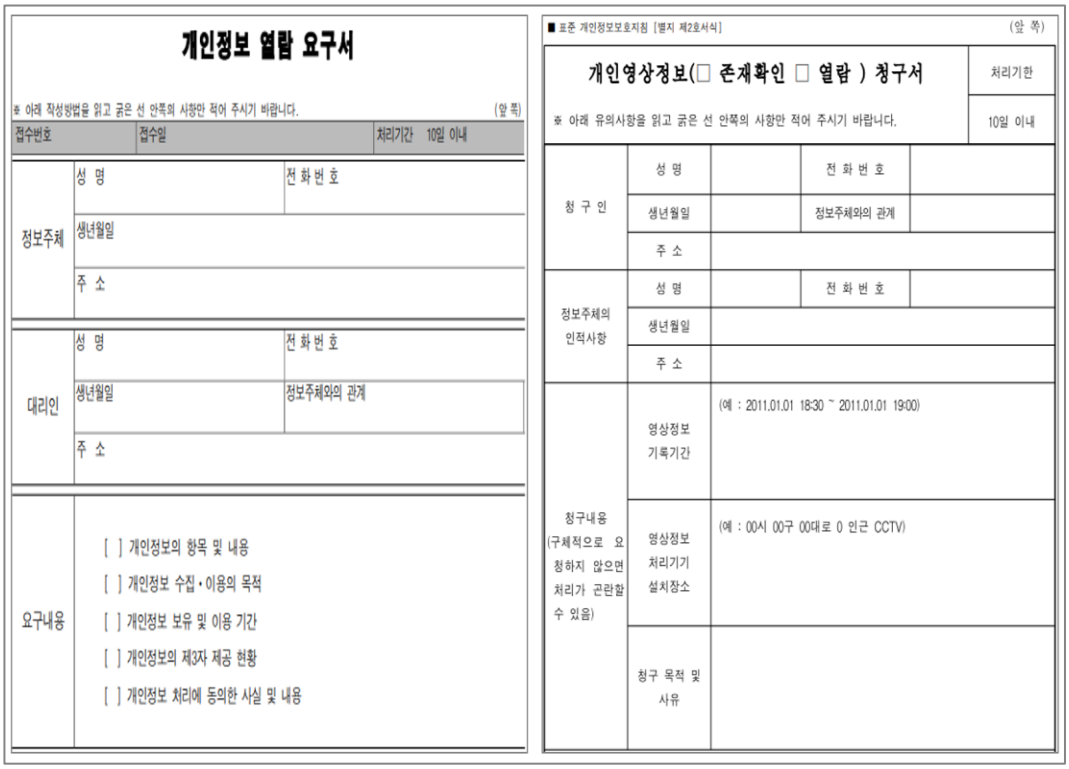
≫ 개인정보의 수집·이용의 목적

≫ 개인정보 보유 및 이용 기간

≫ 개인정보의 제3자 제공 현황

≫ 개인정보 처리에 동의한 사실 및 내용

② 개인정보 열람, 정정·삭제, 처리정지, 이의제기, 동의 철회 등의 요구 및 처리 결과에 대하여 기록



개인정보 열람 요구서

※ 아래 작성방법을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다. (앞쪽)

접수번호	접수일	처리기간 10일 이내
정보주체	성 명	전 화 번 호
	생년월일	
	주 소	
대리인	성 명	전 화 번 호
	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	

■ 표준 개인정보보호지침 [별지 제2호서식] (앞 쪽)

개인영상정보(□ 존재확인 □ 열람) 청구서

※ 아래 유의사항을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다.

처리기한
10일 이내

청 구 인	성 명		전 화 번 호	
	생년월일		정보주체와의 관계	
	주 소			
정보주체의 인적사항	성 명		전 화 번 호	
	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 CCTV)		
	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

「**정보통신망법**」 제44조 (정보통신망에서의 권리보호)

≫ 이용자는 사생활 침해 또는 명예훼손 등 타인의 권리를 침해하는 정보를

	정보통신망에 유통시켜서는 아니 된다. ≫ 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 처리한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 "삭제등"이라 한다)를 요청할 수 있다.

3.5.3 이용내역 통지

세부분야	3.5.3 이용내역 통지
인증 기준	개인정보의 이용내역 등 정보주체(이용자)에게 통지하여야 할 사항을 파악하여 그 내용을 주기적으로 통지하여야 한다.
주요 확인사항	• 법적 의무 대상자에 해당하는 경우 개인정보 이용내역을 주기적으로 정보주체에게 통지하고 그 기록을 남기고 있는가? • 개인정보 이용내역 통지 항목은 법적 요구항목을 모두 포함하고 있는가?
기준 요약도	
운영 방안	**◇ 법적 의무 대상자에 해당하는 경우 개인정보 이용내역을 주기적으로 정보주체(이용자)에게 통지하고 그 기록을 남기고 있는가?** **→ 통지 의무 적용대상** ① 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만 명 이상 ② 정보통신서비스 부문 전년도 매출액이 100억 원 이상 **→ 통지 주기 및 방법** ① 통지 주기: 연 1회 이상 ② 통지 방법: 전자우편·서면·모사전송·전화 또는 유사한 방법 중 어느 하나의 방법 ③ 통지 예외: 연락처 등 이용자에게 통지할 수 있는 개인정보를 수집하지 않은 경우

※ 휴면 이용자 정보는 통지 대상에서 제외

◇ 개인정보 이용내역 통지 항목은 법적 요구항목을 모두 포함하고 있는가?

→ 개인정보 이용내역 통지 항목

① 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목

개인정보 이용 내역 안내드립니다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제30조의 2(개인정보 이용내역의 통지)에 의거하여 **고객님**의 개인정보 이용 내역을 다음과 같이 안내 드립니다.

1. 개인정보 수집/이용목적 및 항목

구분	수집/이용목적	수집항목
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

※ 개인정보 이용 내역 안내(이해를 돕기 위한 예시)

정보보호 및 개인정보보호관리체계(ISMS-P) 운영 가이드

SK쉴더스(주) 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 취약점진단팀
제　작 : SK쉴더스 커뮤니케이션그룹