SK 쉴더스

안녕을 지키는 기술

개인정보보호 가이드

- 관리적 기술적 물리적 보호조치 기준

개인정보보호 가이드 발간사

안녕하십니까? SK쉴더스입니다.

최근 기업에서 보유하고 있는 고객의 개인정보 및 처리시스템의 안정성 확보조치가 소홀하여 고객의 소중한 개인정보가 유출되는 사건·사고가 빈번히 발생하고 있습니다.

SK쉴더스 취약점진단팀에서는 개인정보보호의 중요성과 개인정보 처리시스템의 안정성 확보조치를 위해 '개인정보보호 가이드(관리적·기술적·물리적 보호조치 기준)'를 발간하게 되었습니다.

본 가이드는 개인정보보호 관리체계, 개인정보처리시스템 관리적 보호조치, 개인정보 처리단계별 보호조치, 개인정보 기술적 보호조치, 영상정보 보호조치, 개인정보 물리적 보호조치 영역으로 분류되어 있으며, 각 영역별 보안정책 설정방법과 점검방법에 대한 설명을 담고 있습니다. 이를 통해 개인정보처리 시스템의 위협에 대응하고, ISMS-P 인증심사 및 컴플라이언스 기준을 충족할 수 있도록 구성하였습니다.

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

더불어, 개인정보보호 가이드 발간에 많은 시간과 노력을 투자한 팀원들에게 감사인사를 드립니다. 감사합니다.

취약점진단팀 팀장 김 상 춘

목 차

그 림 목 차

I. 개인정보 처리시스템 보안진단 항목

1. 개인정보보호 보안진단 체크리스트 항목

대분류	중분류	
개인정보보호 관리체계	1.1	개인정보보호조직
	1.2	개인정보보호계획
	1.3	개인정보 침해대응
	1.4	정보주체 권리보장
개인정보처리시스템 관리적 보호조치	2.1	개인정보 처리방침
	2.2	개인정보취급자 관리
	2.3	개인정보파일 관리
개인정보 처리단계별 보호조치	3.1	개인정보 수집
	3.2	개인정보 보유
	3.3	개인정보 이용 • 제공
	3.4	개인정보 위탁
	3.5	개인정보 파기
개인정보 기술적 보호조치	4.1	개인정보처리시스템 접근관리
	4.2	접 개인정보처리시스템 접근통제
	4.3	개인정보의 암호화
	4.4	접속기록 및 접근권한 기록 보관 및 점검
	4.5	개인정보처리시스템 운영보안
	4.6	Mobile 기기의 소프트웨어관리
	4.7	개인정보취급자 단말보안
	4.8	개발 환경 통제
영상정보보호 조치	5.1	영상정보처리기기 관리적 보호조치

	5.2	영상정보처리기기 기술적 보호조치
개인정보 물리적 보호조치	**6.1**	물리적 통제

II. 세부항목 설정

1. 개인정보보호 관리체계

1.1. 개인정보보호조직

1.1.1 최고경영자는 개인정보보호 업무를 총괄할 최고책임자를 공식 지정하고 있습니까?			
항목구분			
대구분	개인정보보호 관리체계	**항목코드**	1.1.1
중구분	개인정보보호조직	**중요도**	**H**
항목 개요	개인정보보호 업무를 총괄할 책임자를 공식적으로 지정하고 있는지 확인해야 함.		
평가기준			
판단 기준	Y - 개인정보 보호책임자가 인사발령 등을 통해 공식적으로 지정되어 있음. P - 개인정보 보호책임자가 업무 총괄하여 책임질 수 있는 법적 요건 충족하지 않음. N - 개인정보 보호책임자가 지정되어 있지 않음.		
점검 방법	▶ 개인정보 보호책임자가 법적 지정 기준에 따라 공식 지정되어 있는 확인. ① 최고경영자가 인사발령 등의 절차를 통해 공식적으로 지정한 내역 ② 개인정보보호 책임자는 예산, 인력 등 자원을 할당할 수 있는 임원급으로 지정하고 관련 법령에 따라 자격요건을 충족하는지 확인. - 개인정보보호 책임자 임명관련 자료(인사명령, 인사카드 등) - 개인정보보호 조직도 - 개인정보보호 정책 및 지침 - 직무기술서(개인정보 보호책임자의 역할 및 책임에 관한 사항) - 내부관리계획(개인정보보호 책임자 지정에 관한 사항) - 개인정보보호 책임자 지정요건(기업)		

개인정보 보호법	정보통신망법
사업주 또는 대표자 임원(임원이 없는 경우에는 개인정보 처리업무를 담당하는 부서의 장)	임원 개인정보보호와 관련하여 이용자의 고충처리를 담당하는 부서의 장 ※ 단, 상시 종업원 수가 5명 미만인 정보통신서비스 제공자등은 개인정보 보호책임자를 지정하지 아니할 수 있으며, 이때는 업주 또는 대표자가 개인정보 보호책임자가 됨

※ 출처: ISMS-P 인증제도안내서

<그림 1> 개인정보보호 책임자 지정요건(기업)

- 개인정보보호 책임자 지정요건(공공)

★ 개인정보 보호법 시행령 제32조(개인정보 보호책임자의 업무 및 지정요건 등) 제2항 제1호

가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관: 고위공무원단에 속하는 공무원(이하 "고위공무원"이라 한다) 또는 그에 상당하는 공무원

나. 가목 외에 정무직공무원을 장(長)으로 하는 국가기관: 3급 이상 공무원(고위공무원을 포함한다) 또는 그에 상당하는 공무원

다. 가목 및 나목 외에 고위공무원, 3급 공무원 또는 그에 상당하는 공무원 이상의 공무원을 장으로 하는 국가기관: 4급 이상 공무원 또는 그에 상당하는 공무원

라. 가목부터 다목까지의 규정에 따른 국가기관 외의 국가기관(소속 기관을 포함한다): 해당 기관의 개인정보 처리 관련 업무를 담당하는 부서의 장

마. 시·도 및 시·도 교육청: 3급 이상 공무원 또는 그에 상당하는 공무원

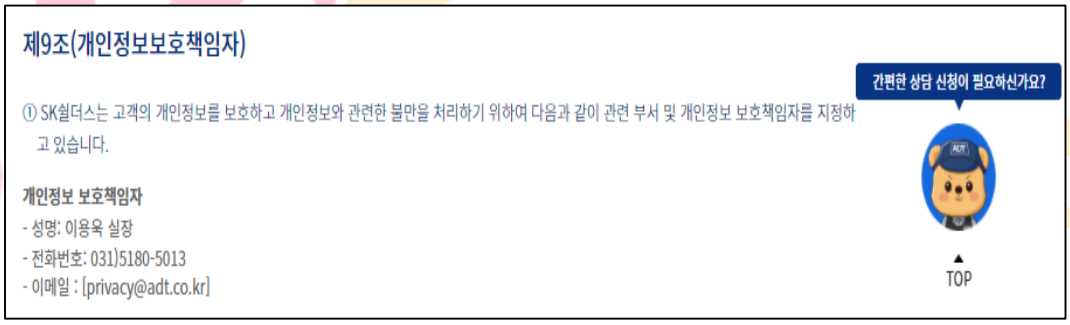
바. 시·군 및 자치구: 4급 공무원 또는 그에 상당하는 공무원

사. 제2조제5호에 따른 각급 학교: 해당 학교의 행정사무를 총괄하는 사람

아. 가목부터 사목까지의 규정에 따른 기관 외의 공공기관: 개인정보 처리 관련 업무를 담당하는 부서의 장. 다만, 개인정보 처리 관련 업무를 담당하는 부서의 장이 2명 이상인 경우에는 해당 공공기관의 장이 지명하는 부서의 장이 된다.

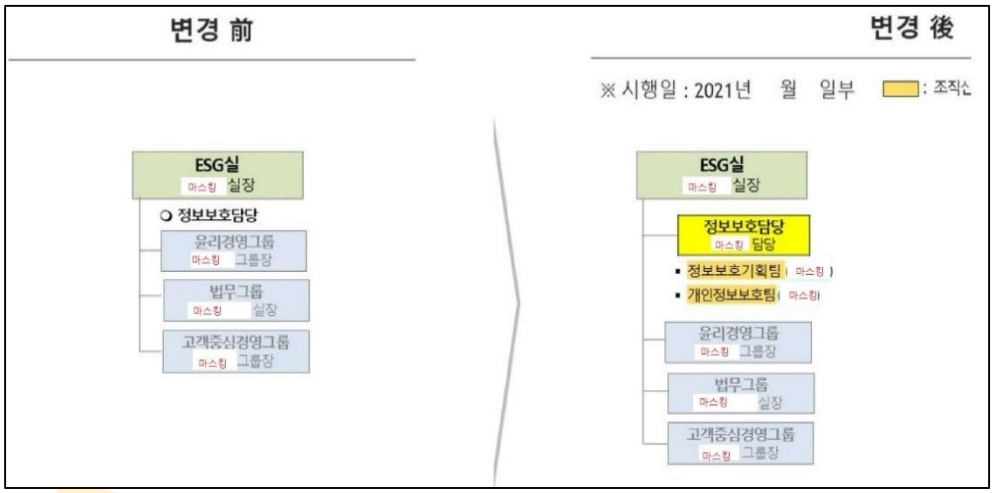
※ 출처: ISMS-P 인증제도안내서

<그림 2> 개인정보보호 책임자 지정요건(공공)

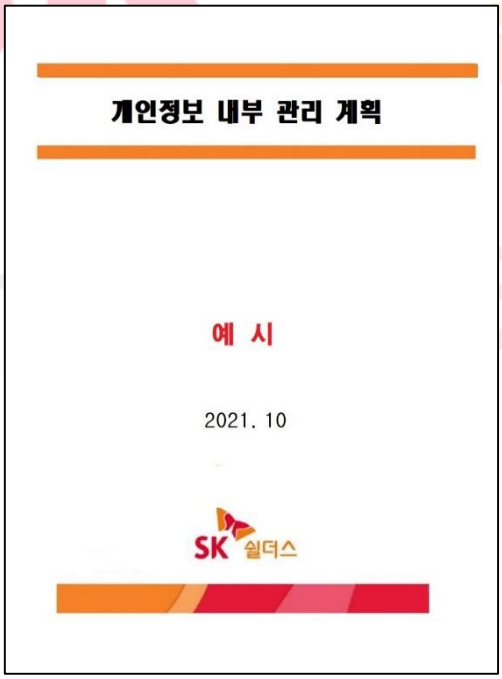


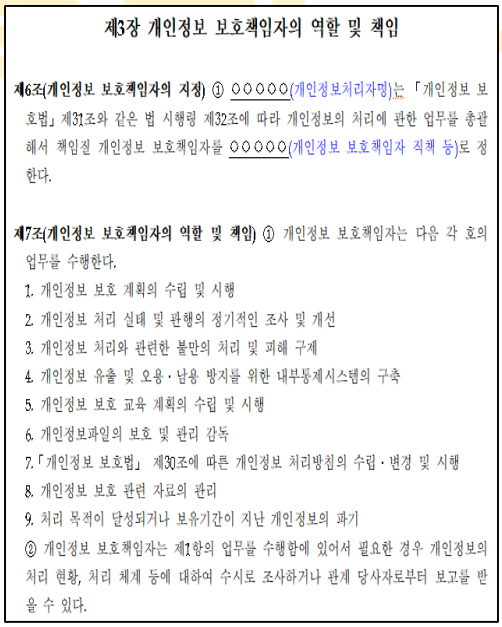
<그림 3> 개인정보보호 책임자 공개

<그림 4> 개인정보보호 책임자 인사발령 문서

	 **<그림 5> 개인정보보호 책임자 업무분장 및 조직도**
관련 근거	※ 개인정보보호법 <제29조> 안전조치 의무 ※ 개인정보보호법 <제31조> 개인정보 보호책임자의 지정 ※ 정보통신망법 <제27조> 개인정보 보호책임자의 지정 ※ 정보통신망법 <제45조의 3> 정보보호 최고책임자의 지정
과징금 및 벌칙	※ 개인정보보호법 <제29조의 제1항> 위반하여 개인정보 보호책임자를 지정하지 않은 경우 1천만원 이하의 과태료

1.1.2 개인정보 보호책임자에 법률이 정하는 책임 및 역할이 부여되어 있으며, 관련 업무를 수행하고 있습니까?			
항목구분			
대구분	개인정보보호 관리체계	**항목코드**	1.1.2
중구분	개인정보보호조직	**중요도**	**H**
항목 개요	개인정보 보호책임자 책임과 역할을 공식적으로 부여되어야 함.		
평가기준			
판단 기준	Y - 개인정보 보호책임자에게 법률 등에서 정하는 책임 및 역할이 공식적으로 부여되어 있음. P - 개인정보보호 보호책임자가 법률에서 요구하는 요건 일부 누락. N - 개인정보보호 보호책임자 법률에서 요구하는 요건을 부여하지 않거나 업무 하지 않음.		
점검 방법	▶ 개인정보 보호책임자의 업무가 문서로 정의되어 있는지 확인 ① 개인정보 보호책임자의 책임 및 역할이 내부관리계획, 개인정보보호지침 등의 문서로 정의되어 승인되었는지 확인		





제3장 개인정보 보호책임자의 역할 및 책임

제6조(개인정보 보호책임자의 지정) ① ○○○○○(개인정보처리자명)는 「개인정보 보호법」 제31조와 같은 법 시행령 제32조에 따라 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 ○○○○○(개인정보 보호책임자 직책 등)로 정한다.

제7조(개인정보 보호책임자의 역할 및 책임) ① 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리 감독
7. 「개인정보 보호법」 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
8. 개인정보 보호 관련 자료의 관리
9. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

② 개인정보 보호책임자는 제1항의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.

※ 출처: 한국인터넷진흥원 개인정보 교육 관련 별첨 자료

<그림 6> 개인정보보호지침의 책임자 역할

② 개인정보 보호책임자의 역할에 누락이 없는지 확인하고 실제 역할을 수행하는지에

<table>
<tr><td></td><td>대해 확인

제31조(개인정보 보호책임자의 지정)
① 개인정보처리자는 개인정보의 처리
에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다.

② 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.
1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독

<표1> 개인정보보호법 제31조(개인정보 보호책임자의 지정)</td></tr>
<tr><td>관련
근거</td><td>※ 개인정보보호법 <제31조> 개인정보 보호책임자의 지정
※ 개인정보보호법 시행령 <제32조> 개인정보 보호책임자의 업무 및 지정요건 등</td></tr>
<tr><td>과징금
및
벌칙</td><td>※ 개인정보보호법 <제29조의제1항> 위반하여 개인정보 보호책임자를 지정하지 않은 경우 1천만원 이하의 과태료</td></tr>
</table>

1.2. 개인정보보호 계획

1.2.1 개인정보의 안전한 처리를 위한 내부관리 계획을 수립 시행하고 있습니까?			
항목구분			
대구분	개인정보보호 관리체계	**항목코드**	1.2.1
중구분	개인정보보호계획	**중요도**	**H**
항목 개요	내부관리계획을 수립하고 내부 의사결정 절차를 통해 공식 시행하여야 함.		
평가기준			
판단 기준	Y - 내부관리계획을 수립하고 내부 의사결정 절차를 통해 공식적으로 수립 시행하고 있음. P - 내부관리계획 공식적으로 수립 시행하였으나, 일부 누락이 있음. N - 내부관리계획이 없음.		
점검 방법	▶ 내부관리계획을 수립하고 내의 의사 결정절차를 통해 공식적으로 시행하는지 확인. ① 개인정보보호법의 경우 <개인정보 안전성 확보조치 기준>에 명시된 모든 내용이 포함되어야 함. (공공) 제4조(내부 관리계획의 수립·시행) 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다. 1. 개인정보 보호책임자의 지정에 관한 사항 2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항 3. 개인정보취급자에 대한 교육에 관한 사항 4. 접근 권한의 관리에 관한 사항 5. 접근 통제에 관한 사항 6. 개인정보의 암호화 조치에 관한 사항 7. 접속기록 보관 및 점검에 관한 사항 8. 악성프로그램 등 방지에 관한 사항 9. 물리적 안전조치에 관한 사항 10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항 11. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항 12. 위험도 분석 및 대응방안 마련에 관한 사항 13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항		

14. 개인정보 처리업무를 위탁의 경우 수탁자에 대한 관리 및 감독관한 사항
15. 그 밖에 개인정보 보호를 위하여 필요한 사항

<표2> 개인정보의 안전성 확보조치 기준 제4조(내부 관리계획의 수립·시행)

② 정보통신망법의 <개인정보 기술적 관리적 보호조치 기준> 에 명시된 모든 내용이 포함되어야 함. (기업)

제3조(내부관리계획의 수립·시행)

① 정보통신서비스 제공자 등은 다음 각 호의 사항을 정하여 개인정보보호 조직을 구성·운영하여야 한다.

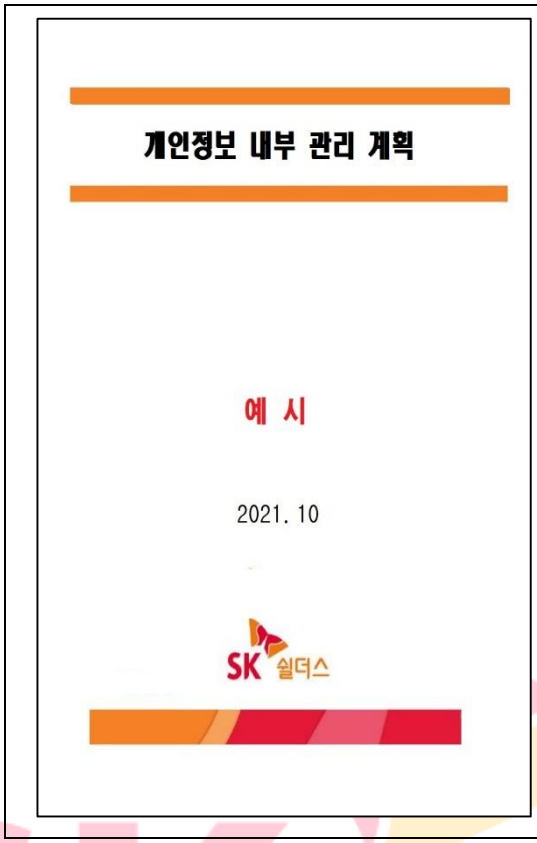
1. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
2. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보 내부관리계획의 수립 및 승인에 관한 사항
4. 개인정보의 기술적·관리적 보호조치 이행 여부의 내부 점검에 관한 사항
5. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독의 사항
6. 개인정보의 분실·도난·유출·위조·변조·훼손 등이 발생한 경우의 대응절차 및 방법에 관한 사항
7. 그 밖에 개인정보보호를 위해 필요한 사항

② 정보통신서비스 제공자 등은 다음 각 호의 사항을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수 등을 고려하여 필요한 교육을 정기적으로 실시하여야 한다.

1. 교육목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

③ 정보통신서비스 제공자 등은 제1항 및 제2항에 대한 세부 계획, 제4조부터 제8조까지의 보호조치 이행을 위한 세부적인 추진방안을 포함한 내부관리계획을 수립·시행하여야 한다.

<표3> 개인정보의 기술적·관리적 보호조치 기준 제3조(내부 관리계획의 수립·시행)



목 차

※ 출처: 한국인터넷진흥원 개인정보 교육 관련 별첨 자료

<그림 7> 개인정보보호 내부관리계획 예시

관련 근거	※ 개인정보보호법 <제29조> 안전조치 의무 ※ 개인정보안전성 확보조치기준 <제4조> 내부관리계획의 수립 시행 ※ 개인정보의 기술적 관리적 보호조치 <제3조> 내부관리계획의 수립 시행
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보조치 의무를 위반한 경우 3천만원 이하 과태료

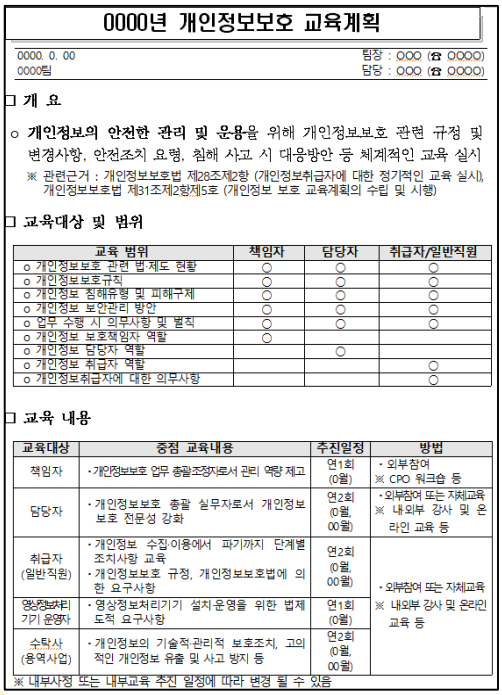
1.2.2 개인정보보호 교육, 실태 점검 등 개인정보 보호 활동에 대한 연간 수행계획을 수립 시행하고 있습니까?			
항목구분			
대구분	개인정보보호 관리체계	**항목코드**	1.2.2
중구분	개인정보보호계획	**중요도**	**H**
항목 개요	개인정보보호 연간 계획이 수립되어, 내부 승인절차에 따라 시행되어야 함.		
평가기준			
판단 기준	Y - 개인정보보호 연간 계획에 필요사항을 누락없이 수립하고 내부승인에 따라 시행되어야 함. P - 개인정보보호 연간계획을 수립 시행하였으나, 일부 누락이 있음. N - 개인정보보호 연간계획이 없음.		
점검 방법	▶ 개인정보보호 연간 계획을 수립하고 내부 승인 절차에 따라 시행되고 있는지 확인. ▶ 개인정보보호 연간 계획에 아래 상세 내용이 포함되어 있는지 확인. 1. 개인정보보호 조직, 인력 2. 개인정보보호 활동 계획 및 이에 따른 예산 3. 개인정보 실태 점검 계획(수탁자 포함) 4. 개인정보보호 교육 계획(책임자, 담당자, 취급자/일반직원 대상) 등 * 실질적인 실행이 가능하도록 일정, 담당자, 예산 등 구체적인 방안이 필요 ※ 출처: 개인정보의 안전성 확보조치 기준 해설서 **<그림 8> 개인정보보호 연간 계획 내 필수 포함 사항** ▶ 개인정보 연간 계획에 따라 개인정보보호 활동이 이행되고 있는지 여부를 정기적으로 검토하여 개인정보 보호책임자 보고내용 확인.		

개인정보보호 연간 운영 계획서

예 시

2021. 10

SK 실더스



0000년 개인정보보호 교육계획

0000. 0. 00 팀장 : OOO (☎ OOOO)
0000팀 담당 : OOO (☎ OOOO)

□ 개 요

○ 개인정보의 안전한 관리 및 운용을 위해 개인정보보호 관련 규정 및 변경사항, 안전조치 요령, 침해 사고 시 대응방안 등 체계적인 교육 실시

※ 관련근거 : 개인정보보호법 제28조제2항 (개인정보취급자에 대한 정기적인 교육 실시), 개인정보보호법 제31조제2항제5호 (개인정보 보호 교육계획의 수립 및 시행)

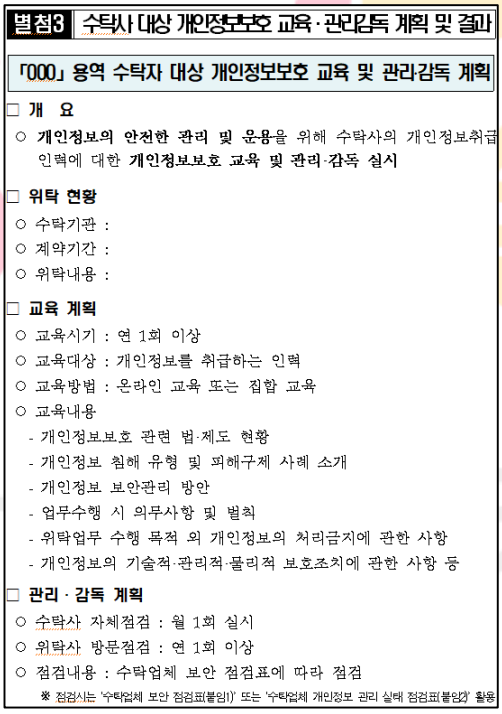
□ 교육대상 및 범위

교육 범위	책임자	담당자	취급자/일반직원
○ 개인정보보호 관련 법·제도 현황	○	○	○
○ 개인정보보호규칙	○	○	○
○ 개인정보 침해유형 및 피해구제	○	○	○
○ 개인정보 보안관리 방안	○	○	○
○ 업무 수행 시 의무사항 및 벌칙	○	○	○
○ 개인정보 보호책임자 역할	○		
○ 개인정보 담당자 역할		○	
○ 개인정보 취급자 역할			○
○ 개인정보취급자에 대한 의무사항			○

□ 교육 내용

교육대상	중점 교육내용	주진일정	방법
책임자	·개인정보보호 업무 총괄조정자로서 관리 역량 제고	연1회 (0월)	·외부참여 ※ CPO 워크숍 등
담당자	·개인정보보호 총괄 실무자로서 개인정보 보호 전문성 강화	연2회 (0월, 00월)	·외부참여 또는 자체교육 ※ 내외부 강사 및 온라인 교육 등
취급자 (일반직원)	·개인정보 수집·이용에서 파기까지 단계별 조치사항 교육 ·개인정보보호 규정, 개인정보보호법에 의한 요구사항	연2회 (0월, 00월)	·외부참여 또는 자체교육 ※ 내외부 강사 및 온라인 교육 등
영상정보처리기기 운영자	·영상정보처리기기 설치·운영을 위한 법제도적 요구사항	연1회 (0월)	
수탁사 (용역사업)	·개인정보의 기술적·관리적 보호조치, 고의적인 개인정보 유출 및 사고 방지 등	연2회 (0월, 00월)	

※ 내부사정 또는 내부교육 추진 일정에 따라 변경 될 수 있음



별첨3 수탁사 대상 개인정보보호 교육·관리감독 계획 및 결과

「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 :

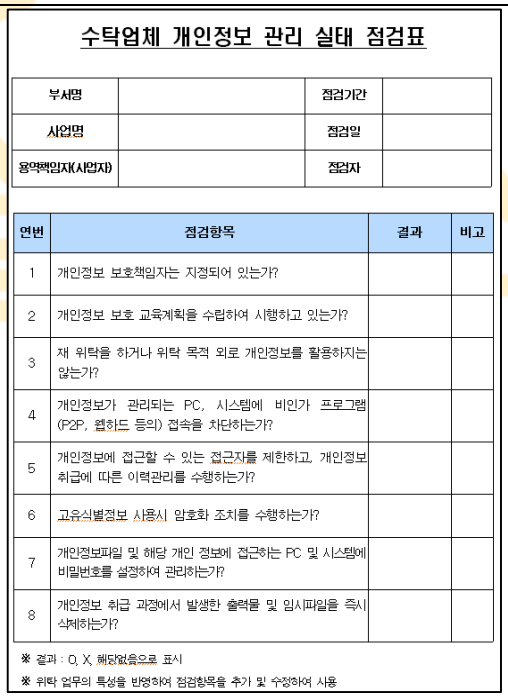
□ 교육 계획

○ 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: 한국인터넷진흥원 개인정보 교육 관련 별첨 자료

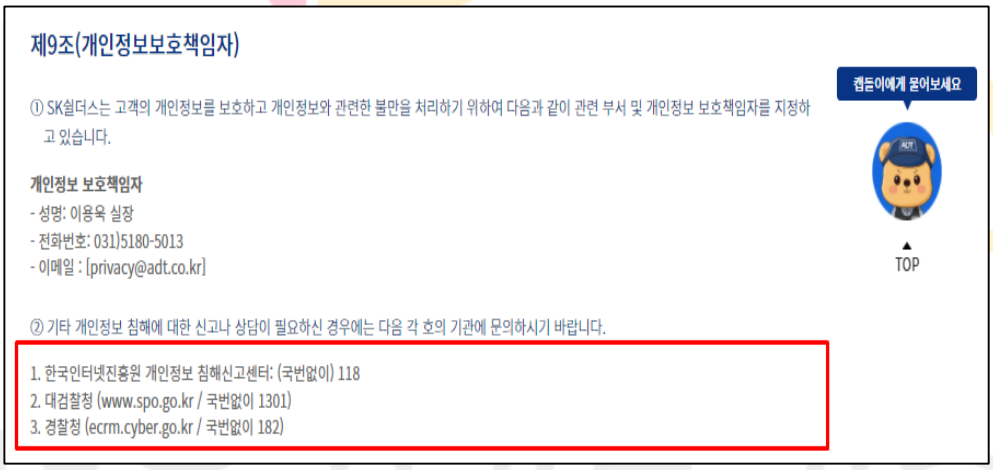
<그림 9> 개인정보보호 교육 계획 및 예산

관련 근거	※ 개인정보보호법 <제29조> 안전조치 의무 ※ 개인정보안전성 확보조치기준 <제4조> 내부관리계획의 수립 시행 ※ 개인정보의 기술적 관리적 보호조치 <제3조> 내부관리계획의 수립 시행
과징금	※ 개인정보보호법 <제29조> 안전성 확보조치 의무를 위반한 경우 3천만원 이하 과태료

및 벌칙	

1.3. 개인정보 침해대응

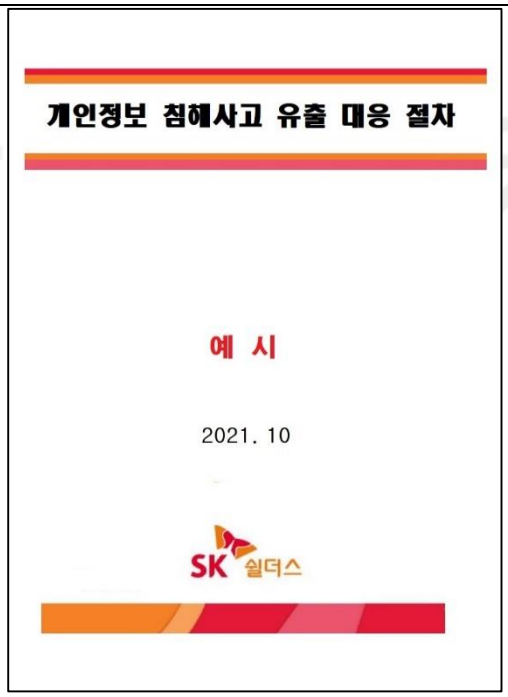
1.3.1 개인정보 침해사실을 신고할 수 있는 방법을 정보주체에게 안내하고 있습니까?			
항목구분			
대구분	개인정보보호 관리체계	**항목코드**	1.3.1
중구분	개인정보 침해대응	**중요도**	H
항목 개요	개인정보 침해사고 절차를 수립하고 침해신고 방법을 홈페이지에 안내해야 함.		
평가기준			
판단 기준	Y - 개인정보 침해신고 절차를 수립하고, 신고방법을 홈페이지에 고지하고 있음. N - 개인정보 침해신고 절차 및 고지 내용이 없음.		
점검 방법	▶ 개인정보 침해(권리 침해, 개인정보 유출 등)에 대해 신고할 수 있는 방법을 정보주체가 쉽게 확인할 수 있도록 안내하고 있는지 확인.		
관련 근거	※ 개인정보보호법 <제30조> 개인정보 처리방침의 수립 및 공개 ※ 개인정보보호법 <제34조> 개인정보 유출통지 등 ※ 개인정보보호법 <제62조> 침해사실의 신고 등		
과징금 및 벌칙	※ 개인정보보호법 <제34조의제1항, 3항> 위반하여 조치 결과를 신고하지 않은 경우 5천만원 이하의 과태료		

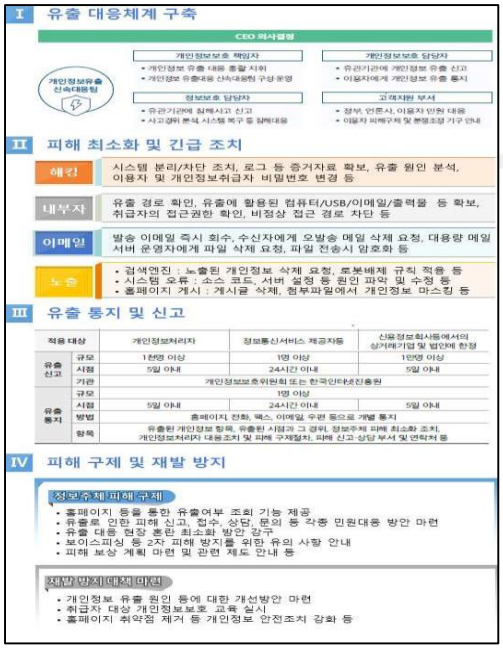


<그림 10> 개인정보처리방침에 침해사고 및 불만 처리 방법 안내 예시

1.3.2 개인정보 유출 신고 통지 절차, 긴급 연락체계, 사고 대응 조직 구성 등을 포함한 개인정보

침해사고 대응절차를 수립하여 실시하고 있습니까?			
항목구분			
대구분	개인정보보호 관리체계	**항목코드**	1.3.2
중구분	개인정보 침해대응	**중요도**	**H**
항목 개요	개인정보 침해사고 절차를 수립하고 침해신고 방법을 홈페이지에 안내해야 함.		
평가기준			
판단 기준	Y - 개인정보 침해신고 절차를 수립하고, 신고방법을 홈페이지에 고지하고 있음. N - 개인정보 침해신고 절차 및 고지 내용이 없음.		
점검 방법	▶ 공식적인 개인정보 침해사고(권리침해, 개인정보 유출 등)에 대한 대응절차가 마련되어 시행되는지 확인 ▶ 개인정보 침해사고 대응 절차에 필수 사항이 포함되어 있는지 확인. - 개인정보 유출 시 신고 및 통지절차 - 비상연락망 등 긴급 연락체계 - 사고 대응조직 구성 및 업무분장 - 침해사고 유형별 조치 방법 및 절차 - 정보주체 피해구제 방법 ▶ 개인정보 침해사고 대응절차를 이해관계자들이 인지할 수 있도록 공유하는지 확인.		





※ 출처: 개인정보보호위원회 개인정보 유출 대응 매뉴얼

	<그림 11> 침해사고 대응 매뉴얼 예시
관련 근거	※ 개인정보보호법 <제30조> 개인정보 처리방침의 수립 및 공개 ※ 개인정보보호법 <제34조> 개인정보 유출통지 등 ※ 개인정보보호법 <제62조> 침해사실의 신고 등
과징금 및 벌칙	※ 개인정보보호법 <제34조의제1항,3항> 위반하여 조치 결과를 신고하지 않은 경우 5천만원 이하의 과태료

1.4. 정보주체 권리보장

1.4.1 개인정보 열람, 정정, 삭제 및 처리정지, 수집 출처 고지 등 정보주체의 요구에 대한 처리절차를 수립하여 안내하고 있습니까?			
항목구분			
대구분	개인정보보호 관리체계	**항목코드**	1.4.1
중구분	정보주체 권리보장	**중요도**	**H**
항목 개요	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 있는지 확인		
평가기준			
판단 기준	Y - 정보주체의 개인정보 요구에 대한 절차를 수립하고 안내하고 있음 N - 정보주체의 개인정보 요구에 대한 절차가 없음.		
점검 방법	▶ 정보주체의 개인정보 열람, 정정 삭제, 처리정지, 수집 출처 요구에 대하여 대응할 수 있는 처리 절차가 공식적으로 수행되고 있는지 확인. ▶ 정보주체 요구 처리절차에 상세 내역이 모두 포함되어 있는지 확인. - 정보주체 요구 유형(열람, 정정, 삭제, 처리정지, 수집 출처 요구)에 따른 대응 절차 - 정보주체 요구 접수 부서 및 담당자 - 정보주체 요구 관리대장 양식 - 정보주체 또는 법정대리인 본인 여부 확인할 수 있는 절차 - 정보주체 요구 거절 기준 및 이에 따른 절차 등 ▶ 정보주체 요구 시 조치 내역을 확인하여, 열람이나 제공을 요구하는 정보가 상세내역에 포함되어 있는지 확인한다.		

개인정보 보호법	정보통신망법
1. 개인정보의 항목 및 내용 2. 개인정보의 수집·이용의 목적 3. 개인정보 보유 및 이용 기간 4. 개인정보의 제3자 제공 현황 5. 개인정보 처리에 동의한 사실 및 내용	1. 정보통신서비스 제공자등이 가지고 있는 이용자의 개인정보 2. 정보통신서비스 제공자등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황 3. 정보통신서비스 제공자등에게 개인정보 수집·이용·제공 등의 동의를 한 현황

※ 출처: ISMS-P 인증제도안내서

<그림 12> 정보주체 권리보장 제공내역

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

AS 접수가 필요하신가요?

TOP

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

제7조(아동의 개인정보보호 및 법정대리인의 권리)

① SK쉴더스는 만14세 미만 아동(이하 '아동')의 개인정보 수집/이용/제공 등을 하는 경우 해당 아동의 법정대리인의 동의를 얻도록 하고 있습니다.
② SK쉴더스는 아동의 서비스 이용신청시 법정대리인의 동의를 얻기 위하여 법정대리인의 성명, 연락처등 필요한 최소한의 정보를 요구할 수 있습니다. 이 경우 개인정보의 수집•이용 또는 제공 목적 및 법정대리인의 동의가 필요하다는 취지를 아동이 쉽게 이해할 수 있는 평이한 표현으로 아동에게 고지합니다.
③ SK쉴더스는 법정대리인의 동의를 얻기 위하여 수집한 법정대리인의 개인정보를 해당 법정대리인의 동의 여부를 확인하는 목적 외의 용도로 이를 이용하거나 제3자에게 제공하지 않습니다.
④ 아동의 법정대리인은 아동에 관해 SK쉴더스가 보유하고 있는 개인정보 수집•이용•제공 동의를 철회할 수 있고, SK쉴더스가개인정보를이용하거나 제3자에게 제공한현황, 개인정보의수집•이용•제공등의동의현황을 열람하거나 제공받을 수 있으며, 오류가있는경우에는그정정을요구할수있습니다.

<그림 13> 정보주체 권리보장 절차 방법 안내

■ 개인정보 보호법 시행규칙 [별지 제8호서식]

개인정보([ ] 열람 [ ] 정정·삭제 [ ] 처리정지) 요구서

※ 아래 작성방법을 읽고 굵은 선 안쪽의 사항만 적어 주시기 바랍니다. (앞 쪽)

접수번호	접수일	처리기간 10일 이내
	성 명	전 화 번 호
	생년월일	
	주 소	
대리인	성 명	전 화 번 호
	생년월일	정보주체와의 관계
	주 소	
요구내용	[ ] 열람	[ ] 개인정보의 항목 및 내용 [ ] 개인정보 수집·이용의 목적 [ ] 개인정보 보유 및 이용 기간 [ ] 개인정보의 제3자 제공 현황 [ ] 개인정보 처리에 동의한 사실 및 내용
	[ ] 정정·삭제	※ 정정·삭제하려는 개인정보의 항목과 그 사유를 적습니다.
	[ ] 처리정지	※ 개인정보의 처리정지를 원하는 대상·내용 및 그 사유를 적습니다.

「개인정보 보호법」 제35조제1항·제2항, 제36조제1항 또는 제37조제1항과 같은 법 시행령 제41조제1항, 제43조제1항 또는 제44조제1항에 따라 위와 같이 요구합니다.

년 월 일

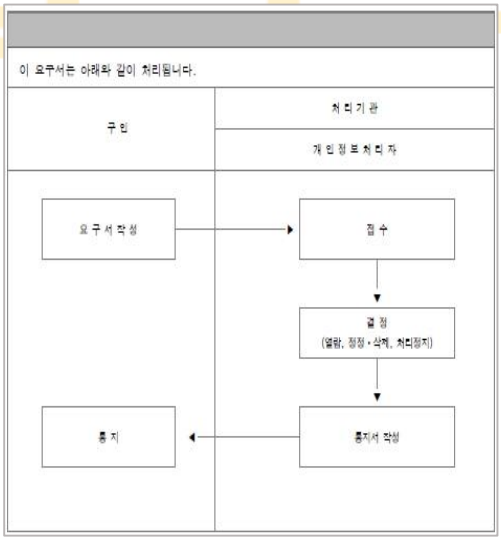
요구인 (서명 또는 인)

귀하

작 성 방 법

1. '대리인' 란은 대리인이 요구인일 때에만 적습니다.
2. 개인정보의 열람을 요구하려는 경우에는 '열람' 란에 [√] 표시를 하고 열람하려는 사항을 선택하여 [√] 표시를 합니다. 표시를 하지 않은 경우에는 해당 항목의 열람을 요구하지 않은 것으로 처리됩니다.
3. 개인정보의 정정·삭제를 요구하려는 경우에는 '정정·삭제' 란에 [√] 표시를 하고 정정하거나 삭제하려는 개인정보의 항목과 그 사유를 적습니다.
4. 개인정보의 처리정지를 요구하려는 경우에는 '처리정지' 란에 [√] 표시를 하고 처리정지 요구의 대상·내용 및 그 사유를 적습니다.

210mm×297mm[일반용지 70g/㎡(재활용품)]



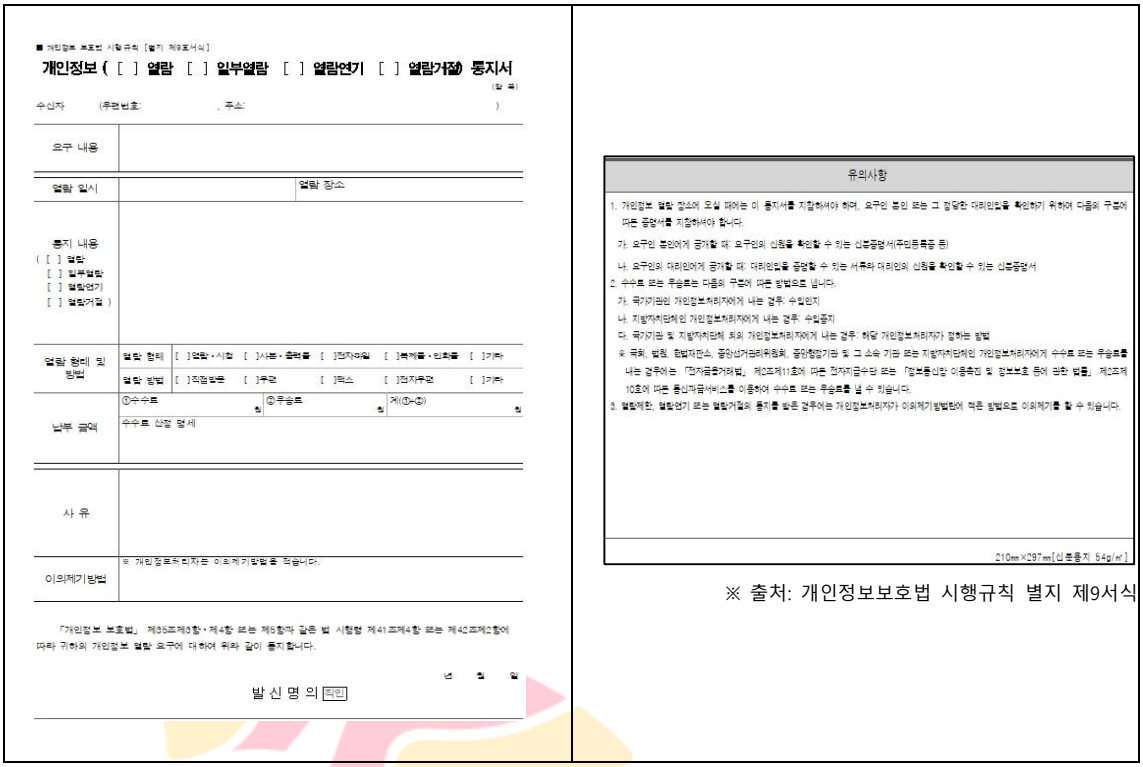
※ 출처: 개인정보보호법 시행규칙 별지 제8호서식

<그림 14> 개인정보 열람 정정 삭제 처리정지 요구서

관련	※ 개인정보보호법 <제4조> 정보주체의 권리 보장

근거	※ 개인정보보호법 <제20조> 정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지 ※ 개인정보보호법 <제35조> 개인정보의 열람
과징금 및 벌칙	※ 개인정보보호법 <제20조의 제1항> 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우 5천만원 이하의 과태료

1.4.2 정보주체(이용자) 또는 그 대리인 개인정보 열람 요구를 하는 경우 규정된 기간내에 열람 가능하도록 필요한 조치를 하고 있습니까?			
항목구분			
대구분	개인정보보호 관리체계	**항목코드**	1.4.2
중구분	정보주체 권리보장	**중요도**	**H**
항목 개요	정보주체(이용자) 또는 그 대리인으로부터 개인정보 열람을 요구 받은 경우 10일 이내(또는 지체 없이)에 정보주체가 해당 개인정보를 열람할 수 있도록 조치하는지 확인이 필요함.		
평가기준			
판단 기준	Y - 정보주체의 개인정보 요구에 대한 개인정보처리자의 조치 불복의 경우 절차가 있음. N - 정보주체의 개인정보 요구에 대한 개인정보처리자의 조치 불복의 경우 절차가 없음		
점검 방법	▶ 정보주체(이용자) 또는 그 대리인으로부터 개인정보 열람을 요구 받은 경우 10일 이내(또는 지체 없이)에 정보주체가 해당 개인정보를 열람할 수 있도록 조치하는지 확인 ① 개인정보보호법 - 개인정보의 항목 및 내용 - 개인정보의 수집, 이용의 목적 - 개인정보 보유 및 이용 기간 - 개인정보의 제3자 제공 현황 - 개인정보 처리에 동의한 사실 및 내용 ② 정보통신망법 - 정보통신서비스 제공자 등이 가지고 있는 이용자의 개인정보 - 정보통신서비스 제공자 등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황 - 정보통신서비스 제공자 등에게 개인정보 수집, 이용, 제공 등의 동의를 한 현황 ▶ 정보주체(이용자) 또는 그 대리인으로부터 개인정보의 처리정지 요구를 받은 경우 특별한 사유가 없는 한 지체 없이 처리의 전부 또는 일부를 정지하고 그 결과를 정보주체(이용자)에게 알리는지 확인 ① 개인정보 정정, 삭제 요구를 받은 날부터 10일 이내에 조치 결과 회신		



■ 개인정보 보호법 시행규칙 [별지 제9호서식]

개인정보 ([ ] 열람 [ ] 일부열람 [ ] 열람연기 [ ] 열람거절) 통지서

(앞 쪽)

수신자 (우편번호: , 주소:)

요구 내용			
열람 일시		열람 장소	
통지 내용 ([ ] 열람 [ ] 일부열람 [ ] 열람연기 [ ] 열람거절)			
열람 형태 및 방법	열람 형태	[ ] 업무 · 시험 [ ] 사본 · 출력물 [ ] 전자매체 [ ] 복제물 · 인화물 [ ] 기타	
	열람 방법	[ ] 직접 방문 [ ] 우편 [ ] 팩스 [ ] 전자우편 [ ] 기타	
납부 금액	①수수료 원	②우송료 원	계(①+②) 원
	수수료 산정 명세		
사 유			
이의제기방법	※ 개인정보처리자는 이의제기방법을 적습니다.		

「개인정보 보호법」 제35조제3항·제4항 또는 제5항과 같은 법 시행령 제41조제4항 또는 제42조제2항에 따라 귀하의 개인정보 열람 요구에 대하여 위와 같이 통지합니다.

년 월 일

발 신 명 의 직인

유의사항

1. 개인정보 열람 장소에 오실 때에는 이 통지서를 지참하셔야 하며, 요구인 본인 또는 그 정당한 대리인임을 확인하기 위하여 다음의 구분에 따른 증명서를 지참하셔야 합니다.
   가. 요구인 본인에게 공개할 때: 요구인의 신원을 확인할 수 있는 신분증명서(주민등록증 등)
   나. 요구인의 대리인에게 공개할 때: 대리인임을 증명할 수 있는 서류와 대리인의 신원을 확인할 수 있는 신분증명서
2. 수수료 또는 우송료는 다음의 구분에 따른 방법으로 냅니다.
   가. 국가기관인 개인정보처리자에게 내는 경우: 수입인지
   나. 지방자치단체인 개인정보처리자에게 내는 경우: 수입증지
   다. 국가기관 및 지방자치단체 외의 개인정보처리자에게 내는 경우: 해당 개인정보처리자가 정하는 방법
   ※ 국회, 법원, 헌법재판소, 중앙선거관리위원회, 중앙행정기관 및 그 소속 기관 또는 지방자치단체인 개인정보처리자에게 수수료 또는 우송료를 내는 경우에는 「전자금융거래법」 제2조제11호에 따른 전자지급수단 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제10호에 따른 통신과금서비스를 이용하여 수수료 또는 우송료를 낼 수 있습니다.
3. 열람제한, 열람연기 또는 열람거절의 통지를 받은 경우에는 개인정보처리자가 이의제기방법란에 적은 방법으로 이의제기를 할 수 있습니다.

210㎜×297㎜[신문용지 54g/㎡]

※ 출처: 개인정보보호법 시행규칙 별지 제9서식

<그림 15> 개인정보 열람 통지서

관련 근거	※ 개인정보보호법 <제38조> 권리행사의 방법 및 절차 ※ 개인정보보호법 <제20조> 정보주체 이외 로부터 수집한 개인정보의 수집 출처 등 고지
과징금 및 벌칙	※ 개인정보보호법 <제20조의제1항> 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우 5천만원 이하의 과태료

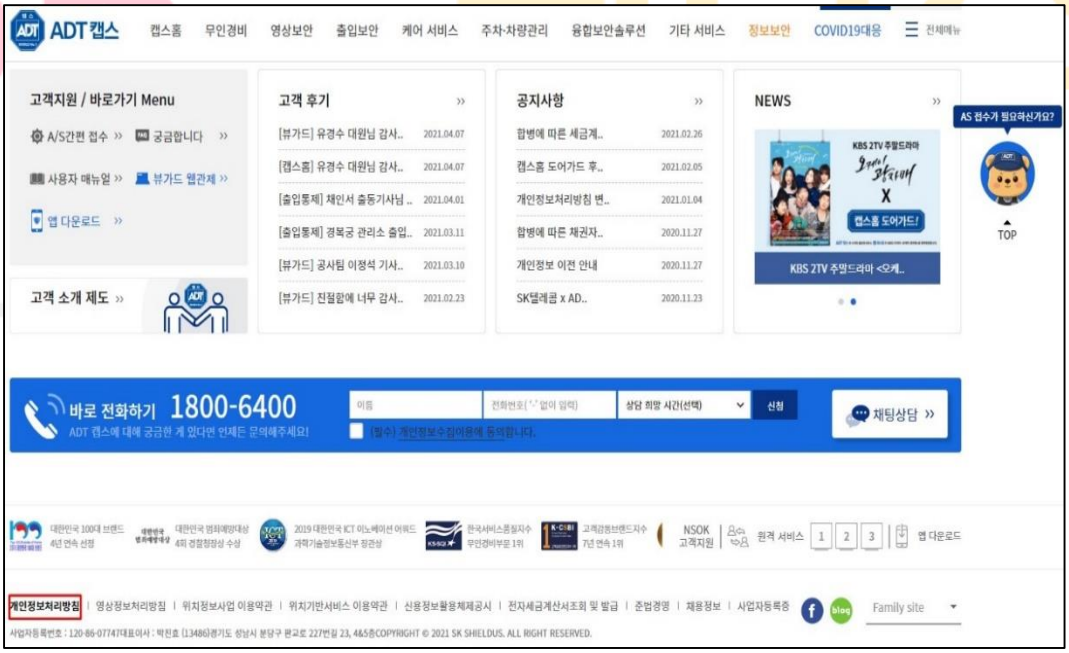
2. 개인정보처리시스템 관리적 보호조치

2.1. 개인정보 처리방침

2.1.1 개인정보 처리방침이 적절하게 수립되어 있습니까?			
항목구분			
대구분	개인정보 관리적 보호조치	**항목코드**	2.1.1
중구분	개인정보 처리방침	**중요도**	**H**
항목 개요	개인정보를 처리하는 경우 "개인정보 처리방침"을 정하여 정보주체가 언제든 확인할 수 있도록 공개하여 하고, 준수해야 함.		
평가기준			
판단 기준	Y - 개인정보 처리방침이 적절하게 수립되어 있음 P - 개인정보 처리방침이 수립되어 있으나 일부 누락된 내용이 있음 N - 개인정보 처리방침을 수립하고 있지 않음		
점검 방법	▶ 개인정보 처리방침이 수립되어 있으며, 아래 내용이 빠짐없이 포함되어 있는지 확인 ① 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집방법(수집하는 개인정보의 필수/선택 구분) ② 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법인인 경우 법인의 명칭), 제공받는 자의 이용 목적과 제공하는 개인정보의 항목 - 위탁에 대한 동의가 필요한 경우, 법령에 따라 필요한 사항을 알리고 동의 필요 - 수탁자 변동 또는 위탁업무 범위 및 계약상의 변동사항이 발생할 경우, 정보주체(이용자)로부터 별도의 동의 또는 고지 절차 필요 ③ 개인정보의 보유 및 이용 기간 (1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위한 개인정보의 파기 등 필요한 조치) ④ 개인정보의 파기절차 및 파기방법 (개인정보를 보존하여야 하는 경우, 보존근거와 보존하는 개인정보 항목을 포함) ⑤ 개인정보 처리위탁을 하는 업무의 내용 및 수탁자 (해당되는 경우에만 처리방침에 포함) ⑥ 이용자 및 법정대리인의 권리와 그 행사방법 ⑦ 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항 - 서비스 이용 과정에서 생성되는 정보: 쿠키, 결제기록, 접속정보 등		

	⑧ 개인정보 보호책임자/보호책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처 ⑨ 개인정보안정성 확보조치 ⑩ 개인정보처리방침의 변경에 관한 사항 (변경일자, 버전(일자)별 관리, 이전 버전 전문확인 등)  **<그림 16> 개인정보처리방침 수립 예시**
관련 근거	※ 개인정보보호법 <제30조> 개인정보 처리방침의 수립 및 공개 ※ 개인정보보호법 시행령 <제31조> 개인정보 처리방침의 내용 및 공개방법 등 ※ 개인정보처리방침 작성 가이드라인
과징금 및 벌칙	※ 개인정보보호법 <제30조의제1항, 2항> 개인정보 처리방침을 정하지 않거나 공개하지 않은 경우 1천만원 이하의 과태료

2.1.2 개인정보 처리방침을 Website/Mobile App에 고지 시 첫 화면에 링크명을 "개인정보

<table>
<tr><th colspan="4">처리방침”으로 하여 눈에 띄게 표시되어 있습니까?</th></tr>
<tr><th colspan="4">항목구분</th></tr>
<tr><td>대구분</td><td>개인정보 관리적 보호조치</td><td>항목코드</td><td>2.1.2</td></tr>
<tr><td>중구분</td><td>개인정보 처리방침</td><td>중요도</td><td>H</td></tr>
<tr><td>항목
개요</td><td colspan="3">개인정보를 처리하는 경우 “개인정보 처리방침”을 정하여 정보주체가 언제든 확인할 수 있도록 공개하여 하고, 준수해야 함.</td></tr>
<tr><th colspan="4">평가기준</th></tr>
<tr><td>판단
기준</td><td colspan="3">Y - "개인정보 처리방침"을 적절하게 표기하여 게시함
P - "개인정보 처리방침"을 게시하고 있으나 표기방법을 준수하지 못함
N - "개인정보 처리방침"을 적절하게 고지하고 있지 않음
N/A - 대외 서비스중인 Website/Mobile App이 없음</td></tr>
<tr><td>점검
방법</td><td colspan="3">▶ 개인정보 처리방침 고지 관련 사항 확인
① 개인정보 처리방침을 Website/Mobile App을 통해 고지할 경우, 첫 화면에 링크명을 "개인정보 처리방침"으로 하여 링크 설정 및 글자 크기/색상을 달리하여 눈에 띄도록 조치여부 확인
 

<그림 17> 개인정보처리방침 공개 예시</td></tr>
<tr><td>관련
근거</td><td colspan="3">※ 개인정보보호법 <제30조> 개인정보 처리방침의 수립 및 공개
※ 개인정보보호법 시행령 <제31조> 개인정보 처리방침의 내용 및 공개방법</td></tr>
</table>

과징금 및 벌칙	※ 개인정보보호법 <제30조의제1항, 2항> 개인정보처리방침을 정하지 않거나 공개하지 않은 경우 1천만원 이하의 과태료

2.1.3 개인정보 처리방침 변경 시 변경 이유 및 내용을 공지하고 있습니까?			
항목구분			
대구분	개인정보 관리적 보호조치	**항목코드**	2.1.3
중구분	개인정보 처리방침	**중요도**	**H**
항목 개요	"개인정보 처리방침"의 변경 시, 변경 이유 및 내용을 인터넷 홈페이지의 첫 화면에 공지사항 or 팝업창을 통해 공지하거나 전자우편을 통해 공지하여야 함.		
평가기준			
판단 기준	Y - "개인정보 처리방침"의 변경 내용을 적절하게 공지하고 있음 N - "개인정보 처리방침"의 변경 내용의 공지를 시행하지 않음 N/A - 대외 서비스중인 Website/Mobile App이 없음		
점검 방법	▶ 개인정보 처리방침 고지 관련 사항 확인 ① 개인정보 처리방침의 변경 시, 변경 이유 및 내용을 인터넷 홈페이지의 첫 화면에 공지사항 또는 팝업창을 통해 공지하거나 전자우편을 통해 공지하였는지 확인		
관련 근거	※ 개인정보보호법 <제30조> 개인정보 처리방침의 수립 및 공개 ※ 개인정보보호법 시행령 <제31조> 개인정보 처리방침의 내용 및 공개방법		
과징금 및 벌칙	※ 개인정보보호법 <제30조의제1항, 2항> 개인정보처리방침을 정하지 않거나 공개하지 않은 경우 1천만원 이하의 과태료		
2.1.4 개인정보 처리방침을 버전별로 관리하고, 이전 버전에 대해 확인 가능하게 제공하고 있습니까?			

<그림 18> 개인정보처리방침 변경사항 공지 예시

<table>
<tr><th colspan="4">항목구분</th></tr>
<tr><td>대구분</td><td>개인정보 관리적 보호조치</td><td>항목코드</td><td>2.1.4</td></tr>
<tr><td>중구분</td><td>개인정보 처리방침</td><td>중요도</td><td>H</td></tr>
<tr><td>항목
개요</td><td colspan="3">"개인정보 처리방침"이 버전별로 관리되고, 이전 버전에 대해 확인 가능 해야 함</td></tr>
<tr><th colspan="4">평가기준</th></tr>
<tr><td>판단
기준</td><td colspan="3">Y - "개인정보 처리방침"을 버전별로 관리하고 이전 버전을 확인할 수 있도록 제공
N - "개인정보 처리방침"을 버전별로 관리하고 있지 않거나 이전 버전을 확인할 수 있도록 제공하지 않음
N/A - 대외 서비스중인 Website/Mobile App이 없음</td></tr>
<tr><td>점검
방법</td><td colspan="3">▶ 개인정보 처리방침 고지 관련 사항 확인
① 개인정보 처리방침을 버전별로 관리하고 이전 버전을 확인할 수 있도록 제공하고 있는지 확인
 

<그림 19> 개인정보처리방침 버전 별 확인 예시</td></tr>
<tr><td>관련
근거</td><td colspan="3">※ 개인정보보호법 <제30조> 개인정보 처리방침의 수립 및 공개
※ 개인정보보호법 시행령 <제31조> 개인정보 처리방침의 내용 및 공개방법</td></tr>
<tr><td>과징금
및</td><td colspan="3">※ 개인정보보호법 <제30조의제1항,2항> 개인정보처리방침을 정하지 않거나 공개하지 않은 경우 1천만원 이하의 과태료</td></tr>
</table>

벌칙	

2.2. 개인정보취급자 관리

2.2.1 업무별로 접근권한은 구분되어 있고, 최소한의 업무수행자(1인 1계정 사용 등)에게만 부여하고 있습니까?

항목구분			
대구분	개인정보 관리적 보호조치	**항목코드**	2.2.1
중구분	개인정보취급자 관리	**중요도**	**H**
항목 개요	개인정보 취급자의 업무별로 접근권한을 구분하여. 해당 업무 범위 내에서만 권한을 최소한으로 부여하고 있어야 함.		
평가기준			
판단 기준	Y - 업무별 접근권한의 분리 및 최소화 적용 N - 업무별 접근권한의 분리 및 최소화 미적용		
점검 방법	▶ 업무별 접근권한 구분되어 최소한의 업무수행자에게만 부여 확인 ① 관리자, 일반사용자 등으로 업무별 접근권한 구분 (OS, DB, App(Web, Mobile App, C/S) 모두 포함) ② 접근이 타당한 업무수행자에게 최소화(사용자 1인 1계정) 부여 확인 - 관리자 외의 사용자에게 Admin 권한이 제한되어 있고, 관리자/사용자 그룹에 불필요한 사용자가 존재하는지 확인 (OS, DB, Web/Mobile App) - 관리자 계정 및 권한의 타당성 검토 및 책임자/담당자 승인 여부 (Super User, 업무상 불가피한 공용계정 포함) ③ 정보시스템 설치 후 제조사 또는 판매사의 기본 계정(Admin 등), 시험 계정 등은 제거하거나 추측하기 어려운 계정으로 변경 여부 (디폴트 패스워드 변경 포함)		
관련	※ 개인정보보호법 <제29조> 안전조치의무		

메뉴명		개인정보처리여부	권한 그룹														
			최고 관리자					회원 관리자					게시판 관리자				...
1단계	2단계		조회	쓰기	수정	삭제	다운로드	조회	쓰기	수정	삭제	다운로드	조회	쓰기	수정	삭제	다운로드	...
회원관리	회원정보 관리	O	V	V	V	V	V	V	V	V	V	-	-	-	-	-	-	
	문의/상담 관리	O	V	V	V	V	V	V	V	V	V	-	-	-	-	-	-	
	회원 통계	O	V	V	V	V	V	V	V	V	V	-	-	-	-	-	-	
게시판 관리	공지사항	-	V	V	V	V	V	V	-	-	-	-	V	V	V	V	-	
	자유게시판	O	V	V	V	V	V	V	-	-	-	-	V	V	V	V	-	
...	...																	

※ 출처: 개발자 대상 개인정보 보호조치 적용 가이드

<그림 20> 사용자 별 접근 권한 설정

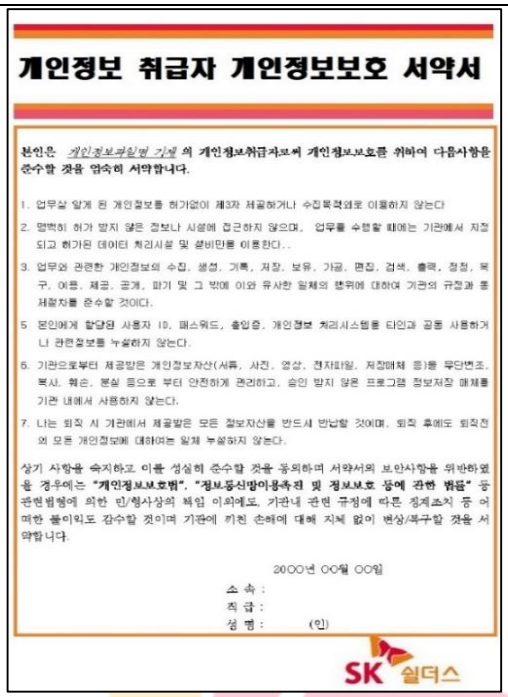
근거	※ 개인정보보호법 <제39조의5> 개인정보의 보호조치에 대한 특례 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제5조> 접근 권한의 관리 ※ 표준 개인정보 보호지침 <제15조> 개인정보취급자에 대한 감독
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보조치 의무를 위반한 경우 3천만원 이하 과태료

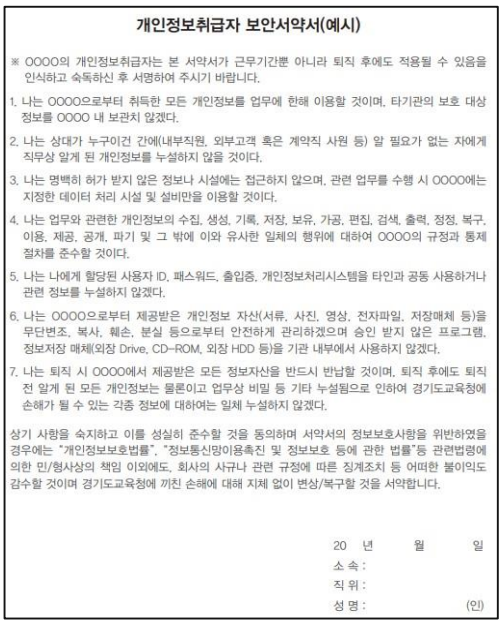
2.2.2 접근권한 추가/삭제/변경 절차를 보유하고 있습니까?			
항목구분			
대구분	개인정보 관리적 보호조치	**항목코드**	2.2.2
중구분	개인정보취급자 관리	**중요도**	**H**
항목 개요	개인정보처리시스템에 접근할 수 있는 계정 추가 시 인가된 사용자만 접근이 가능하도록 접근권한 추가/삭제/변경에 대한 절차 및 현황 관리가 되어야 함.		
평가기준			
판단 기준	Y - 계정 관리 절차를 수립하고 이행함 N - 계정 관리 절차가 수립되지 않음		
점검 방법	▶ 접근권한 관리 절차 확인 ① 계정 추가/삭제/변경 절차 존재 여부 확인 ex) 계정 추가/삭제/변경 요청 시 담당자에게 메일/신청서로 관련 요청을 하고(담당자는 신청현황 관리), 담당자는 이 내역을 시스템 운영자에게 전달하여 반영 ※ 관리 절차 내역 증적(메일/신청서)으로 확인		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제5조> 접근 권한의 관리		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보조치 의무를 위반한 경우 3천만원 이하 과태료		

2.2.3 개인정보 다운로드 권한은 반드시 필요한 인력에게만 부여되어 있습니까?			
항목구분			
대구분	개인정보 관리적 보호조치	**항목코드**	2.2.3
중구분	개인정보취급자 관리	**중요도**	**H**
항목 개요	개인정보 다운로드 기능이 존재하는 경우, 최소한의 인력에게 최소화의 정보만 다운로드가 가능하게 설정되어야 함		
평가기준			
판단 기준	Y - 개인정보 다운로드 권한을 합리적으로 부여하고 있음 N - 1) 개인정보 다운로드 권한을 부적절하게 부여하고 있음 2) 개인정보 다운로드가 가능하나 권한 분리 기능이 존재하지 않음 N/A - 개인정보 다운로드 기능이 존재하지 않음		
점검 방법	▶ 개인정보 다운로드 기능 권한 부여 확인 ① 다운로드 기능이 존재하는 경우, 권한 부여 현황 확인 - 해당 기능의 취급자 별 권한 확인 - 취급자 별 권한이 분리되어 있지 않을 경우, 다운로드 가능 인력에 대한 당위성 확인		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제5조> 접근 권한의 관리		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보조치 의무를 위반한 경우 3천만원 이하 과태료		

2.2.4 개인정보취급자 목록을 최신화하고 있으며, 불필요 계정에 대한 제한을 하고 있습니까?			
항목구분			
대구분	개인정보 관리적 보호조치	**항목코드**	2.2.4
중구분	개인정보취급자 관리	**중요도**	**H**
항목 개요	개인정보를 처리하는 모든 인원의 목록 최신화 및 변동 발생 시 지체없이 접근권한의 변경 또는 말소를 수행하여야 함		
평가기준			
판단 기준	Y - 개인정보취급자 목록 최신화 적용 P - 개인정보취급자 목록을 관리 중이나 일부 누락 N - 개인정보취급자 목록을 관리하지 않음		
점검 방법	▶ 개인정보취급자 목록 최신화 확인 ① 목록에는 개인정보를 처리하는 모든 인원(임직원, 파견 근로자, 시간제 근로자 등)이 포함되어 있는지 확인 ② 프로젝트 투입, 종료 및 인력 퇴직 등 개인정보취급자 변동 발생 시 지체없이 접근권한의 변경 또는 말소 확인 ③ 불필요한 계정 제한 개인정보취급자 현황(계정관리대장 등)과 실제 사용자 계정을 비교하여 불필요한 계정 존재 여부 확인 ④ 개인정보 취급자 관리대장 보유여부		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제5조> 접근 권한의 관리 ※ 표준 개인정보 보호지침 <제15조> 개인정보취급자에 대한 감독		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보조치 의무를 위반한 경우 3천만원 이하 과태료		

2.2.5 개인정보취급자에 대해 보안서약서를 징구하고 있습니까?			
항목구분			
대구분	개인정보 관리적 보호조치	**항목코드**	2.2.5
중구분	개인정보취급자 관리	**중요도**	**H**
항목 개요	개인정보 취급자에 대해서 입사 및 퇴사 시 보안서약서를 징구하고, 연 1회 이상 갱신해야 함.		
평가기준			
판단 기준	Y - 표준 보안서약서를 사용하고 있고, 연 1회 이상 징구하고 있음 P - 1) 표준 보안서약서를 징구하고 있으나, 누락인원이 존재하거나, 연 1회 이상 갱신을 하지 않음 2) 비밀누설, 업무규정 등이 기재된 자체 보안 서약서를 사용하여 연 1회 이상 징구하고 있음 N - 징구하고 있지 않음		
점검 방법	▶ 보안서약서 징구 여부 및 절차 확인 ① 입사 및 퇴사 시 징구 여부 확인 ② 정기적인 서약서 갱신 여부 확인(연 1회 이상) ③ 사업/운영부서 담당자 관리 여부 확인 ▶ 보안서약서 상 명시내용 확인 ① 개인정보 탐지·누출·변조·훼손에 관한 사항 ② 비밀누설에 관한 사항 ③ 보안업무규정 준수에 관한 사항 ④ 보안서약서 위반시 발생하는 처벌 감수에 관한 사항 등		

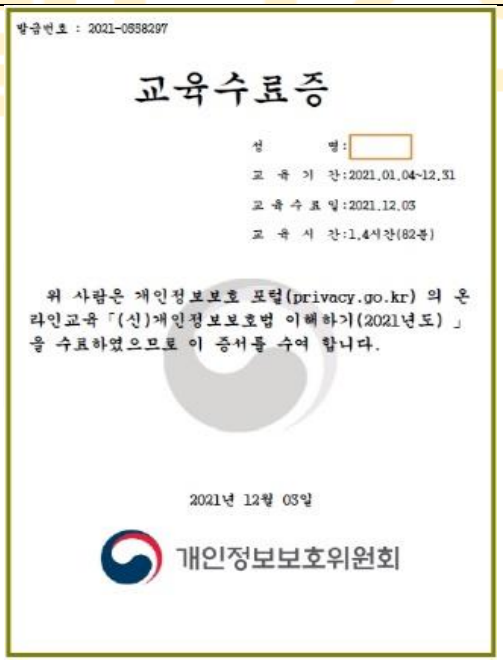
<table>
<tr>
<td></td>
<td>




※ 출처: 개인정보보호법시행령 별첨양식

<그림 21> 개인정보취급자 보안서약서 예시
</td>
</tr>
<tr>
<td>관련
근거</td>
<td>※ 개인정보보호법 <제28조> 개인정보취급자에 대한 감독
※ 개인정보보호법 <제29조> 안전조치의무
※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치
※ 표준개인정보 보호지침<제15조> 개인정보취급자에 대한 감독
※ 정보보호 및 개인정보보호 관리체계 인증 <2.2.3> 보안 서약</td>
</tr>
<tr>
<td>과징금
및
벌칙</td>
<td>※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금
※ 개인정보보호법 <제29조> 안전성 확보조치 의무를 위반한 경우 3천만원 이하 과태료</td>
</tr>
</table>

2.2.6 개인정보 취급자가 연 1회 이상 정기적인 교육을 수행하고 있습니까? (정보통신망법 회원가입 웹 페이지 취급자 연 2회)			
항목구분			
대구분	개인정보 관리적 보호조치	**항목코드**	2.2.6
중구분	개인정보취급자 관리	**중요도**	**H**
항목 개요	개인정보 취급자에 대해서 입사 및 퇴사 시 보안서약서를 징구하고, 연 1회 이상 갱신해야 함.		
평가기준			
판단 기준	Y - 개인정보보호 교육을 실시하는 경우 N - 개인정보보호 교육을 실시하지 않은 경우		
점검 방법	▶ 개인정보취급자(임직원, 파견근로자, 시간제 근로자 등) 법적 요구사항에 따라 연 1회 이상 개인정보보호 교육 수행 확인 (정보통신망법 회원가입 웹페이지 개인정보취급자는 연2회) ① 개인정보보호 교육 결과 보고 확인 ② 개인정보보호 취급자 별 온라인 상 개인정보보호 교육 수료증 확인		
관련	※ 개인정보보호법 <제28조> 개인정보취급자에 대한 감독		



※ 출처: 개인정보보호 교육 포털

<그림 22> 온라인 개인정보보호 교육 수료증

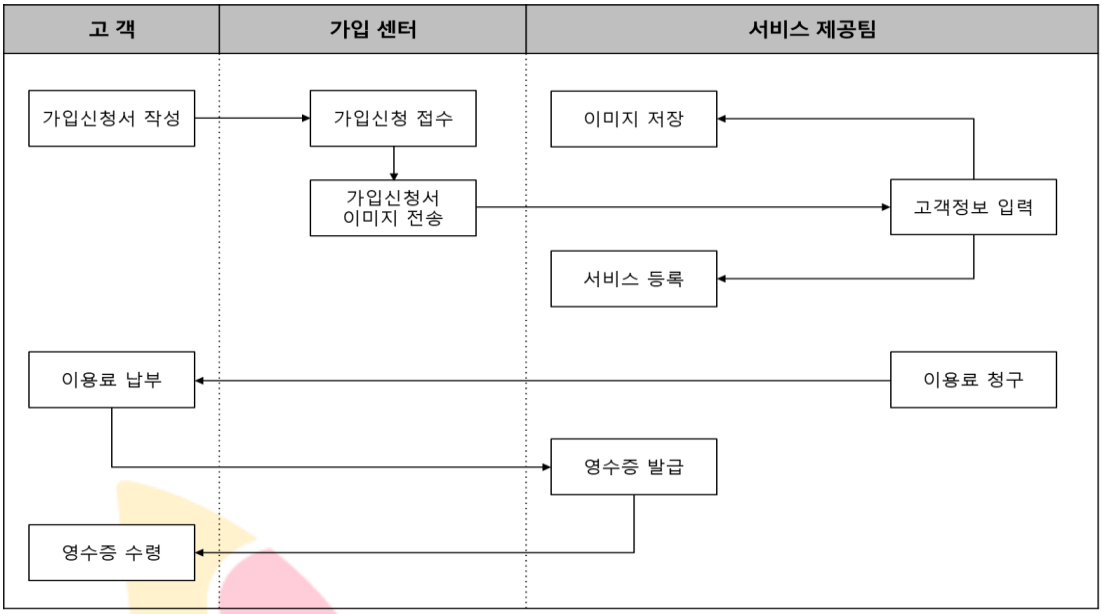
근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 표준개인정보 보호지침<제15조> 개인정보취급자에 대한 감독 ※ 정보보호 및 개인정보보호 관리체계 인증 <2.2.3> 보안 서약
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보조치 의무를 위반한 경우 3천만원 이하 과태료

2.3. 개인정보파일 관리

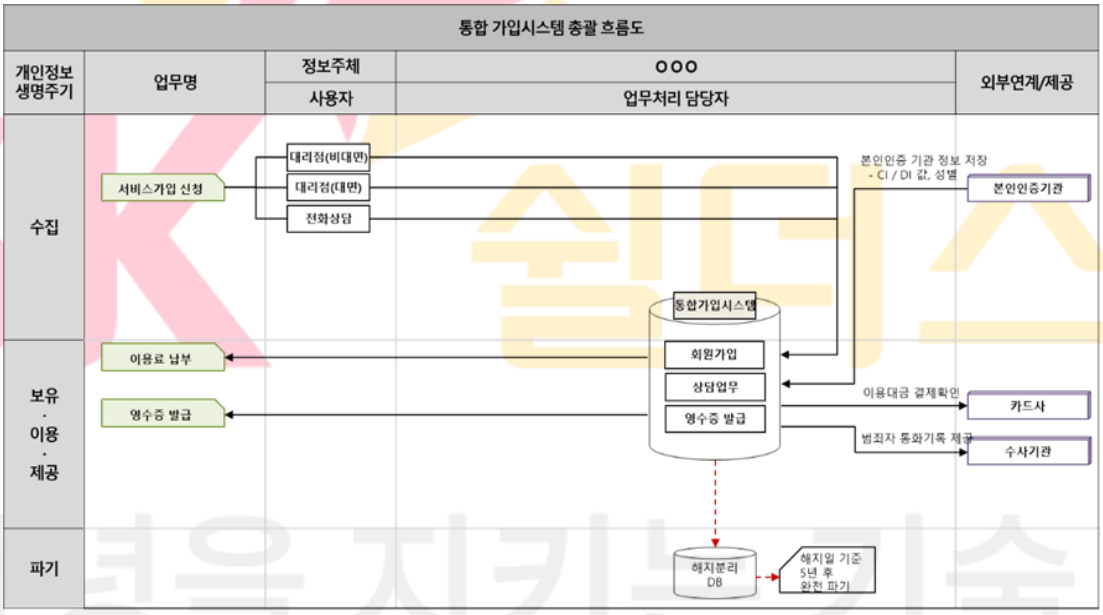
2.3.1 수집, 보유하고 있는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리하고 있습니까?			
항목구분			
대구분	개인정보 관리적 보호조치	**항목코드**	2.3.1
중구분	개인정보파일 관리	**중요도**	**H**
항목 개요	수집 보유 중인 개인정보에 대한 현황 및 흐름 등 개인정보 생명주기에 맞춰 기록 관리되어야 함.		
평가기준			
판단 기준	Y - 개인정보 수집 보유에 대한 정기적인 관리를 하고 있음 N - 개인정보 수집 보유에 대한 정기적인 관리를 되지 않음		
점검 방법	▶ 수집, 보유하고 있는 개인정보의 항목, 보유량, 처리 목적 및 방법, 보유기간 등 현황을 정기적으로 관리 여부 ① 개인정보 처리목적 및 업무 ② 보유 수량 처리 근거 ③ 개인정보 흐름표 및 흐름도		

업무명	처리목적	처리 개인정보	담당부서	고객정보 건수 (고유식별정보 수)	법적근거	중요도
회원가입	서비스 제공	필수 : 성명, 생년월일, 이메일 선택 : 직장주소	고객관리팀	100만건 (0건)	정보주체동의	5
세금계산서발급	서비스 이용 세금계산서발행	필수 성명, 이메일 전화번호	세무회계팀	3천건 (0건)	부가가치세법 <제71조>정부의 작성·보관	5
상담업무	고객 문의 및 응대	필수: 성명 전화번호, 녹취파일	고객관리팀	6만건 (0건)	정보주체동의	3

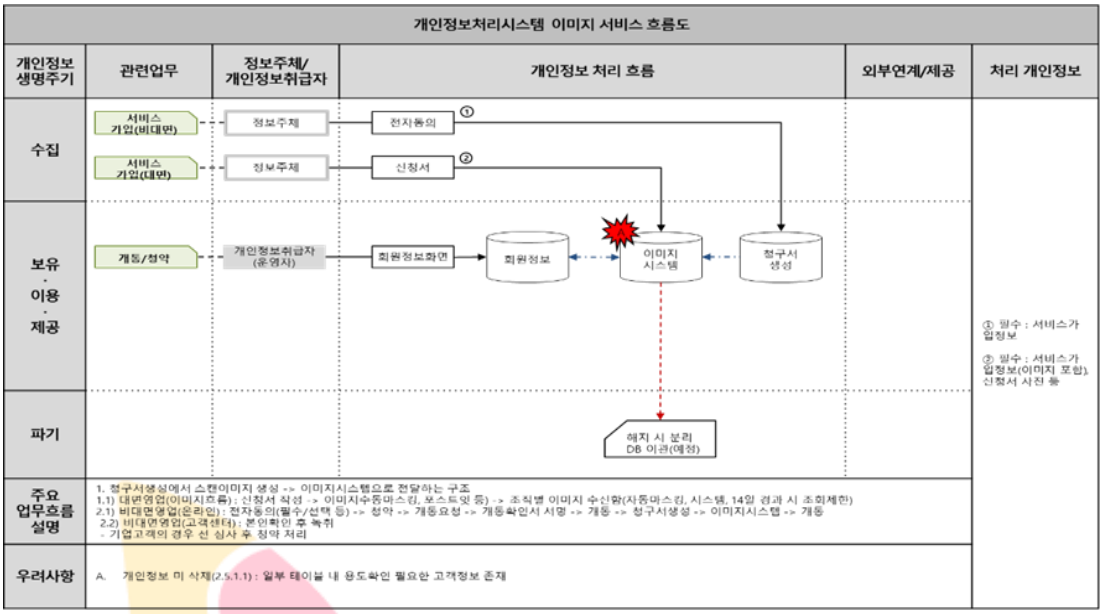
<그림 23> 개인정보 업무 현황표



<그림 24> 개인정보처리 업무 흐름



<그림 25> 개인정보처리시스템 총괄 흐름도



<그림 26> 개인정보처리시스템 흐름도

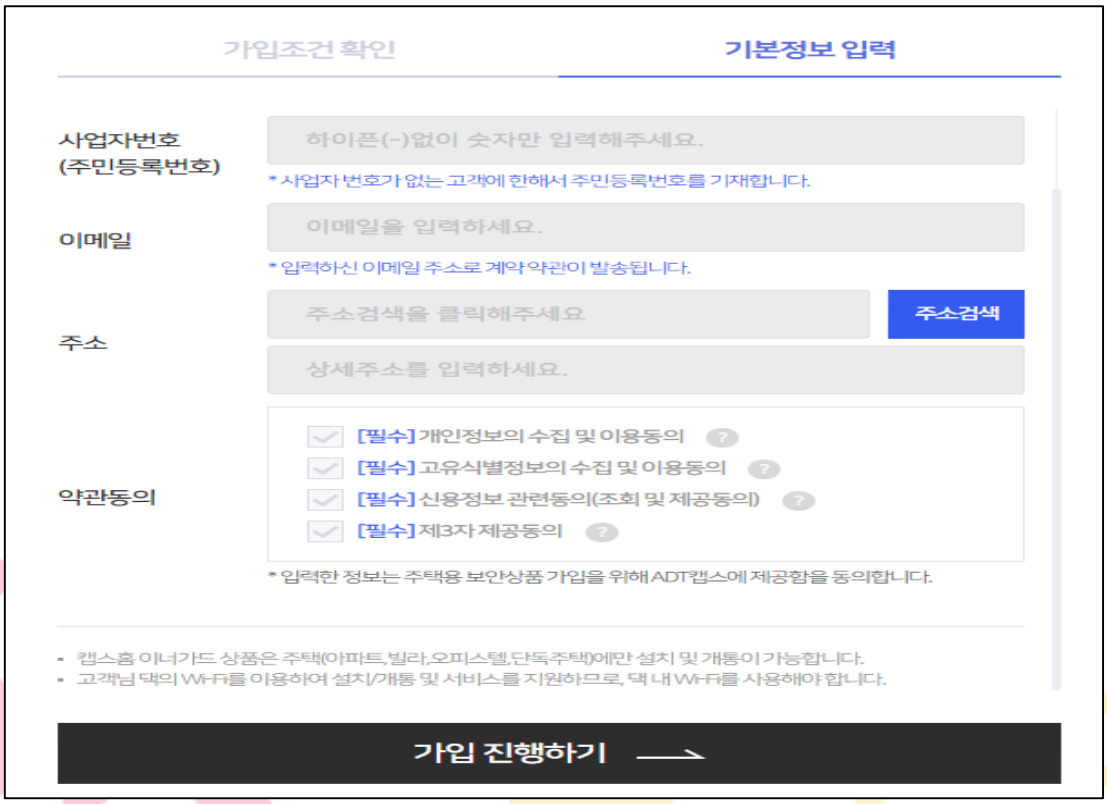
관련 근거	※ 개인정보보호법 <제29조> 안전성 확보 조치 ※ 개인정보 보호법 <제32조> 개인정보파일의 등록 및 공개
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금

3. 개인정보 처리단계별 보호조치

3.1. 개인정보 수집

3.1.1 개인정보 수집 동의를 이용자가 이해하기 쉽게 받고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.1.1
중구분	개인정보 수집	**중요도**	**H**
항목 개요	개인정보 수집 시 간결/명확한 방법으로 이용자가 이해하기 쉽게 동의 받아야 함		
평가기준			
판단 기준	Y - "개인정보 수집 시 동의 방법"에 따라 동의 받고 있음 N - "개인정보 수집 시 동의 방법"에 따라 동의 받고 있지 않음		
점검 방법	▶ 개인정보 수집 동의서/동의화면 작성 시 고려사항 ① "법정 고지사항"만을 간결하게 고지하고, "쉬운 용어", "중요내용은 부호, 색채, 굵고 큰 문자 등"을 활용하여 명확하게 표시 ② 동의가 선택인 사항은 명확히 표시 - 불가피하게 전문용어를 사용하는 경우에는 별도의 용어 설명을 제공 - 글씨의 크기는 최소한 9포인트 이상으로서 다른 내용보다 20퍼센트 이상 크게 하여 알아보기 쉽게 할 것 - 글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 할 것 - 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시 - 14세 미만의 아동에게 개인정보 처리와 관련한 사항의 고지 등을 하는 때에는 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어를 사용 ▶ 개인정보 수집 시 동의 방법 ① 인터넷 사이트 - 동의를 구하는 화면(회원가입 화면, 로그인 화면, 이벤트 참여 화면 등) 또는 동의를 구하는 절차 상에서 동의 내용을 게재하고 정보주체가 동의 여부를 직접 표시하도록 함 - 동의/비동의란 모두 공란으로 처리하거나 비 동의 란에 Default Check하여 정보주체가 직접 동의 란에 Check하도록 해야 함		

- 필수동의와 선택동의를 순차적으로 구성하여 이용자가 이해하기 쉽도록 구성
- 화면 배경과 글자 색 등은 이용자가 읽기 쉽도록 조합하여 사용하도록 구성
- 일괄동의 기능에 선택동의 사항이 포함되어 있는 경우 선택동의 사항이 포함되어 있음을 알린 후 동의를 받아야 함



<그림 27> 개인정보 수집 시 동의 방법 예시 (캡스홈)

② 서면

- 동의 내용이 기재된 서면(가입신청서 등)을 정보주체에게 직접 교부, 우편 또는 Fax등을 통해 전달하고, 정보주체가 기명날인 하거나 자필 서명 후 제출하도록 함

③ 전자우편

- 동의 내용이 기재된 전자우편을 발송하여 동의 의사가 표시(동의 란에 체크)된 전자우편을 전송 받도록 함

④ 전화

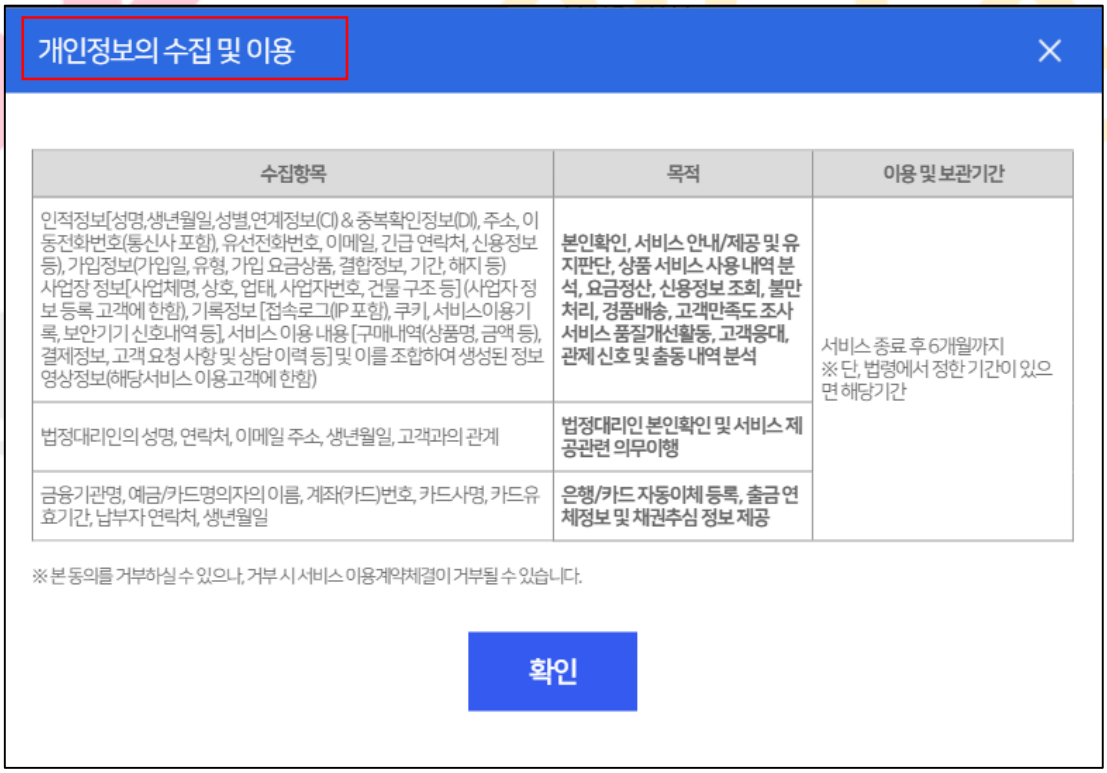
- 전화를 통해 개인정보를 수집하는 경우에는 '법정 고지사항'을 '일상 대화 속도'로 설명하고 이해했는지 여부를 확인
- 전화를 통해 동의 내용을 전부 전달하기가 곤란한 경우 정보주체가 동의 내용을 확인할 수 있는 방법을 안내하고, 재차 전화를 통해 동의를 얻도록 함

⑤ Mobile 기기

- 모바일 기기에 보여줄 수 있는 최소한의 법정고지사항을 알리고 동의를 받되,

	별도의 웹 사이트를 운영하고 있는 경우에는 확인할 수 있는 방법을 안내
관련 근거	※ 개인정보보호법 <제15조> 개인정보의 수집·이용 ※ 개인정보보호법 <제22조> 동의를 받는 방법 ※ 개인정보보호법 시행령 <제17조> 동의를 받는 방법 ※ 개인정보 최소 수집·보관을 위한 온라인 개인정보 취급 가이드라인
과징금 및 벌칙	※ 개인정보보호법 <제15조1항> 수집·이용 기준을 위반하여 개인정보를 수집한 경우 5천만원 이하 과태료 ※ 개인정보보호법 <제15조2항> 정보주체에 대한 고지의무를 위반한 경우 3천만원 이하 과태료 ※ 개인정보보호법 <제22조> 정보주체의 동의를 받을 때 각각의 동의 사항을 구분하여 동의를 받지 아니한 경우 1천만원 이하의 과태료

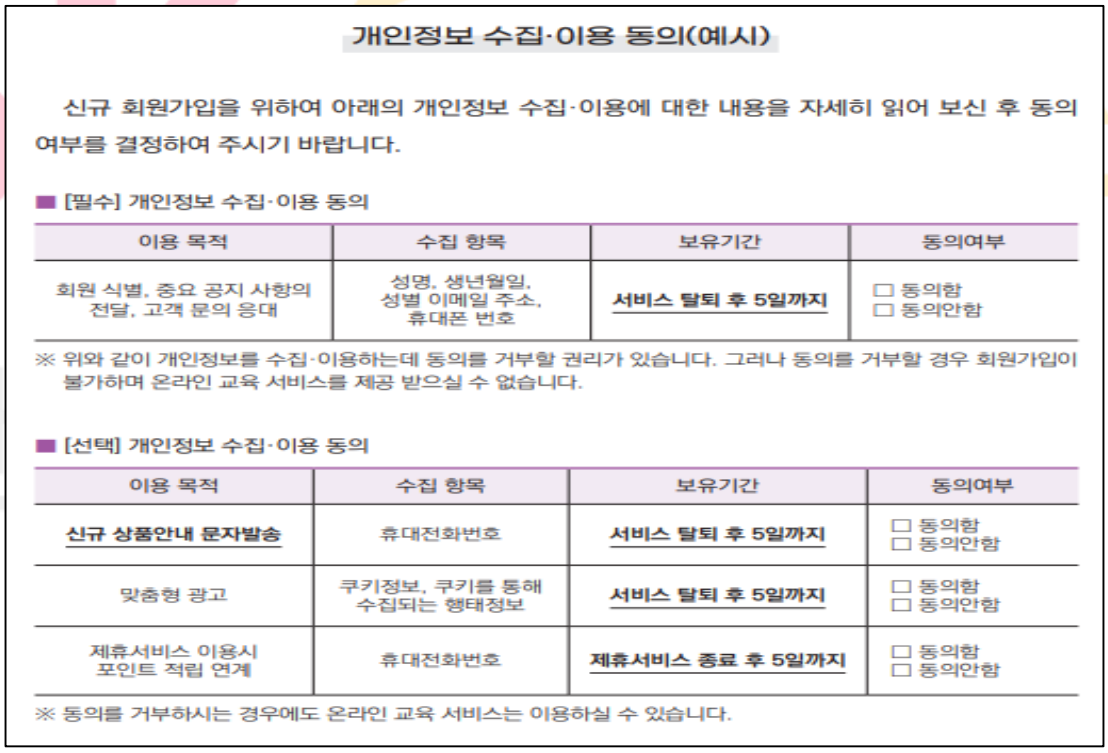
3.1.2 개인정보의 수집·이용 목적, 수집항목, 보유·이용 기간, 동의 거부권리 및 거부에 따른 불이익에 대해서 알리고 동의 받고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.1.2
중구분	개인정보 수집	**중요도**	H
항목 개요	개인정보를 수집할 시에 수집 항목에 대한 동의 획득이 우선 되어야 함.		
평가기준			
판단 기준	Y - 개인정보 수집 시 동의 받아야 할 항목에 대해 모두 동의 받고 있음 N - 개인정보 수집 시 동의 받아야 할 항목에 대해 동의 받고 있지 않음		
점검 방법	▶ 개인정보 수집 시 동의 항목 (해당 내용에 대해 별도의 동의를 받아야 함) ① 개인정보의 수집·이용 목적 ② 수집하는 개인정보의 항목 ③ 개인정보의 보유·이용 기간 ④ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 등		
관련	※ 개인정보보호법 <제15조> 개인정보의 수집·이용		



<그림 28> 개인정보 수집 방법 예시

근거	※ 개인정보보호법 <제22조> 동의를 받는 방법 ※ 개인정보보호법 <제39조의3> 개인정보 수집·이용 동의 등에 대한 특례
과징금 및 벌칙	※ 개인정보보호법 <제15조제1항> 수집·이용 기준을 위반하여 개인정보를 수집한 경우 5천만원 이하 과태료 ※ 개인정보보호법 <제15조제2항> 정보주체에 대한 고지의무를 위반한 경우 3천만원 이하 과태료 ※ 개인정보보호법 <제22조> 정보주체의 동의를 받을 때 각각의 동의 사항을 구분하여 동의를 받지 아니한 경우 1천만원 이하의 과태료

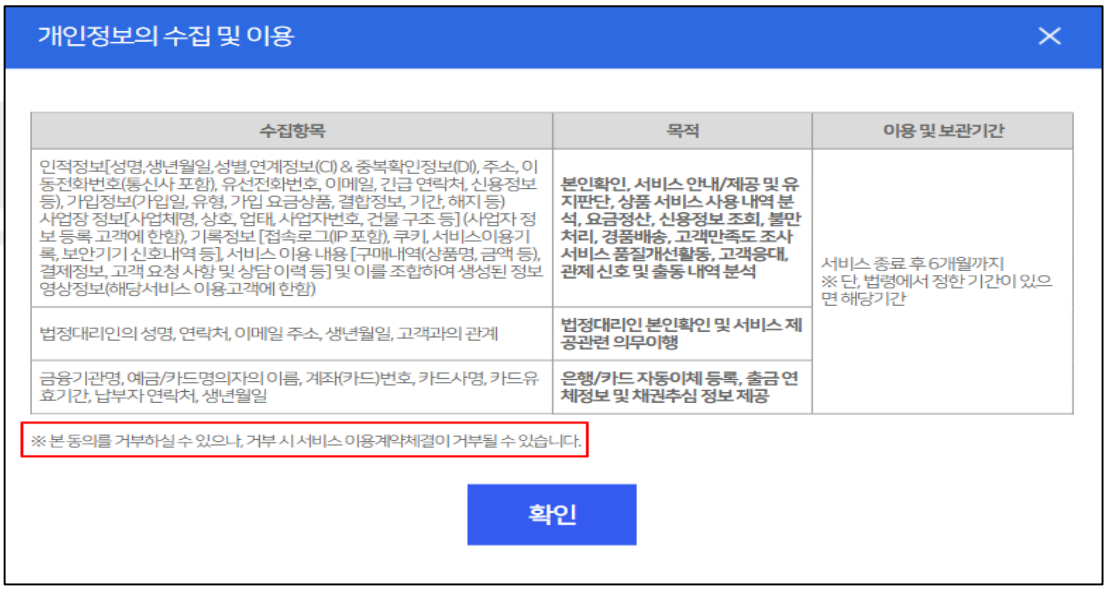
3.13 개인정보 수집 동의에 관한 기록을 항목별로 보관하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.1.3
중구분	개인정보 수집	**중요도**	**H**
항목 개요	개인정보 수집 시 동의를 받은 기록을 별도로 관리하여야 함		
평가기준			
판단 기준	Y - 개인정보 수집 동의 기록을 별도 보관하여 관리하고 있음 N - 개인정보 수집 동의 기록을 보관하고 있지 않음 N/A - 고객을 통한 직접 수집 절차 없음		
점검 방법	▶ 개인정보 수집 동의에 관한 기록의 항목별 보관여부 확인 ① 인터넷 사이트, 서면, 전자우편, 전화 등을 통하여 동의 받은 내역에 대해서 항목별 보관 및 관리 여부 확인 ② DB 등 Data 저장 내역에 이용자에게 동의 받은 기록(시점) 저장여부 확인 ex) (최초 가입일자 기준) 기록으로 남겨야 할 사항 - 필수항목/선택항목, 동의일시, 동의방법, 보존기간 등 ※ 개인정보 수집 시 필수항목만 존재하는 경우 가입일자를 동의기록으로 판별할 수 있으나, 선택항목이 존재하는 경우 선택항목에 대한 동의시점을 별도 기록/보관하여야 함		
관련 근거	※ 개인정보보호법 <제15조> 개인정보의 수집 이용 ※ 정보보호 및 개인정보보호 관리체계 인증 <3.1.2> 개인정보의 수집 동의		
과징금 및 벌칙	※ 개인정보보호법 <제15조제1항> 수집·이용 기준을 위반하여 개인정보를 수집한 경우 5천만원 이하 과태료 ※ 개인정보보호법 <제15조제2항> 정보주체에 대한 고지의무를 위반한 경우 3천만원 이하 과태료		

<table>
<tr><th colspan="4">3.1.4 개인정보 수집 시 항목이 필수항목과 선택항목으로 구분되어 있습니까?</th></tr>
<tr><th colspan="4">항목구분</th></tr>
<tr><td>대구분</td><td>개인정보 처리단계별 보호조치</td><td>항목코드</td><td>3.1.4</td></tr>
<tr><td>중구분</td><td>개인정보 수집</td><td>중요도</td><td>H</td></tr>
<tr><td>항목
개요</td><td colspan="3">개인정보는 수집 시 최소 항목만 수집하여야 하고, 수집 시 필수항목과 선택항목으로 구분하여 수집해야 함.</td></tr>
<tr><th colspan="4">평가기준</th></tr>
<tr><td>판단
기준</td><td colspan="3">Y - 개인정보 수집 시 필수항목과 선택항목으로 구분됨
N - 개인정보 수집 시 필수항목과 선택항목으로 구분되어 있지 않음
N/A - 고객을 통한 직접 수집 절차 없음</td></tr>
<tr><td>점검
방법</td><td colspan="3">▶ 수집되는 개인정보에 대해서 필수항목과 선택항목으로 구분여부 확인
- 서비스 가입신청서, Website 가입 시 수집되는 정보에 대해서 필수항목, 선택항목으로 구분되어 있어야 함
 

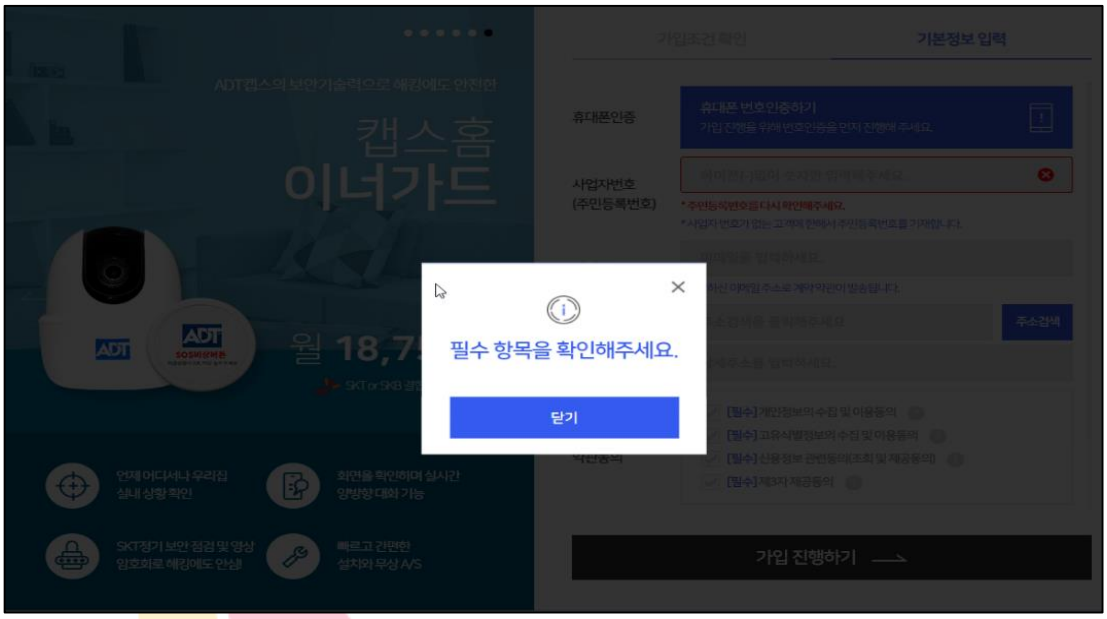
※ 출처: 개발자 대상 개인정보 보호조치 적용 가이드
<그림 29> 개인정보 필수/선택 항목 수집 방법 예시</td></tr>
<tr><td>관련
근거</td><td colspan="3">※ 개인정보보호법 <제15조> 개인정보의 수집 이용</td></tr>
</table>

과징금 및 벌칙	※ 개인정보보호법 <제15조제1항> 수집·이용 기준을 위반하여 개인정보를 수집한 경우 5천만원 이하 과태료 ※ 개인정보보호법 <제15조제2항> 정보주체에 대한 고지의무를 위반한 경우 3천만원 이하 과태료

3.1.5 필수동의 항목 거절/철회 시 서비스 사용이 불가하고, 선택동의 항목 동의 거절/철회 시 서비스를 정상 제공하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.1.5
중구분	개인정보 수집	**중요도**	**H**
항목 개요	서비스 제공을 위한 필수항목 수집 미 동의 시 상품·서비스 제공 자체가 어렵다는 내용을 정보주체에게 확인시켜줘야 하고, 기능상으로도 필수항목 수집 미 동의 시 서비스 사용 불가하게 구현되어야 함.		
평가기준			
판단 기준	Y - 필수항목 미 동의 시 서비스 제공이 불가하며, 선택항목 동의 거절/철회 시 서비스를 정상제공 하고 있음 N - 1) 필수항목 미 동의 시 서비스 제공이 가능하거나, 선택항목 동의 거절/철회 시 서비스를 정상제공 하지 않고 있음 2) 항목별 동의에 따른 서비스 이용 가능 여부를 고지하지 않음 N/A - 고객을 통한 직접 수집 절차 없음		
	▶ 필수항목에 대해서는 동의 거절/철회 시 서비스 실행이 불가하고, 선택항목에 대해서는 동의 거절/철회 시 해당 기능만 사용되지 않고, 기타 기능의 정상 사용 여부 확인 ▶ 필수/선택항목 동의 여부에 따른 서비스 이용가능 여부 확인		



<그림 30> 개인정보 필수 항목 미동의 관련사항 고지 예시

<table>
<tr><td></td><td> 

<그림 31> 개인정보 필수 항목 미동의 화면 예시</td></tr>
<tr><td>관련
근거</td><td>※ 개인정보보호법 <제16조> 개인정보의 수집 제한
※ 개인정보보호법 <제39조의3> 개인정보 수집·이용 동의 등에 대한 특례</td></tr>
<tr><td>과징금
및
벌칙</td><td>※ 개인정보보호법 <제16조제3항> 개인정보 수집에 동의거부로 재화 또는 서비스의 미제공한 경우 3천만원 이하 과태료
※ 개인정보보호법 <제39조제3항> 서비스의 제공을 거부한 경우 3천만원 이하 과태료</td></tr>
</table>

3.1.6 필수/선택동의 항목이 서비스 제공에 불필요한 정보를 수집하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.1.6
중구분	개인정보 수집	**중요도**	**H**
항목 개요	개인정보 수집 시 선택항목은 해당상품의 서비스 특성을 고려한 합리적인 범위내로 수집해야 함.		
평가기준			
판단 기준	Y - 수집되는 개인정보가 합리적인 범위내로 한정되어 있음 N - 수집되는 개인정보 중 불필요 항목 포함되어 있음 N/A - 고객을 통한 직접 수집 절차 없음		
점검 방법	▶ 개인정보 수집 시 개인정보 내역을 확인하고, 각 수집 항목별 사용 용도를 확인하여, 불필요 정보 유무 확인 ※ 해당 서비스의 본질적 기능을 수행하기 위해 반드시 필요한 정보 외의 정보는 수집 제한 필요. - '본질적 기능'은 사업자가 해당 서비스 제공 과정에서 업무처리를 위해 반드시 필요한 기능을 의미 ※ 최소정보의 예 - 쇼핑업체가 고객에게 상품을 배송하기 위해 수집한 이름, 주소, 전화번호(자택 및 휴대전화번호) 등은 필요 최소한의 개인정보라고 할 수 있으나, 직업, 생년월일 등 배송과 관련 없는 개인정보를 요구하는 것은 최소정보의 범위를 벗어남 - 취업 희망자의 경력, 전공, 자격증 등에 관한 정보는 업무능력을 판단하기 위한 최소한의 정보라고 할 수 있으나 가족관계, 결혼유무, 본적(원적) 등에 관한 정보는 최소정보의 범위를 벗어남		
관련 근거	※ 개인정보보호법 <제15조> 개인정보의 수집 이용 ※ 개인정보보호법 <제16조> 개인정보의 수집 제한		
과징금 및 벌칙	※ 개인정보보호법 <제15조제1항> 수집·이용 기준을 위반하여 개인정보를 수집한 경우 5천만원 이하 과태료 ※ 개인정보보호법 <제15조제2항> 정보주체에 대한 고지의무를 위반한 경우 3천만원 이하 과태료		
3.1.7 관련 법령에 의해 허용되어 주민등록번호를 사용하는 경우에는 대체 인증수단을 제공하고			

있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.1.7
중구분	개인정보 수집	**중요도**	**H**
항목 개요	정보통신서비스 제공자는 본인확인 기관이거나 법령에서 주민등록번호의 수집 · 이용을 요구하는 경우 외에 주민등록번호를 수집하지 않고 있어야 함.		
평가기준			
판단 기준	Y - 관련 법령에 의해 허용되어 주민등록번호 수집 중이고, 대체 인증수단을 제공함 N - 1) 관련 법령에 의해 허용되어 주민등록번호 수집 중이나, 대체 인증수단을 제공하지 않음 2) 관련 법령에 근거하지 않고 주민등록번호 수집 N/A - 주민등록번호 수집하고 있지 않음		

점검 방법

▶ 주민등록번호를 수집하고 있는지에 대한 여부 확인

① 주민등록번호 수집 허용 법령은 총 866개 외 수집 금지

붙임 5 주민번호 수집 · 이용 허용 법령 사례

o 아래 법령을 포함하여 기존 주민번호 수집 이용을 허용하는 법령은 총 866개
- 법률 77개, 시행령 404개, 시행규칙(서식 포함) 385개

법률	수집주체 (법 적용 대상)	사유	관련 조문	비고
금융실명거래 및 비밀보장에 관한 법률	금융회사 등 (은행, 보험회사 및 카드회사 등)	-금융거래 시 거래자의 성명 · 주민등록번호로 실지명의 확인	<법률> 제3조(금융실명거래) ① 금융회사등은 거래자의 실지명의(이하 "실명"이라 한다)로 금융거래를 하여야 한다. <시행령> 제3조(실지명의) 법 제2조제4호의 규정에 의한 실지명의는 다음 각호의 구분에 따른 명의로 한다. 1. 개인의 경우 주민등록표에 기재된 성명 및 주민등록번호. 다만, 재외국민의 경우에는 여권에 기재된 성명 및 여권번호(여권이 발급되지 아니한 재외국민은 「재외국민등록법」에 의한 등록부에 기재된 성명 및 등록번호)	거래자 (대리인 포함) 주민번호 수집
전자상거래 등에서의 소비자 보호에 관한 법률	전자상거래 사업자 (쇼핑몰 등 전자상거래 업자)	-거래 기록 및 그와 관련한 개인정보(성명 주민번호 등) 보존	<법률> 제6조(거래기록의 보존 등)①사업자는 전자상거래 및 통신판매에서의 표시·광고, 계약내용 및 그 이행 등 거래에 관한 기록을 상당한 기간 보존하여야 한다. 이 경우 소비자가 쉽게 거래기록을 열람·보존할 수 있는 방법을 제공하여야 한다. ②제1항의 규정에 의하여 사업자가 보존하여야 할 거래의 기록 및 그와 관련된 개인정보(성명·주소·주민등록번호 등 거래의 주체를 식별할 수 있는 정보에 한한다)는 소비자가 개인정보의 이용에 관한 동의를 철회하는 경우에도 정보통신망이용촉진및정보보호등에관한법률 제30조제3항의 규정에 불구하고 이를 보존할 수 있다.	거래가 이루어진 경우에 수집

※ 출처: 주민등록번호 수집 금지 제도 가이드라인

<그림 32> 주민등록번호 허용 수집법령

분야	주요 사례
회원관리	홈페이지 회원 가입, 도서·DVD 대여, 마일리지, 포인트 카드 발급

본인확인	▸성명, 주민번호를 이용한 본인확인(I-PIN, 휴대전화 등으로 대체) ▸골프장, 호텔 등 숙박시설 등 시설물 이용 출입자 기록 ▸고객센터, A/S센터 단순 상담(단, 금융거래 업무는 제외)
기타	▸입사지원 단계에 있는 근로자(채용 여부 확정시 주민번호 수집) ▸직장교육 및 협회, 단체 교육, 아파트 주차 증 발급 등 불필요한 경우

<표 1> 주민번호 수집이 금지되는 경우

※ 주민등록번호 수집 가능 경우 (정보통신망법 23조의 2 (주민등록번호의 사용제한))

1. 제23조의3에 따라 본인확인기관으로 지정 받은 경우
2. 삭제
3. 「전기통신사업법」 제38조제1항에 따라 기간통신사업자로부터 이동통신서비스 등을 제공받아 재 판매하는 전기통신사업자가 제23조의3에 따라 본인 확인기관으로 지정 받은 이동통신사업자의 본인확인업무 수행과 관련하여 이용자의 주민등록 번호를 수집·이용하는 경우

▶ 주민등록번호 수집·이용 가능 시에도 주민등록번호 대체수단 적용여부 확인

① 휴대폰, I-PIN, 범용공용인증서 인증 등 적용여부 확인

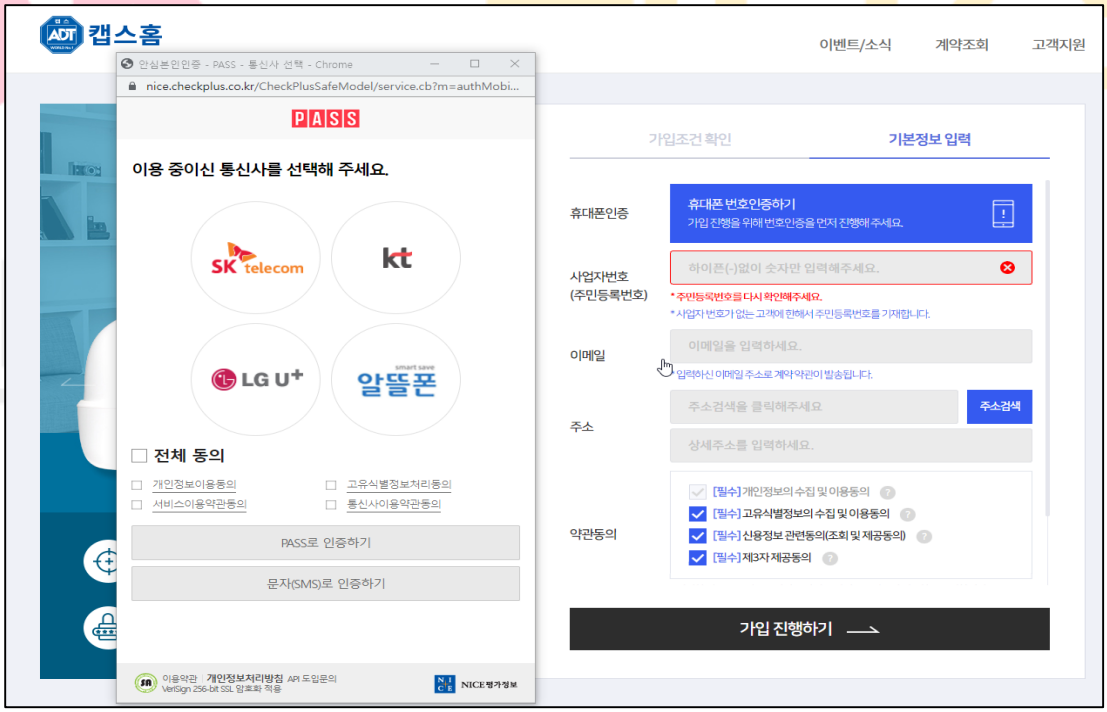
※ 출처: 한국인터넷진흥원 주민등록번호 대체수단

<그림 33> 대체인증수단 안내

관련 근거	※ 정보통신망법 <제23조의2> 주민등록번호의 사용 제한 ※ 개인정보보호법 <제24조의2> 주민등록번호 처리의 제한 ※ 개인정보보호법 시행령 <제19조> 고유식별정보의 범위 ※ 개인정보보호법 시행령 <제62조의2> 민감정보 및 고유식별정보의 처리
과징금 및 벌칙	※ 개인정보보호법 <제24조제1항> 동의를 받지 않거나 법령근거 없이 고유식별정보를 처리한 경우 5년 이하의 징역 또는 5천만원 이하의 벌금 ※ 개인정보보호법 <제24조의2제1항> 동의를 받지 않거나 법령근거 없이 고유식별정보를 처리한 3천만원 이하의 과태료

	※ 개인정보보호법 <제24조의2제3항> 정보주체가 주민등록번호를 사용하지 아니할 수 있는 방법을 제공하지 않는 경우 3천만원 이하의 과태료

3.1.8 개인정보 수집, 열람, 정정요구, 해지요청 등 요청 시 명의도용 등 이용자 피해 방지를 위한 "본인확인"을 하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.1.8
중구분	개인정보 수집	**중요도**	H
항목 개요	개인정보 열람 및 정정 요구 등의 본인의 의사 확인이 필요한 경우 본인 확인 후 정보에 접근할 수 있게 해야 함		
평가기준			
판단 기준	Y - 서명/우편/온라인/전화 등으로 본인 확인 절차 수행 N - 본인 확인 절차 없음		
점검 방법	▶ 아래의 경우 서면/우편/온라인(휴대폰, i-PIN, 공인인증서 등)/전화 등을 통해 최소한의 정보로 본인확인 진행여부 확인 ① 명의도용이 발생 가능한 서비스(과금, 금융거래 등)에 대한 가입 또는 이용 시 ② 정보주체의 권리요구(개인정보 열람 및 정정 요구, 처리정지 요구) 시 ▶ 본인확인 시 본인확인에 필요한 최소한의 정보만 요구하는지 확인		
관련	※ 개인정보보호법 <제29조> 안전조치의무		



<그림 34> 캡스 홈 본인 확인 절차

근거	※ 개인정보보호법 <제35조> 개인정보의 열람 ※ 개인정보보호법 시행령 <제41조> 개인정보의 열람절차 등
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보조치 의무를 위반한 경우 3천만원 이하 과태료

3.1.9 만 14세 미만 아동(형사미성년자)의 개인정보에 대해 수집·이용·제공 등의 동의를 받는 경우, 법정대리인의 동의를 획득하고, 최소한의 정보만 수집하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.1.9
중구분	개인정보 수집	**중요도**	**H**
항목 개요	만 14세 미만 아동으로부터 개인정보 수집·이용·제공 등 동의가 필요한 경우에 해당 아동의 법정대리인으로부터 동의를 받아야 함.		
평가기준			
판단 기준	Y - 법정대리인을 통하여 만 14세 미만의 개인정보 관련 동의를 받고, 최소한의 정보만 수집함 P - 법정대리인을 통하여 만 14세 미만의 개인정보 관련 동의를 받고 있으나, 불필요한 정보를 수집함 N - 법정대리인을 통하여 만 14세 미만의 개인정보 관련 동의를 받지 않음 N/A - 만 14세 미만 아동 개인정보 수집하지 않음		
점검 방법	▶ 만 14세 아동이 가입할 수 있는 별도의 절차 확인하고, 개인정보 수집 경로에 따라 적절한 방법의 법정대리인 동의를 할 수 있도록 해야함 ① 방통위의 가이드라인대로 생년월일을 일시적으로 입력 받아 이용자의 나이 확인을 하는 방식 ② 만 14세 미만은 가입할 수 없거나 가입이 제한됨을 밝히고 만 14세 이상임을 본인이 체크박스로 체크하도록 하는 방식		

※ 출처: 개발자 대상 개인정보 보호조치 적용 가이드

<그림 35> 만 14세 미만 회원가입 창 분리 예시

▶ 정보통신서비스 제공자는 법 제39조의3제4항에 따라 다음 각 호의 어느 하나에 해당하는 방법으로 법정대리인이 동의했는지를 확인해야 한다. (개인정보보호법 시행령 제48조의3)

▶ 정보통신서비스 제공자는 만 14세 미만의 아동에게 개인정보 처리와 관련한 사항의 고지 등을 하는 때에는 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어를 사용하여야 한다. (개인정보보호법 제39조의3)

※ 법정대리인 동의를 얻기 위한 방법 (예시)

① 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 정보통신서비스 제공자가 그 동의 표시를 확인했음을 법정대리인의 휴대전화 문자메시지로 알리는 방법

② 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 신용카드·직불카드 등의 카드정보를 제공받는 방법

③ 동의 내용을 게재한 인터넷사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 휴대전화 본인인증 등을 통하여 본인 여부를 확인하는 방법

④ 동의 내용이 적힌 서면을 법정대리인에게 직접 발급하거나, 우편 또는 팩스를 통하여 전달하고 법정대리인이 동의 내용에 대하여 서명날인 후 제출하도록 하는 방법

⑤ 동의 내용이 적힌 전자우편을 발송하고 법정대리인으로부터 동의의 의사표시가 적힌 전자우편을 전송 받는 방법

⑥ 전화를 통하여 동의 내용을 법정대리인에게 알리고 동의를 받거나 인터넷주소 등 동의

	내용을 확인할 수 있는 방법을 안내하고 재차 전화 통화를 통하여 동의를 받는 방법 ⑦ 그 밖에 제1호부터 제6호까지의 규정에 따른 방법에 준하는 방법으로 법정 대리인에게 동의 내용을 알리고 동의의 의사표시를 확인하는 방법 ※ 실사 시 사용자 테이블에 생년월일까지 확인해서 만 14세 미만 아동 가입여부 확인
관련 근거	※ 개인정보보호법 <제22조> 동의를 받는 방법 ※ 개인정보보호법 <제39조의3> 개인정보의 수집·이용 동의 등에 대한 특례 ※ 개인정보보호법 시행령 <제45조> 대리인의 범위 등 ※ 개인정보보호법 시행령 <제48조의3> 법정대리인 동의의 확인방법
과징금 및 벌칙	※ 개인정보보호법 <제22조6항> 법정대리인 동의를 받지 않은 경우 5천만원 이하 과태료

3.1.10 법정대리인의 동의에 대한 기록을 보관하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.1.10
중구분	개인정보 수집	**중요도**	**H**
항목 개요	만 14세 미만의 아동으로부터 개인정보 수집·이용·제공 등의 동의를 받으려면 법정대리인의 동의를 받아야 하고, 동의 받은 내역에 대해서는 사후에 확인이 가능할 수 있도록 별도 보관하여야 함.		
평가기준			
판단 기준	Y - 법정대리인의 동의 기록을 보관함 N - 법정대리인의 동의 기록 보관하지 않음 N/A - 만 14세 미만 아동 개인정보 수집하지 않음		
점검 방법	▶ 법정대리인 동의에 대한 기록(동의자, 동의 여부, 동의 일시 등)은 사후에 확인이 가능하도록 개인정보처리시스템 등에 기록 보관 여부 확인 ① 보존 항목: 법정 대리인 정보(이름, 연락처 등), 동의 일시 등 ② 보존 기간: 서비스 해지 또는 아동의 개인정보 파기 시점까지		
관련 근거	※ 개인정보보호법 <제22조> 동의를 받는 방법 ※ 개인정보보호법 시행령 <제45조> 대리인의 범위 등 ※ 정보보호 및 개인정보보호 관리체계 인증 <3.1.2> 개인정보의 수집 동의		
과징금 및 벌칙	※ 개인정보보호법 <제22조6항> 법정대리인 동의를 받지 않은 경우 5천만원 이하 과태료		

3.1.11 법정대리인의 동의 거부가 있거나 동의 의사가 확인되지 않은 채 수집일로부터 3일이 경과된 경우에는 즉시 파기하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.1.11
중구분	개인정보 수집	**중요도**	**H**
항목 개요	법정대리인의 동의 거부가 있거나 법정대리인의 동의 의사가 확인되지 않는 경우 수집일로부터 3일 이내에 파기해야 함.		
평가기준			
판단 기준	Y - 법정대리인의 동의 거부 및 동의 의사가 확인되지 않을 시 수집일로부터 3일 경과 후 즉시 파기함. N - 법정대리인의 동의 거부 및 동의 의사가 확인되지 않을 시 수집일로부터 3일 경과 후 즉시 파기하지 않음. N/A - 만 14세 미만 아동 개인정보 수집하지 않음.		
점검 방법	▶ 법정대리인의 동의거부, 의사 미확인 경우 5일 경과 후 즉시 파기 확인		
관련 근거	※ 개인정보보호법 <제21조> 개인정보의 파기 ※ 개인정보보호법 시행령 <제16조> 개인정보의 파기방법 ※ 개인정보 안전성 확보조치 기준 <제13조> 개인정보의 파기 ※ 표준 개인정보보호지침 <제13조> 법정대리인의 동의		
과징금 및 벌칙	※ 개인정보보호법 <제21조제1항> 개인정보가 불필요하게 되었을 때 파기하지 않은 경우 2년 이하의 징역 또는 2천만원 이하의 벌금 ※ 개인정보보호법 <제21조제1항> 개인정보의 파기 등 필요한 조치를 아니한 경우 3천만원 이하 과태료		

3.1.12 고유식별정보 및 민감정보 수집 시 해당 사항을 정보주체에게 알리고 별도의 동의를 받습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.1.12
중구분	개인정보 수집	**중요도**	**H**
항목 개요	고유식별정보 및 민감정보를 수집해야 하는 경우 개인정보 항목 / 수집·이용목적 / 보유·이용기간 / 동의를 거부할 권리에 대한 사실 등을 알리고 별도의 동의를 받아야 함.		
평가기준			
판단 기준	Y - 고유식별정보 및 민감정보 수집 시 적절한 동의를 받음 N - 고유식별정보 및 민감정보 수집 시 동의 받지 않거나, 일부 누락된 항목이 존재함 N/A - 고유식별정보 및 민감정보 수집하고 있지 않음		

점검 방법

▶ 고유식별정보 및 민감정보 수집 시 관련 법령에 근거하여 수집하고, 4가지 필수 항목에 대해 정보주체에게 고지 및 별도의 동의를 받는지 여부 확인

① 개인정보의 수집·이용 목적

② 수집하는 개인정보의 항목

③ 개인정보의 보유·이용 기간

④ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 등

분류	범위
고유식별정보	주민등록번호(법정주의 필수), 여권번호, 운전면허번호, 외국인등록번호
민감정보	사상·신념, 정치적 견해, 건강, 성생활, 유전정보, 범죄경력에 관한 정보
	개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보
	인증이나 민족에 관한 정보

<표 4> 고유식별정보 및 민감정보의 범위

아래와 같이 민감정보를 처리합니다.

항 목	수집목적	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 처리하는데 동의하십니까?

동의 ☐ 미동의 ☐

년 월 일

※ 출처: 개인정보 수집. 제공 동의서 작성 가이드라인

<그림 36> 민감정보 수집 동의

< 작성 예시 >

아래와 같이 고유식별정보를 처리합니다.

항 목	수집목적	보유·이용기간
여권번호	출입증 발급 시, 본인확인 용도	2년

※ 위와 같이 고유식별정보 처리에 동의를 거부할 권리가 있습니다.
그러나 동의를 거부할 경우 출입증 발급 및 본인확인이 제한 될 수 있습니다.
위와 같이 고유식별정보를 처리하는데 동의하십니까?

동의 ☐ 미동의 ☐

년 월 일

※ 출처: 개인정보 수집. 제공 동의서 작성 가이드라인

<그림 37> 고유식별정보 수집 동의

관련 근거	※ 개인정보보호법 <제22조> 동의를 받는 방법 ※ 개인정보보호법 <제23조> 민감정보의 처리 제한 ※ 개인정보보호법 <제24조> 고유식별정보의 처리 제한 ※ 정보통신망법 <제23조의2> 주민등록번호의 사용 제한 ※ 개인정보보호법 시행령 <제62조의2> 민감정보 및 고유식별정보의 처리
과징금 및 벌칙	※ 개인정보보호법 <제24조제1항> 동의를 받지 않거나 법령근거 없이 고유식별정보를 처리한 경우 5년 이하의 징역 또는 5천만원 이하의 벌금 ※ 개인정보보호법 <제24조제2의1항> 법령근거 없이 주민등록번호를 처리한 경우 3천만원 이하의 과태료

3.1.13 광고성 정보 전송에 대한 수신동의 여부를 매 2년마다 확인하고 관련 고지사항을 알리고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.1.13
중구분	개인정보 수집	**중요도**	H
항목 개요	광고성 정보를 전송할 경우 수신자에게 수신동의 여부를 확인하여야 함		
평가기준			
판단 기준	Y - 광고성 정보 전송 시 별도 동의를 받으며, 수신동의 여부를 매 2년마다 확인하고, 관련사항을 고지하고 있음 P - 광고성 정보 전송 시 별도 동의를 받거나, 관련사항 고지를 일부 시행하고 있음 N - 광고성 정보 전송 시 별도 동의절차가 없거나, 수신동의 여부를 매 2년마다 확인하지 않거나, 관련사항을 고지하지 않음 N/A - 직접 마케팅 활동 없음		
점검 방법	▶ 홍보, 판매 권유 등의 직접마케팅을 하는 경우, 정보주체가 이를 명확하게 인지할 수 있도록 알리고 별도의 동의를 받으며, 매 2년 마다 수신동의 여부를 확인하고 아래의 사항을 알리고 있는지 확인 ① 전송자의 명칭 ② 수신자의 수신동의 사실과 수신에 동의한 날짜 ③ 수신동의에 대한 유지 또는 철회의 의사를 표시하는 방법  ※ 출처: 불법스팸 방지 안내서 **<그림 38> 정기적 광고 수신 동의 안내 예시** ※ '정보통신망법 시행령 제62조의3(수신동의 여부의 확인), 2014.11.28' 기준 시행일자 이후 2년 경과된 서비스에 해당함		

	※ 마케팅 사전 동의 예외 ① 재화 등 거래관계를 통하여 직접 연락처를 수집한지 6개월 이내에 동종의 재화 구매에 대하여 영리목적의 광고성 정보를 전송하는 경우 ② 전화권유판매업자로 등록된 자가 육성으로 개인정보 수집 출처를 고지하고 전화권유를 하는 경우 - 단, 수신자가 수신거부의사를 표시할 경우, 전송 불가함
관련 근거	※ 개인정보보호법 <제22조> 동의를 받는 방법 ※ 개인정보보호법 <제26조> 업무위탁에 따른 개인정보 처리 제한 ※ 정보통신망법 <제50조> 영리목적의 광고성 정보 전송 제한 ※ 정보통신망법 시행령 <제62조의3> 수신동의 여부의 확인 ※ 정보통신망법 시행령 <제62조의3> 수신동의 여부의 확인
과징금 및 벌칙	※ 정보통신망법 <제50조> 영리목적의 광고성 정보 수신동의를 확인하지 않은 경우 3천만원 이하의 과태료

3.1.14 광고성 정보 전송에 대한 수신동의/거부/동의 철회 시 수신자에게 처리결과를 알리고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.1.14
중구분	개인정보 수집	**중요도**	H
항목 개요	광고성 정보 전송에 대한 수신동의/거부/동의 철회 시 수신자에게 처리결과를 고지하여야 함		
평가기준			
판단 기준	Y - 광고성 정보 전송에 대한 수신동의/거부/동의 철회 내역을 수신자에게 고지함 N - 광고성 정보 전송에 대한 수신동의/거부/동의 철회 내역을 수신자에게 미 고지함 N/A - 직접 마케팅 활동 없음		
점검 방법	▶ 광고성 정보 전송에 대한 수신동의/거부/동의 철회 시 수신자에게 처리결과 고지 확인 ① Web/App/Mobile Web 등에서 실제 광고성 정보 전송에 대해 수신동의/철회하여 처리결과를 14일이내에 안내하는지 확인 1) 전송자의 명칭 2) 수신동의, 수신거부 또는 수신동의 철회 사실과 해당 의사를 표시한 날짜 3) 처리결과 ② 광고성 수신동의 철회 시 실제 철회 처리되어 광고 전송 대상에서 제외처리여부 확인		
관련	※ 정보통신망법 <제50조> 영리목적의 광고성 정보 전송 제한		

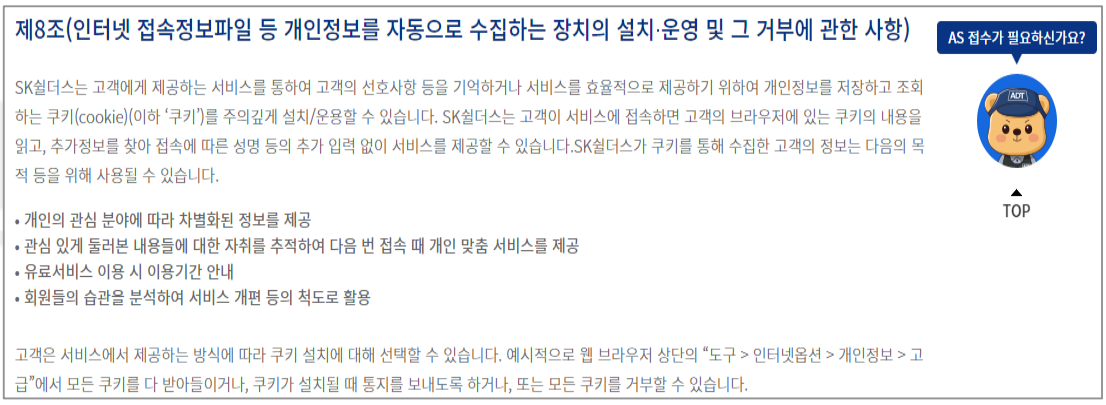
※ 출처: 불법스팸 방지 안내서

<그림 39> 수신동의/거부/동의 철회 처리결과 예시

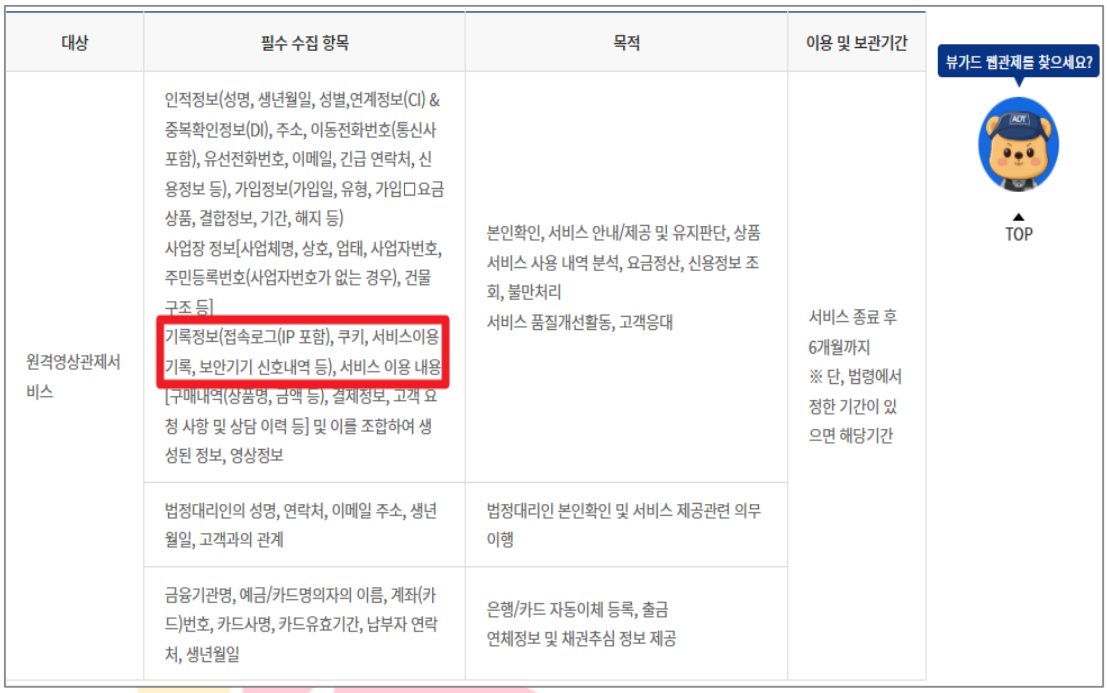
근거	※ 정보통신망법 시행령 <제62조의2> 수신동의 등 처리결과의 통지
과징금 및 벌칙	※ 정보통신망법 <제50조> 영리목적의 광고성 정보 수신동의를 확인하지 않은 경우 3천만원 이하의 과태료

3.1.15 영리목적의 광고성 정보를 전송하는 경우 야간시간에는 전송하지 않도록 하고 있는가?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.1.15
중구분	개인정보 수집	**중요도**	**H**
항목 개요	광고성 정보 전송에 대한 수신동의/거부/동의 철회 시 수신자에게 처리결과를 고지하여야 함		
평가기준			
판단 기준	Y - 광고성 정보 전송에 대한 수신동의/거부/동의 철회 내역을 수신자에게 고지함 N - 광고성 정보 전송에 대한 수신동의/거부/동의 철회 내역을 수신자에게 미 고지함 N/A - 직접 마케팅 활동 없음		
점검 방법	▶ 영리성 목적의 광고 야간 전송 제한 확인 ① 야간시간(오후 9시 ~ 익일 오전 8시)에 광고성 정보 전송여부 확인 - MMS, App Push, Mail 등 정보주체에게 유/무선으로 전달하는 방식 모두 포함 ② 시간대를 지정하여 전송하고 있는지 확인 ③ 야간시간 전송에 대한 별도의 동의를 받고 있는지 확인		
관련 근거	※ 정보통신망법 <제50조> 영리목적의 광고성 정보 전송 제한		
과징금 및 벌칙	※ 정보통신망법 <제50조> 영리목적의 광고성 정보 수신동의를 확인하지 않은 경우 3천만원 이하의 과태료		

3.1.16 자동수집장치 등에 의해 수집·생성하는 개인정보(이용내역 등)의 경우에도 최소수집 원칙을 적용하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.1.16
중구분	개인정보 수집	**중요도**	**H**
항목 개요	자동 수집 정보의 경우 해당 서비스의 계약 이행 및 제공을 위해 필요한 최소한의 개인정보만 수집하여야 함.		
평가기준			
판단 기준	Y - 자동수집 개인정보 최소 수집 또는 정보주체의 동의를 취득하여 수집하고 있음 N - 자동수집 개인정보 최소 수집 또는 정보주체의 동의를 받지 않음 N/A - 자동수집 정보가 없음		
점검 방법	▶ 서비스 계약 이행을 위해 필요한 경우로서 사업자가 서비스 제공과정에서 자동수집장치 등에 의해 수집·생성되는 개인정보(통화기록, 접속로그, 결제기록, 이용내역 등)에 대해서도, 해당 서비스의 계약 이행 및 제공을 위해 필요한 최소한의 개인정보만을 하는지 확인 다만, 서비스 제공 계약 이행과는 무관한 목적으로 이용하기 위해 수집하는 경우에는 선택 동의 항목으로 분류하여 별도의 사전 동의를 받아야 함		



<그림 40> 개인정보 자동수집 및 거부 절차

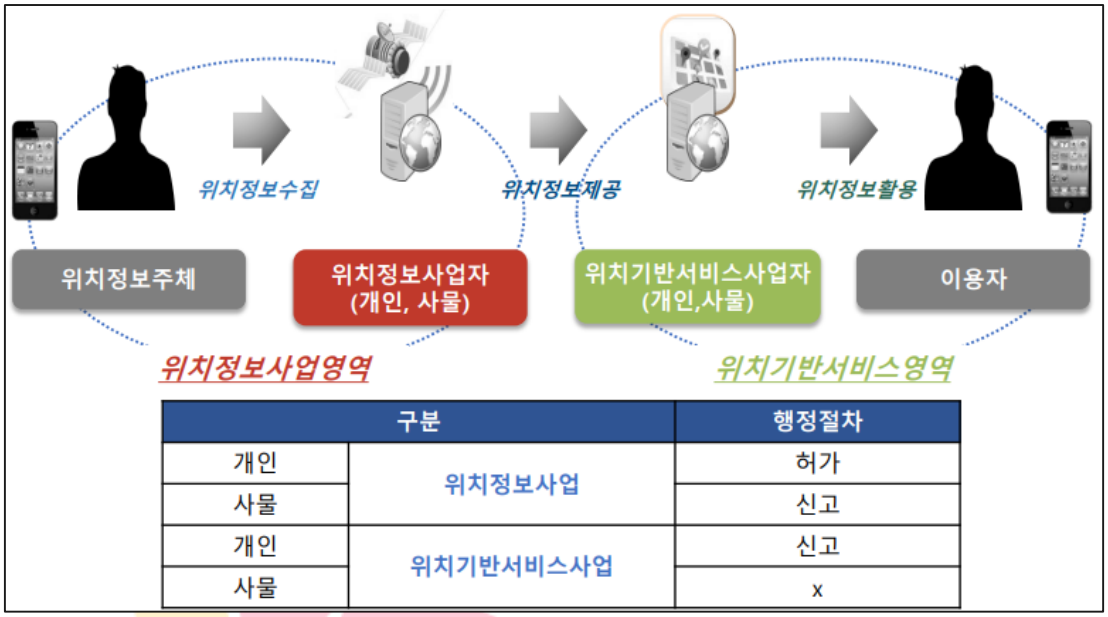
<table>
<tr><td></td><td>


<그림 41> 자동수집 정보 동의항목
</td></tr>
<tr><td>관련 근거</td><td>※ 개인정보보호법 <제16조> 개인정보의 수집 제한
※ 개인정보보호법 <제39조의3> 개인정보 수집·이용 동의 등에 대한 특례</td></tr>
<tr><td>과징금 및 벌칙</td><td>※ 개인정보보호법 <제16조제3항> 개인정보 수집에 동의거부로 재화 또는 서비스의 미제공한 경우 3천만원 이하 과태료
※ 개인정보보호법 <제39조제3항> 서비스의 제공을 거부한 경우 3천만원 이하 과태료</td></tr>
</table>

3.1.17 개인위치정보 수집 시 정보주체 또는 위치정보 수집 장치 소유자에 대해 사전고지와 명시적 동의를 거치도록 계획하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.1.17
중구분	개인정보 수집	**중요도**	H
항목 개요	위치정보사업자 허가 또는 위치기반 서비스사업자의 신고대상자가 위치정보 수집 시 정보주체에 수집에 관한 이용약관명시와 동의를 받아야함.		
평가기준			
판단 기준	Y - 위치정보 수집에 대한 이용약관명시와 동의를 받고 있음 N - 위치정보 수집에 대한 이용약관명시와 동의를 받지 않음 N/A - 위치정보를 취급하지 않음		
점검 방법	▶ 위치정보 수집의 경우 정보 주체의 요구되는 동의사항을 알리고 동의 받고 있는지 확인. ① 위치정보사업자의 상호, 주소, 전화번호 그 밖의 연락처 ② 개인위치정보주체 또는 법정대리인의 권리와 그 행사방법 ③ 위치정보사업자가 위치기반서비스사업자에게 제공하고자 하는 서비스의 내용 ④ 위치정보 수집사실 확인 자료의 보유근거 및 보유기간 개인위치정보의 수집방법		

<그림 42> 위치정보 이용약관 사항

▶ 개인위치정보를 수집하는 경우에는 위치정보사업자 허가 또는 위치기반서비스사업자

<table>
<tr><td></td><td>신고 대상인지 사전에 검토하여 필요시 허가 또는 신고 사실 확인
 

<table>
<tr><th colspan="2">구분</th><th>행정절차</th></tr>
<tr><td>개인</td><td rowspan="2">위치정보사업</td><td>허가</td></tr>
<tr><td>사물</td><td>신고</td></tr>
<tr><td>개인</td><td rowspan="2">위치기반서비스사업</td><td>신고</td></tr>
<tr><td>사물</td><td>x</td></tr>
</table>
※ 출처: 방송통신위원회 사업자 대상 위치정보보호 교육자료
<그림 43> 위치정보 수집 신고 허가</td></tr>
<tr><td>관련 근거</td><td>※ 위치정보보호 및 이용 등에 관한법률 <제39조3호> 개인위치정보의 수집 이용 시 동의</td></tr>
<tr><td>과징금 및 벌칙</td><td>※ 위치정보보호 및 이용 등에 관한법률 <제39조3호> 동의를 받지 않고 사용 시 5년 이하의 징역 또는 5천만원 이하의 벌금</td></tr>
</table>

3.2. 개인정보 보유

3.2.1 개인정보의 보유기간을 법령 기준 및 보유목적에 부합된 최소한의 기간으로 산정하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.2.1
중구분	개인정보 보유	**중요도**	**H**
항목 개요	개인정보를 보유하려는 경우에는 관련 법적 기준 및 보유 목적에 부합된 최소의 기간으로 보유기간을 산정하여야 함.		
평가기준			
판단 기준	Y - 개인정보의 보유기간에 대해 관련 법령기준을 따름 N - 개인정보의 보유기간에 대해 관련 법령기준을 따르지 않음		
점검 방법	▶ 개인정보의 보유기간은 관련 법령기준 및 보유목적에 부합된 최소 기간으로 산정여부 확인 (아래 관련 법령 예시 참조) ※ 아래 관련 법령 예시 참조 - 통신비밀보호법 제15조의2에 의하여 통신사실확인자료 제공 시 필요한 발·착신 통신번호 등 상대방의 가입자번호, 사용 도수: 12개월 - 통신비밀보호법에 따라 로그기록자료, 접속지의 추적자료: 3개월 - 전자상거래 등에서의 소비자보호에 관한 법률, 국세기본법, 부가가치세법에 따른 성명, 주민등록번호, (해지)연락처, 주소, 계약/해지 등에 관한 기록, 요금 등 거래내역 관련 정보: 5년 - 상법 제33조에 따라 상업장부와 영업에 관한 중요 서류는 10년, 전표 등: 5년 - 전자상거래 등에서의 소비자보호에 관한 법률 제6조(거래기록의 보존 등)에 따른 표시, 광고에 관한 기록: 6개월, 불만 또는 분쟁처리에 관한 기록: 3년 - 보유기간을 고객에게 미리 고지하고 그 보유기간이 경과하지 아니한 경우와 개별적으로 고객의 동의를 받을 경우에는 약속한 보유 기간 - 기타 법령이 정하는 기간		
관련 근거	※ 개인정보보호법 <제21조> 개인정보의 파기 ※ 개인정보보호법 시행령 <제16조> 개인정보의 파기방법 ※ 개인정보의 안전성 확보조치 기준 <제13조> 개인정보의 파기		
과징금 및 벌칙	※ 개인정보보호법 <제21조제1항> 개인정보가 불필요하게 되었을 때 파기하지 않은 경우 2년 이하의 징역 또는 2천만원 이하의 벌금 ※ 개인정보보호법 <제21조제1항> 개인정보의 파기 등 필요한 조치를 아니한 경우		

	3천만원 이하 과태료

3.3. 개인정보 이용·제공

3.3.1 개인정보의 제3자 제공 또는 목적 외 시 필요한 보호절차(고지, 동의, 제공 항목 최소화 등)를 모두 이행하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.3.1
중구분	개인정보 이용·제공	**중요도**	**H**
항목 개요	개인정보의 제3자 제공 또는 목적 외 제공 시 필요한 보호절차(고지, 동의, 제공 항목 최소화 등)를 준수해야 함		
평가기준			
판단 기준	Y - 개인정보 제3자 제공 또는 목적 외 제공 시 필요한 보호절차를 모두 이행하고 있음 N - 개인정보 제3자 제공 또는 목적 외 제공 시 필요한 보호절차를 미 이행하고 있음 N/A - 개인정보를 제3자에게 또는 목적 외 제공 제공하고 있지 않음		
점검 방법	▶ 개인정보 제3자 제공 또는 목적 외 제공 시, 다음 보호절차 준수 확인 ① 수집, 이용에 대한 동의와 별도 구분 동의 여부 ② 관련 사항 고지 여부 - 개인정보를 제공받는 자 - 개인정보를 제공받는 자의 개인정보 이용 목적 - 제공하는 개인정보의 항목 - 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 - 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용		

제3조(개인정보의 제3자 제공)

① SK쉴더스는 원칙적으로 고객의 개인정보를 제1조에서 명시한 목적 범위 내에서 처리하며, 고객의 사전 동의 없이는 본래의 범위를 초과하여 처리하거나 제3자에게 제공하지 않습니다. 단, 다음의 각 호의 경우에는 고객 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있습니다.

1. 고객이 사전에 제3자 제공 및 공개에 동의한 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 고객 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 고객 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우

② SK쉴더스는 제1항 제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 고객에게 알립니다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 고객에게 알리고 동의를 받습니다.

1. 개인정보를 제공받는 자
2. 개인정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적을 말한다)
3. 이용 또는 제공하는 개인정보의 항목
4. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ SK쉴더스는 다음과 같이 개인정보를 제공하고 있습니다. 향후 업체 및 업무의 내용이 변경된 경우 지체 없이 본 방침을 통해 고지하겠습니다.

1. 필수적 제공

대상	제공받는 자	제공받는 자의 이용 목적	제공하는 개인정보 항목	제공받는 자의 보유 및 이용 기간
경비서비스 (뷰가드포함) 원격영상관제서비스	효성에프엠에스㈜	즉시인출	**예금주명, 금융기관명,** 생년월일, 사업자번호, 계좌번호	미수완료 시 삭제
	금융결제원	자동이체 신청	**예금주명, 금융기관명,** 생년월일, 사업자번호, 계좌번호	자동이체 해지 시 삭제
	㈜엘지유플러스, NICE페이먼츠㈜	카드 자동결제 처리	**카드사명, 카드번호,** 카드유효기간, 카드명의자의 이름, 생년월일	카드 자동결제 해제시까지
	나이스평가정보	신용정보조회, 채권불이행 등재(해당시만)	성명, 핸드폰번호, 생년월일	미수완료시 삭제
	메리츠화재	보험가입 및 보험금 지급	**주소, 이름연락처**	보험접수 및 처리기간
	DB손해보험	보험가입 및 보험금 지급	**주소, 이름연락처**	보험접수 및 처리기간
	㈜마쉬코리아손해보험중재	보험가입 및 보험금 지급	**주소, 이름연락처**	보험접수 및 처리기간
	KB손해보험㈜	보험가입 및 보험금 지급	**주소, 이름연락처**	보험접수 및 처리기간
	한화손해보험㈜	보험가입 및 보험금 지급	**주소, 이름연락처**	보험접수 및 처리기간

<그림 44> 제3자 제공 시 고지 예시

③ 목적에 맞는 최소한의 항목으로 제한되고 이외 용도로 사용 불가
④ 제공 항목 및 제공 내역 기록

관련 근거	※ 개인정보보호법 <제17조> 개인정보의 제공 ※ 개인정보보호법 <제18조> 개인정보 목적 외 이용 제공 제한 ※ SK 개인정보보호 Policy & Guideline 3.13
과징금 및 벌칙	※ 개인정보보호법 <제18조의3항> 제3자 제공을 알리지 않은 경우 3천만원 이하의 과태료

3.3.2 이용내역을 연 1회 이상 통지하고 있습니까? (대상 : B2C 서비스)

항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.3.2
중구분	개인정보 이용·제공	**중요도**	**H**
항목 개요	전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자는 개인정보 이용내역을 연 1회 이상 통지해야 함		
평가기준			
판단 기준	Y - 개인정보 이용내역을 적합한 방법으로 연 1회 통지하고 있음 N - 개인정보 이용내역을 적합한 방법으로 연 1회 통지하고 있지 않음 N/A - B2C 서비스이나, Open한지 1년이내일 경우		
점검 방법	▶ 개인정보 이용내역을 연 1회 이상 전자우편·서면·모사전송·전화 또는 이와 유사한 방법을 통하여 통지하는지 확인 ① 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목 ② 개인정보를 제공받은 자, 그 제공 목적 및 제공한 개인정보의 항목 ③ 개인정보를 취급위탁 받은 자 및 그 처리위탁을 하는 업무의 내용		

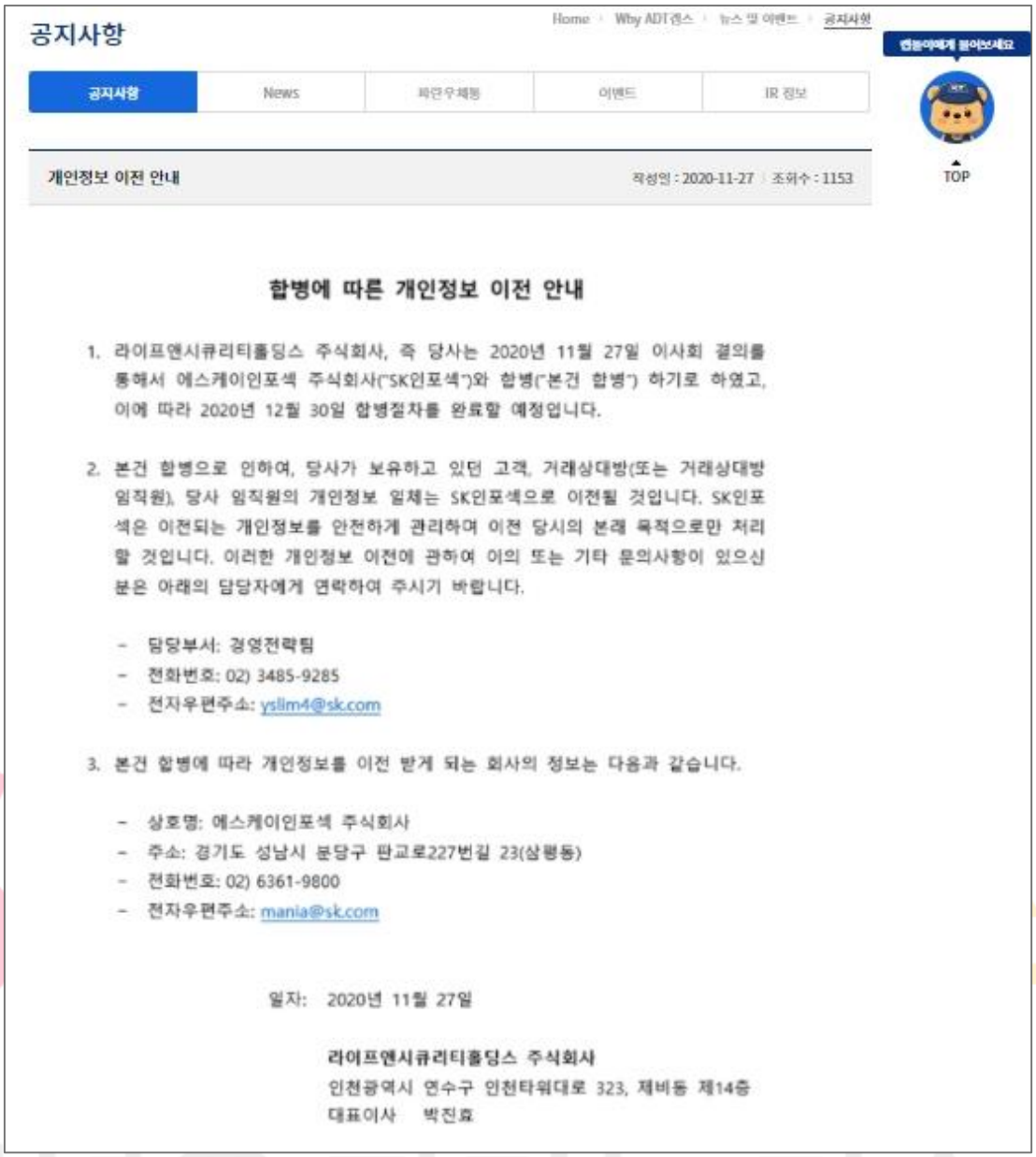
<table>
<tr>
<td></td>
<td>


※ 출처: SK ICT패밀리 가입화면
<그림 45> 개인정보 이용내역 통지 예시
</td>
</tr>
<tr>
<td>관련 근거</td>
<td>※ 개인정보보호법 <제39조의8> 개인정보 이용내역의 통지
※ 개인정보보호법 시행령 <제15조의2> 개인정보 수집 출처 등 고지 대상·방법·절차
※ 개인정보보호법 시행령 <제48조의6> 개인정보 이용내역의 통지</td>
</tr>
<tr>
<td>과징금 및 벌칙</td>
<td>※ 개인정보보호법 <제39조의8제1항> 개인정보 이용내역을 통지하지 않은 경우 3천만원 이하의 과태료</td>
</tr>
</table>

3.3.3 개인정보를 국외에 이전(제공·조회·처리위탁·보관)할 경우(국외 클라우드 포함), 정보주체에게 동의 받거나 공개하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.3.3
중구분	개인정보 이용·제공	**중요도**	**H**
항목 개요	이용자의 개인정보를 국외에 제공·처리위탁·보관하려면 이용자의 동의를 받아야 한다. 다만 국외이전 관련 한 법률 요구사항을 개인정보 처리방침 등으로 이용자에게 알린 경우에는 개인정보 처리위탁·보관에 따른 동의절차를 거치지 않을 수 있다		
평가기준			
판단 기준	Y - 개인정보 국외 이전에 대한 사항을 동의 받거나 개인정보 처리방침 등에 고지하고 있음 N - 개인정보 국외 이전에 대한 사항을 동의 받지 않고, 개인정보 처리방침에도 고지하지 않음 N/A - 개인정보 국외이전 없음		
점검 방법	▶개인정보 국외 이전 시 동의/공개 여부 확인 ① 개인정보 국외 이전 시 동의 여부 확인 1. 이전되는 개인정보 항목 2. 개인정보가 이전되는 국가, 이전일시 및 이전방법 3. 개인정보를 이전 받는 자의 성명 4. 개인정보를 이전 받는 자의 개인정보 이용목적 및 보유·이용 기간 ② WEB/APP 회원가입화면, 회원가입신청서, 개인정보수집동의서 등 관련 서식 내 내용 상세 확인 - 개인정보 처리방침 내 국외 처리에 관한 내용 확인 - 국외 이전 사실을 전자우편, 서면, 모사전송, 전화 등으로 고지하였는지 확인 ③ 국외 이전 개인정보에 대한 사항을 개인정보 처리방침에 공개하였을 경우 동의 절차를 거치지 않을 수 있음 - 단, 해외 지점/법인 등에 3자 제공 형태로 개인정보를 이전/제공하는 경우에는 동의를 받아야 함 ※ 국외 처리 사업자와 계약 시 아래 사항을 포함해야 함. 1. 개인정보보호를 위한 기술적, 관리적 조치 2. 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 사항 3. 그 밖에 이용자의 개인정보 보호를 위하여 필요한 조치		
관련 근거	※ 개인정보보호법 <제39조의12> 국외 이전 개인정보의 보호 ※ 개인정보보호법 시행령 <제48조의10> 개인정보 국외 이전 시 보호조치		

과징금 및 벌칙	※ 개인정보보호법 <제12조제3항> 이전 사실을 이용자에게 알리지 않은 경우 2천만원 이하의 과태료

3.3.4 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우 필요한 사항을 사전에 정보주체(이용자)에게 알리고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.3.4
중구분	개인정보 이용·제공	**중요도**	**H**
항목 개요	영업의 전부 또는 일부의 양도, 합병 등으로 개인정보를 다른 사람에게 이전하는 경우 다음의 사항을 사전에 정보주체(이용자)에게 알리고 있는지 확인		
평가기준			
판단 기준	Y - 양도·합병 등 정보주체(이용자)에게 알리고 있음 N - 양도·합병 등 정보주체(이용자)에게 알리고 있지 않음 N/A - 개인정보 양도·합병 등 사실이 없음		
점검 방법	▶ 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우 다음의 사항을 사전에 정보주체(이용자)에게 알리고 있는지 확인 ① 알려야 할 사항 - 개인정보를 이전하려는 사실 - 개인정보를 이전 받는 자의 성명, 주소, 전화번호 및 그 밖의 연락처 - 이용자가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차 ② 알리는 방법 - 전자우편, 서면, 모사전송, 전화 또는 이와 유사한 방법 중 어느 하나의 방법 - 과실 없이 정보주체(이용자)의 연락처를 알 수 없는 등의 이유로 정보주체에게 직접 알릴 수 없는 경우에는 인터넷 홈페이지에 30일 이상 기재 (단, 인터넷 홈페이지를 운영하지 않는 양도자 등의 경우 사업장 등의 보기 쉬운 장소에 30일 이상 게시 또는 전국을 보급지역으로 하는 둘 이상의 일반일간신문에 1회 이상 공고 등의 방법 이용)		



공지사항

Home > Why ADT캡스 > 뉴스 및 이벤트 > 공지사항

공지사항 | News | 피싱우체통 | 이벤트 | IR 정보

TOP

개인정보 이전 안내 작성일 : 2020-11-27 | 조회수 : 1153

합병에 따른 개인정보 이전 안내

1. 라이프앤시큐리티홀딩스 주식회사, 즉 당사는 2020년 11월 27일 이사회 결의를 통해서 에스케이인포섹 주식회사("SK인포섹")와 합병("본건 합병") 하기로 하였고, 이에 따라 2020년 12월 30일 합병절차를 완료할 예정입니다.

2. 본건 합병으로 인하여, 당사가 보유하고 있던 고객, 거래상대방(또는 거래상대방 임직원), 당사 임직원의 개인정보 일체는 SK인포섹으로 이전될 것입니다. SK인포섹은 이전되는 개인정보를 안전하게 관리하여 이전 당시의 본래 목적으로만 처리할 것입니다. 이러한 개인정보 이전에 관하여 이의 또는 기타 문의사항이 있으신 분은 아래의 담당자에게 연락하여 주시기 바랍니다.

   - 담당부서: 경영전략팀
   - 전화번호: 02) 3485-9285
   - 전자우편주소: yslim4@sk.com

3. 본건 합병에 따라 개인정보를 이전 받게 되는 회사의 정보는 다음과 같습니다.

   - 상호명: 에스케이인포섹 주식회사
   - 주소: 경기도 성남시 분당구 판교로227번길 23(삼평동)
   - 전화번호: 02) 6361-9800
   - 전자우편주소: mania@sk.com

일자: 2020년 11월 27일

라이프앤시큐리티홀딩스 주식회사
인천광역시 연수구 인천타워대로 323, 제비동 제14층
대표이사 박진효

<그림 46> 합병에 따른 개인정보 이전 안내문

관련 근거	※ 개인정보보호법 <제39조의12> 국외 이전 개인정보의 보호 ※ 개인정보보호법 시행령 <제48조의10> 개인정보 국외 이전 시 보호조치
과징금 및 벌칙	※ 개인정보보호법 <제12조제3항> 이전 사실을 이용자에게 알리지 않은 경우 2천만원 하의 과태료

3.4. 개인정보 위탁

3.4.1 개인정보 처리에 관한 업무 위탁 시 위탁하는 업무의 내용, 수탁자 등의 사항을 정보주체에게 공개 또는 통지하고 있습니까?

항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.4.1
중구분	개인정보 위탁	**중요도**	**H**
항목 개요	개인정보의 처리업무를 위탁하는 경우 관련 사항을 정보주체가 확인할 수 있도록 해야 함		

평가기준	
판단 기준	Y - 업무 위탁 시 내용, 수탁자 사항 공개하고 홍보/판매 관련 위탁 시 명시적으로 알림 N - 업무 위탁 시 내용, 수탁자 사항 미 공개하고 홍보/판매 관련 위탁 시 별도 알리지 않음 N/A - 개인정보 위탁 없음
점검 방법	▶ 개인정보의 처리업무를 제3자에게 위탁하는 경우, 관련 사항을 정보주체가 쉽게 확인할 수 있도록 '개인정보 처리방침' 등을 통해 지속적으로 공개해야 함 ① 위탁하는 업무의 내용 ② 개인정보 처리업무를 위탁 받아 처리하는 자(수탁자) ※ 모든 수탁자가 빠짐없이 공개되어야 함

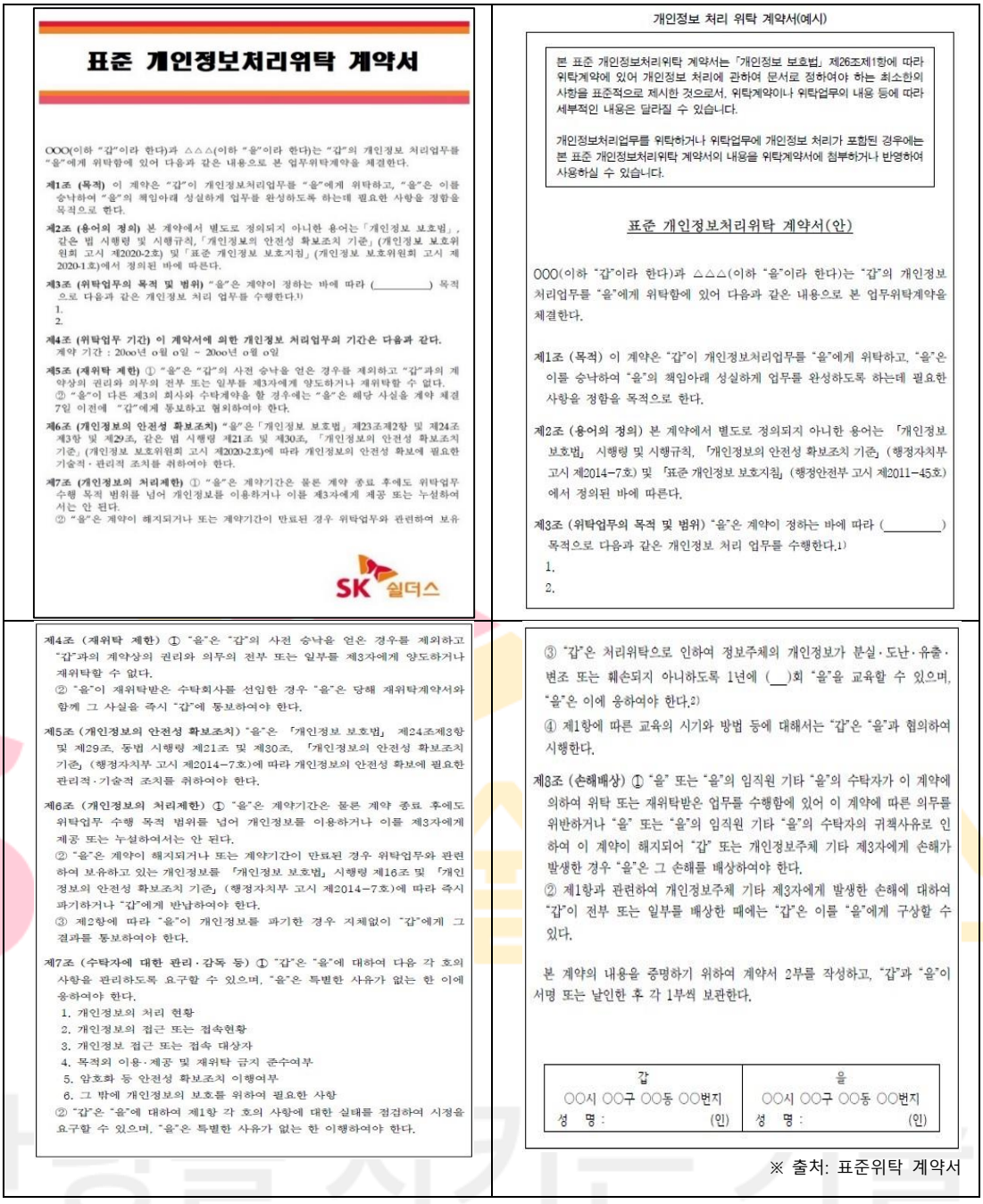
제4조(수집한 개인정보의 처리위탁)

① ADT캡스는 다음과 같이 개인정보 처리업무를 위탁하고 있습니다. 향후 수탁업체 및 위탁하는 업무의 내용이 변경될 경우 지체 없이 본 방침을 통해 고지하겠습니다.

대상	위탁업체	위탁하는 업무의 내용
홈페이지 채팅상담	(주)트라이패스	채팅상담솔루션제공 및 유지보수
	㈜엘지유플러스	카드이체 수금
	효성티앤에스주식회사	전자세금계산서 발행
	엠지신용정보㈜	수납활동
	미래신용정보	채권추심
	고려신용정보	채권추심
	엠엔와이즈	서비스 관련메일 발송
	빌포스트	DM 발송
	트라이패스	고객 대상, 당사 소식지 전달의 목적
	11번가(주)	기프티콘 발송 대행
	유비퍼스트대원	서비스제공을 위한 기기설치 및 관리

	② ADT캡스는 수탁업체와의 위탁계약 체결 시 관련 법령에 따라 위탁업무 수행목적 외 개인정보 처리금지, 기술적·관리적·물리적 보호조치, 위탁업무의 목적 및 범위, 재위탁 제한, 개인정보에 대한 접근제한 등 안전성 확보 조치에 관한 사항, 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항, 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항을 계약서 등 문서에 명시하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하고 있습니다. **<그림 47> 개인정보 처리위탁 시 고지 예시** ▶ 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 정보주체에게 관련 사항을 명시적으로 알려야 함
관련 근거	※ 개인정보보호법 <제26조> 업무위탁에 따른 개인정보의 처리 제한 ※ 개인정보보호법 시행령 <제28조> 개인정보의 처리 업무 위탁 시 조치
과징금 및 벌칙	※ 개인정보보호법 <제26조제1항> 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서에 의하지 않은 경우 1천만원 이하 과태료

3.4.2 개인정보 처리에 관한 업무 위탁 시 개인정보 관리에 관한 책임사항 등이 포함된 문서를 작성하도록 계획하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.4.2
중구분	개인정보 위탁	**중요도**	**H**
항목 개요	개인정보의 처리업무를 위탁하는 경우 책임사항이 포함된 위탁계약서를 작성해야 함		
평가기준			
판단 기준	Y - 개인정보 위탁계약서의 책임사항이 포함된 위탁 계약서를 작성하고 있음. P - 개인정보 위탁계약서의 책임사항이 일부 누락된 위탁 계약서를 작성하고 있음. N - 개인정보 위탁계약서를 작성하지 않음 N/A - 개인정보 제3자 위탁 없음		
점검 방법	▶ 개인정보의 처리업무를 제3자에게 위탁하는 경우, 아래사항이 포함된 위탁계약서를 작성해야 한다. ① 위탁 계약서에 포함되어야 할 상세 내역 1. 위탁업무 수행 목적 외 개인정보 처리 금지에 관한사항 2. 개인정보의 기술적 관리적 보호조치에 관한사항 3. 위탁업무의 목적 및 범위 4. 재 위탁 제한에 관한 사항 5. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한사항 6. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한사항 7. 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한사항		



표준 개인정보처리위탁 계약서

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)

1.
2.

제4조 (위탁업무 기간) 이 계약서에 의한 개인정보 처리업무의 기간은 다음과 같다.

계약 기간 : 20oo년 o월 o일 ~ 20oo년 o월 o일

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.

제6조 (개인정보의 안전성 확보조치) "을"은 「개인정보 보호법」 제23조제2항 및 제24조 제3항 및 제29조, 같은 법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(개인정보 보호위원회 고시 제2020-2호)에 따라 개인정보의 안전성 확보에 필요한 기술적·관리적 조치를 취하여야 한다.

제7조 (개인정보의 처리제한) ① "을"은 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

② "을"은 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유

SK 쉴더스

개인정보 처리 위탁 계약서(예시)

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.

개인정보처리업무를 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」 시행령 및 시행규칙, 「개인정보의 안전성 확보조치 기준」(행정자치부 고시 제2014-7호) 및 「표준 개인정보 보호지침」(행정안전부 고시 제2011-45호)에서 정의된 바에 따른다.

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

1.
2.

제4조 (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 재위탁받은 수탁회사를 선임한 경우 "을"은 당해 재위탁계약서와 함께 그 사실을 즉시 "갑"에 통보하여야 한다.

제5조 (개인정보의 안전성 확보조치) "을"은 「개인정보 보호법」 제24조제3항 및 제29조, 동법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(행정자치부 고시 제2014-7호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제6조 (개인정보의 처리제한) ① "을"은 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.

② "을"은 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보 보호법」 시행령 제16조 및 「개인정보의 안전성 확보조치 기준」(행정자치부 고시 제2014-7호)에 따라 즉시 파기하거나 "갑"에게 반납하여야 한다.

③ 제2항에 따라 "을"이 개인정보를 파기한 경우 지체없이 "갑"에게 그 결과를 통보하여야 한다.

제7조 (수탁자에 대한 관리·감독 등) ① "갑"은 "을"에 대하여 다음 각 호의 사항을 관리하도록 요구할 수 있으며, "을"은 특별한 사유가 없는 한 이에 응하여야 한다.

1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속현황
3. 개인정보 접근 또는 접속 대상자
4. 목적외 이용·제공 및 재위탁 금지 준수여부
5. 암호화 등 안전성 확보조치 이행여부
6. 그 밖에 개인정보의 보호를 위하여 필요한 사항

② "갑"은 "을"에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, "을"은 특별한 사유가 없는 한 이행하여야 한다.

③ "갑"은 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 (__)회 "을"을 교육할 수 있으며, "을"은 이에 응하여야 한다.2)

④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 "갑"은 "을"과 협의하여 시행한다.

제8조 (손해배상) ① "을" 또는 "을"의 임직원 기타 "을"의 수탁자가 이 계약에 의하여 위탁 또는 재위탁받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 "을" 또는 "을"의 임직원 기타 "을"의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 "갑" 또는 개인정보주체 기타 제3자에게 손해가 발생한 경우 "을"은 그 손해를 배상하여야 한다.

② 제1항과 관련하여 개인정보주체 기타 제3자에게 발생한 손해에 대하여 "갑"이 전부 또는 일부를 배상한 때에는 "갑"은 이를 "을"에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, "갑"과 "을"이 서명 또는 날인한 후 각 1부씩 보관한다.

갑	을
OO시 OO구 OO동 OO번지	OO시 OO구 OO동 OO번지
성 명 : (인)	성 명 : (인)

※ 출처: 표준위탁 계약서

<그림 48> 개인정보처리위탁 계약서

관련 근거	※ 개인정보보호법 <제26조> 업무위탁에 따른 개인정보의 처리 제한 ※ 개인정보보호법 시행령 <제28조> 개인정보의 처리 업무 위탁 시 조치
과징금 및 벌칙	※ 개인정보보호법 <제26조제1항> 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서에 의하지 않은 경우 1천만원 이하 과태료

3.5. 개인정보 파기

3.5.1 데이터베이스에 저장된 정보에 대해 파기사유 발생 시 정보주체의 개인정보를 즉시 파기하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.5.1
중구분	개인정보 파기	**중요도**	**H**
항목 개요	개인정보 파기사유 발생 시 5일 이내에 파기하여야 함		
평가기준			
판단 기준	Y - 데이터베이스에 저장된 고객정보 파기사유 발생 시 5일 이내에 파기함 N - 데이터베이스에 저장된 고객정보 파기사유 발생 시 5일 이내에 파기하지 않고 있음		
점검 방법	▶ 데이터베이스에 저장된 고객정보 중 아래와 같은 사유 발생 시 즉시파기(5일 이내 파기)하고 있는지 확인 ① 사업자가 개인정보의 수집·이용 목적을 달성한 경우 ② 정보주체의 동의를 받을 때 고지한 보유기간이 만료된 경우 ③ 사업을 폐업하는 경우 ④ 정보주체가 개인정보 수집·이용·제공 등의 동의를 철회한 경우 ⑤ 정보주체가 개인정보 삭제 또는 파기를 요청한 때		
관련 근거	※ 개인정보보호법 <제21조> 개인정보의 파기 ※ 개인정보보호법 시행령 <제16조> 개인정보의 파기방법 ※ 개인정보 안전성 확보조치 기준 <제13조> 개인정보의 파기 ※ 표준 개인정보 보호지침<제10조> 개인정보의 파기방법 및 절차		
과징금 및 벌칙	※ 개인정보보호법 <제21조제1항> 개인정보가 불필요하게 되었을 때 파기하지 않은 경우 2년 이하의 징역 또는 2천만원 이하의 벌금 ※ 개인정보보호법 <제21조제1항> 개인정보의 파기 등 필요한 조치를 아니한 경우 3천만원 이하 과태료		

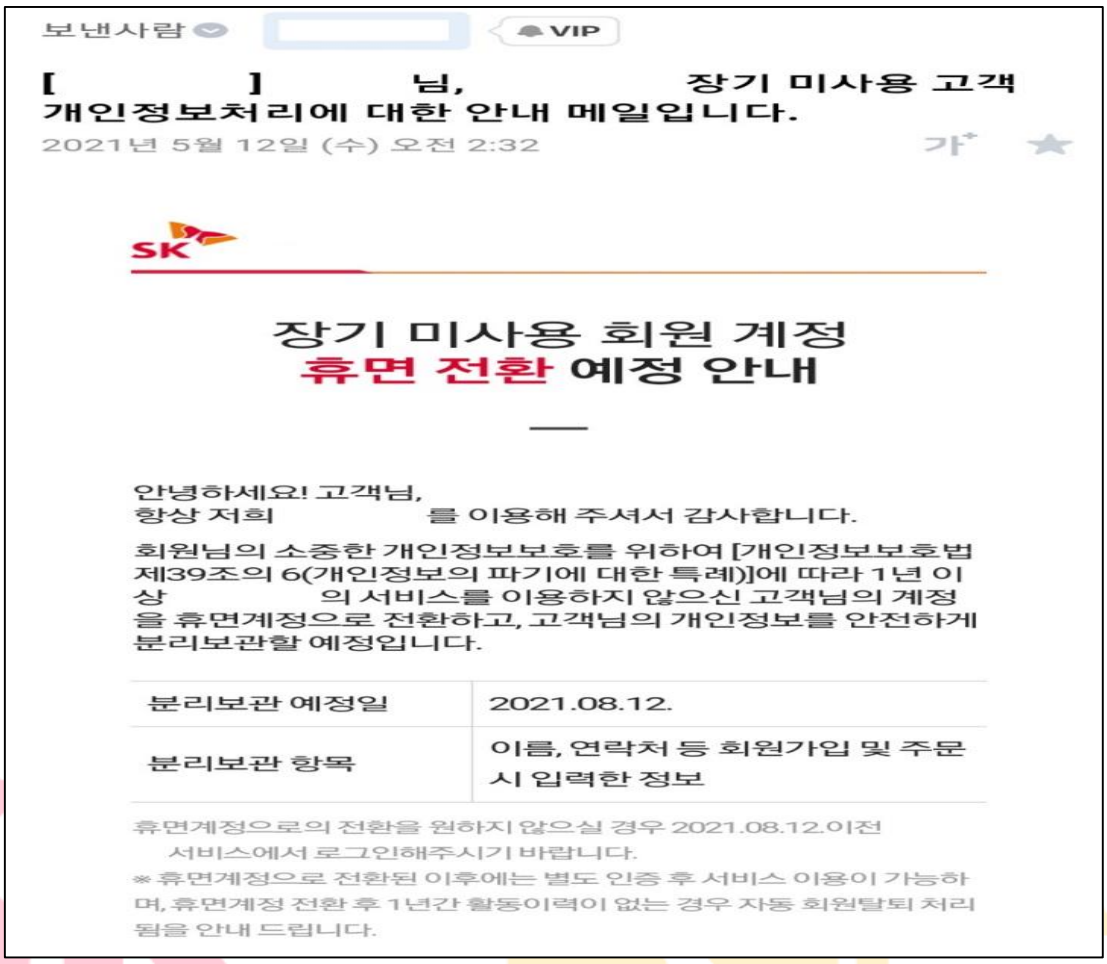
3.5.2 서버에 저장된 파일(로그데이터, 전송된 파일 데이터)의 정보에 대해 파기사유 발생 시 정보주체의 개인정보를 즉시 파기하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.5.2
중구분	개인정보 파기	**중요도**	**H**
항목 개요	개인정보 파기사유 발생 시 5일 이내에 파기하여야 함		
평가기준			
판단 기준	Y - 파일에 저장된 고객정보 파기사유 발생 시 5일 이내에 파기함 N - 파일에 저장된 고객정보 파기사유 발생 시 5일 이내에 파기하지 않고 있음		
점검 방법	▶ 파일에 저장된 고객정보 중 아래와 같은 사유 발생 시 즉시파기(5일 이내 파기) 하고 있는지 확인 ① 사업자가 개인정보의 수집·이용 목적을 달성한 경우 ② 정보주체의 동의를 받을 때 고지한 보유기간이 만료된 경우 ③ 사업을 폐업하는 경우 ④ 정보주체가 개인정보 수집·이용·제공 등의 동의를 철회한 경우 ⑤ 정보주체가 개인정보 삭제 또는 파기를 요청한 때		
관련 근거	※ 개인정보보호법 <제21조> 개인정보의 파기 ※ 개인정보보호법 시행령 <제16조> 개인정보의 파기방법 ※ 개인정보 안전성 확보조치 기준 <제13조> 개인정보의 파기 ※ 표준 개인정보 보호지침<제10조> 개인정보의 파기방법 및 절차		
과징금 및 벌칙	※ 개인정보보호법 <제21조제1항> 개인정보가 불필요하게 되었을 때 파기하지 않은 경우 2년 이하의 징역 또는 2천만원 이하의 벌금 ※ 개인정보보호법 <제21조제1항> 개인정보의 파기 등 필요한 조치를 아니한 경우 3천만원 이하 과태료		

3.5.3 개인정보취급자 단말(관리용 단말, 업무용 단말 포함)에 문서에 대해 파기사유 발생 시 정보주체의 개인정보를 즉시 파기하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.5.3
중구분	개인정보 파기	**중요도**	**H**
항목 개요	개인정보 파기사유 발생 시 5일 이내에 파기하여야 함		
평가기준			
판단 기준	Y - 단말에 저장된 고객정보 파기사유 발생 시 5일 이내에 파기함 N - 단말에 저장된 고객정보 파기사유 발생 시 5일 이내에 파기하지 않고 있음		
점검 방법	▶ 단말에 저장된 고객정보 중 아래와 같은 사유 발생 시 즉시파기(5일 이내 파기) 하고 있는지 확인 ① 사업자가 개인정보의 수집·이용 목적을 달성한 경우 ② 정보주체의 동의를 받을 때 고지한 보유기간이 만료된 경우 ③ 사업을 폐업하는 경우 ④ 정보주체가 개인정보 수집·이용·제공 등의 동의를 철회한 경우 ⑤ 정보주체가 개인정보 삭제 또는 파기를 요청한 때		
관련 근거	※ 개인정보보호법 <제21조> 개인정보의 파기 ※ 개인정보보호법 시행령 <제16조> 개인정보의 파기방법 ※ 개인정보 안전성 확보조치 기준 <제13조> 개인정보의 파기 ※ 표준 개인정보 보호지침<제10조> 개인정보의 파기방법 및 절차		
과징금 및 벌칙	※ 개인정보보호법 <제21조제1항> 개인정보가 불필요하게 되었을 때 파기하지 않은 경우 2년 이하의 징역 또는 2천만원 이하의 벌금 ※ 개인정보보호법 <제21조제1항> 개인정보의 파기 등 필요한 조치를 아니한 경우 3천만원 이하 과태료		

3.5.4 장기(1년) 미 이용자의 개인정보를 파기 또는 분리 저장, 관리하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.5.4
중구분	개인정보 파기	**중요도**	**H**
항목 개요	장기 미 이용자(휴면 계정 등)의 개인정보에 대한 파기기준을 수립하고 유효기간 경과 시 즉시 파기하여야 함		
평가기준			
판단 기준	Y - 장기(1년) 미 이용자에 대한 개인정보를 파기 또는 분리 저장하고 있음 P - 장기(1년) 미 이용자에 대한 개인정보를 파기 또는 분리 보관하여 관리하고 있으나 수동으로 처리하고 있음 N - 장기(1년) 미 이용자에 대한 개인정보의 적절한 파기 또는 분리 보관 관리를 수행하지 않음 N/A - 장기(1년) 미 이용자가 존재하지 않음		
점검 방법	▶ 장기(1년) 미 이용자의 개인정보를 다음과 같은 방법으로 파기 또는 분리 저장, 관리 여부 확인 ① 장기(1년) 미 이용자의 개인정보는 1년 경과시점에 즉시 파기가 원칙임 ② 특정 운영사유에 의해서 장기 미 이용자의 개인정보의 보관이 필요한 경우, 일반 회원(고객)의 개인정보 DB와 분리 - DB 또는 테이블, 파일시스템 등에 별도로 저장, 관리하고 일반 직원들의 접근 제한 등 접근 권한을 최소화 ※ 기존 가입자의 경우 정보통신서비스 미 이용 기간은 시행령 부칙 제2조에 따라 개정 정보통신망법 시행령의 시행일인 2012년 8월 18일을 기점으로 산정해야 한다		
관련 근거	※ 개인정보보호법 <제21조> 개인정보의 파기 ※ 개인정보보호법 <제39조의6> 개인정보의 파기에 대한 특례 ※ 개인정보보호법 시행령 <제16조> 개인정보의 파기방법 ※ 개인정보보호법 시행령 <제48조의5> 개인정보의 파기 등에 관한 특례 ※ 개인정보 안전성 확보조치 기준 <제13조> 개인정보의 파기 ※ 표준 개인정보 보호지침<제10조> 개인정보의 파기방법 및 절차 ※ 표준 개인정보 보호지침<제11조> 법령에 따른 개인정보의 보존		
과징금 및 벌칙	※ 개인정보보호법 <제21조제3항> 개인정보를 분리하여 저장, 관리하지 않은 경우 1천만 이하 과태료 ※ 개인정보보호법 <제39조의6> 개인정보파기 등의 필요한 조치를 하지 않은 경우		

	3천만원 이하 과태료

3.5.5 장기(1년) 미 이용자의 개인정보의 유효기간 만료 30일 전에 통지하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.5.5
중구분	개인정보 파기	**중요도**	**H**
항목 개요	장기 미 이용자(휴면 계정 등)의 개인정보 파기 시, 파기 30일 전에 정보주체에게 통지하고 파기하여야 함		
평가기준			
판단 기준	Y - 유효기간 만료 30일 전까지 개인정보가 파기되는 사실, 기간 만료일 및 파기되는 개인정보의 항목 등을 통지함 N - 유효기간 만료 30일 전까지 개인정보가 파기되는 사실, 기간 만료일 및 파기되는 개인정보의 항목 등을 통지하지 않음 N/A - 장기 미 이용자 없음		
점검 방법	▶ 장기(1년) 미 이용자의 개인정보 유효기간 만료 30일전에 통지하고 있는지 확인 ① 전자우편, 서면, 팩스, 전화 등의 방법 중 하나를 선택하여 이용자의 개인정보가 파기 또는 분리하여 저장, 관리되는 사실, 일시 및 해당 개인정보 항목을 통지 - 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		

<table>
<tr><td></td><td> 

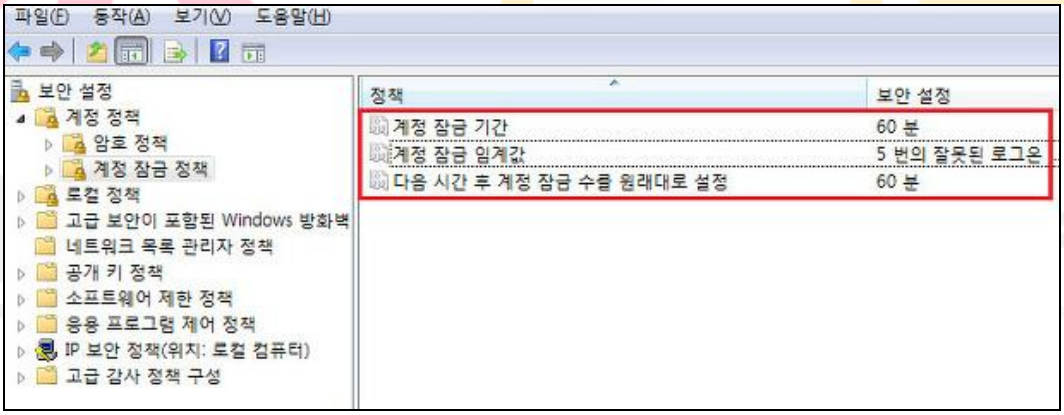
<그림 49> 장기미용자 만료 예정 통지 예시</td></tr>
<tr><td>관련 근거</td><td>※ 개인정보보호법 <제39조의6> 개인정보의 파기에 대한 특례
※ 개인정보보호법 시행령 <제48조의5> 개인정보의 파기 등에 관한 특례
※ 정보보호 및 개인정보보호 관리체계 인증 <3.4.3> 휴면 이용자 관리</td></tr>
<tr><td>과징금 및 벌칙</td><td>※ 개인정보보호법 <제39조의6> 기간만료 30일 전까지 개인정보가 파기되는 사실 및 만료일 등을 알리지 아니한 경우 3천만원 이하 과태료</td></tr>
</table>

3.5.6 회원탈퇴나 보유기간 만료 시 다른 법률에 따라 개인정보를 보존해야 하는 경우에는 기존 개인정보 DB와 분리하여 별도로 보관하고 있습니까?			
항목구분			
대구분	개인정보 처리단계별 보호조치	**항목코드**	3.5.6
중구분	개인정보 파기	**중요도**	**H**
항목 개요	개인정보를 보존하여야 할 경우 정보주체의 개인정보 DB와 별도의 DB에 분리하여 보관 및 관리하여야 함		
평가기준			
판단 기준	Y - 적절하게 분리보관하고 별도의 접근제한을 실시함 P - 분리보관하고 있으나 과도한 정보를 분리보관 하거나 별도의 접근제한을 실시하지 않음 N - 분리보관 대상이 존재하나 별도 분리보관 실시하지 않음 N/A - 분리보관 대상 없음		
점검 방법	▶ 탈퇴회원 포함 개인정보 즉시 파기 대상에 대해서 다른 법률에 따라 관련 개인정보를 보관하는 경우 분리된 DB에 저장·보관 여부를 확인하고, 분리된 DB에 대해서 접근 제한하고 있는지 확인 ① 별도 DB나 파일시스템에 분리 보관여부 확인 ② 분리 보관된 DB 또는 파일시스템은 별도의 접근권한자에 의해서만 접근 가능하도록 조치 ③ 분리보관 된 데이터가 관련 법률에 의해 필요한 정보여부 확인		
관련 근거	※ 개인정보보호법 <제21조> 개인정보의 파기 ※ 개인정보보호법 시행령 <제16조> 개인정보의 파기방법 ※ 개인정보 안전성 확보조치 기준 <제13조> 개인정보의 파기 ※ 표준 개인정보 보호지침<제11조> 법령에 따른 개인정보의 보존		
과징금 및 벌칙	※ 개인정보보호법 <제21조제3항> 개인정보를 분리하여 저장, 관리하지 않은 경우 1천만원 이하 과태료		

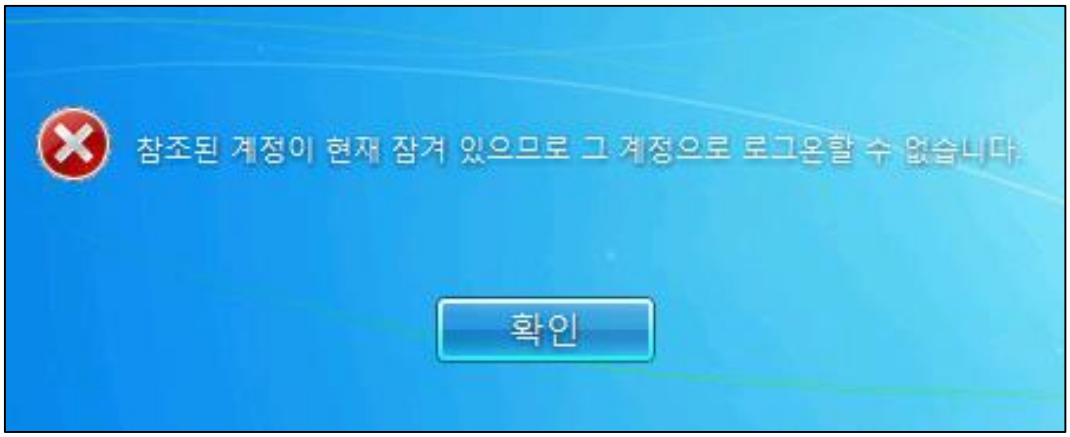
4. 개인정보 기술적 보호조치

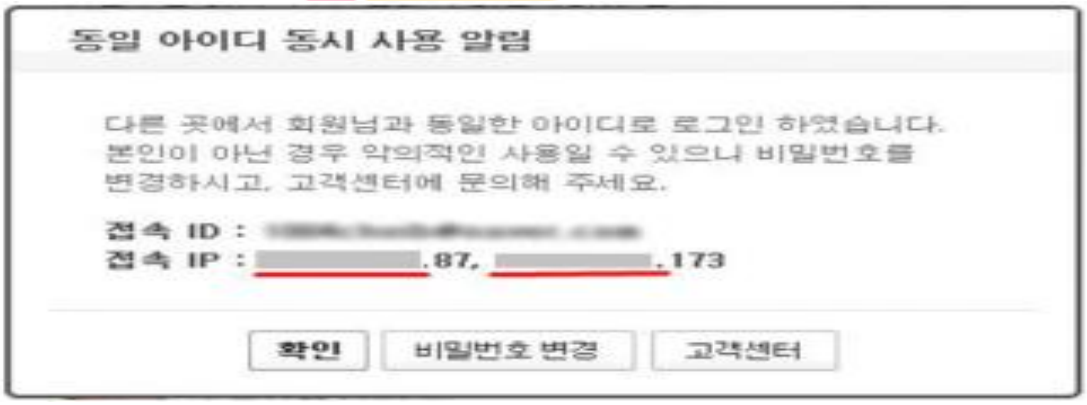
4.1. 개인정보처리시스템 접근관리

4.1.1 개인정보처리시스템 접속 시 동일계정에 대한 로그인 지속 실패에 대한 통제적용을 하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.1.1
중구분	개인정보처리시스템 접근관리	**중요도**	**H**
항목 개요	개인정보처리시스템에 지속적인 로그인 실패 시 이를 차단해야 함.		
평가기준			
판단 기준	Y - 비밀번호 5회 이상 틀렸을 시 계정 차단되고 있음 N - 비밀번호 5회 이상 틀렸을 시 계정 차단되지 않고 있음		
점검 방법	▶ 개인정보처리시스템(응용프로그램, OS) 접근 실패 임계 값 설정 여부 확인 ① 일정 로그인 시도 시 계정 통제 정책 및 설정 확인 - 비밀번호를 5회 이상 틀렸을 경우 계정 자체가 차단되는지 확인 ※ DB는 점검대상에서 미 포함 (DBMS에 따라 관련 설정기능 유무 다름)		



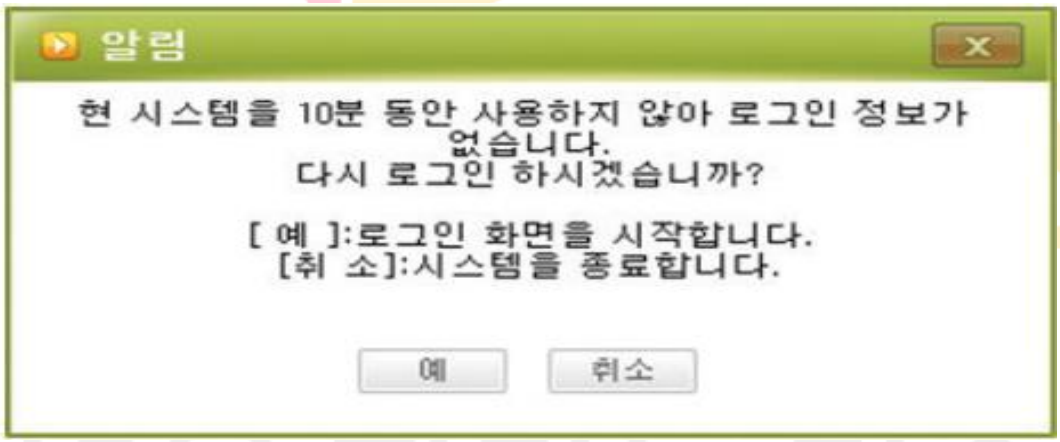
<그림 50> Windows 서버 계정잠금 설정 예시

	 **<그림 51> Windows 서버 계정잠금 화면 예시**
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보의 안전성 확보 조치 기준 <제5조> 접근 권한의 관리 ※ 개인정보의 기술적 관리적 보호조치 기준 <제4조> 접근통제
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

4.1.2 응용프로그램에 대한 세션 수를 통제하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.1.2
중구분	개인정보처리시스템 접근관리	**중요도**	**H**
항목 개요	개인정보를 처리하는 응용프로그램의 계정은 세션 수를 1개로 제한하여 동시 접속되지 않게 해야 함.		
평가기준			
판단 기준	Y - 계정 별 세션 수는 1개로 설정함 N - 계정에 대한 세션 수가 제한되어 있지 않음		
점검 방법	▶ 개인정보처리시스템 응용프로그램(web, Mobile app, C/S등) 접속 시 동일계정 접속 세션 수 제한여부 확인 ① 동일한 계정이 여러 곳에서 접근이 가능한지 확인  ※ 출처: 개인정보영향평가 수행안내서 **<그림 52> 관리자계정 동시 접속**		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보 조치 기준 <제6조> 접근통제 ※ 정보보호 및 개인정보보호 관리체계 인증 <2.6.3> 응용 프로그램 접근		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원이하 과태료		

4.1.3 개인정보처리시스템에 대한 세션타임 아웃이 적용되어 있습니까?

항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.1.3
중구분	개인정보처리시스템 접근관리	**중요도**	**H**
항목 개요	개인정보처리시스템에 접속 후 세션타임 아웃이 설정되어 특정시간 이상 시스템에 지속적으로 접근이 불가능 해야 함.		
평가기준			
판단 기준	Y - 접근 세션타임이 안전하게 적용되어 있음 P - 접근 세션타임이 적용되어 있으나 불필요하게 길게 적용되어 있음 N - 접근 계정 세션타임이 적용되지 않음		
점검 방법	▶ 개인정보처리시스템(응용프로그램, OS) 접근 세션타임 제한여부 확인 ① 일정 시간 사용하지 않는 경우 로그아웃이 되도록 설정되어 있는지 확인 - OS: 5분 및 WEB/WAS: 60분 ※ DB는 점검대상에서 미 포함 (DBMS에 따라 관련 설정 기능 유무 다름)		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보 조치 기준 <제6조> 접근통제		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원이하 과태료		



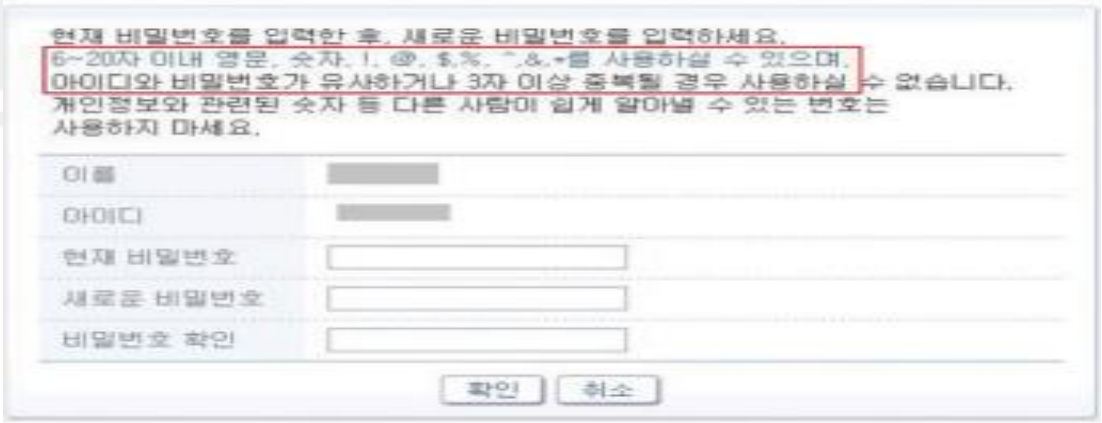
※ 출처: 개인정보영향평가 수행안내서

<그림 53> 세션 타임아웃 팝업 설정 예시

4.1.4 사용자 비밀번호 생성/변경 시 작성규칙을 준수하고 있습니까?

항목구분

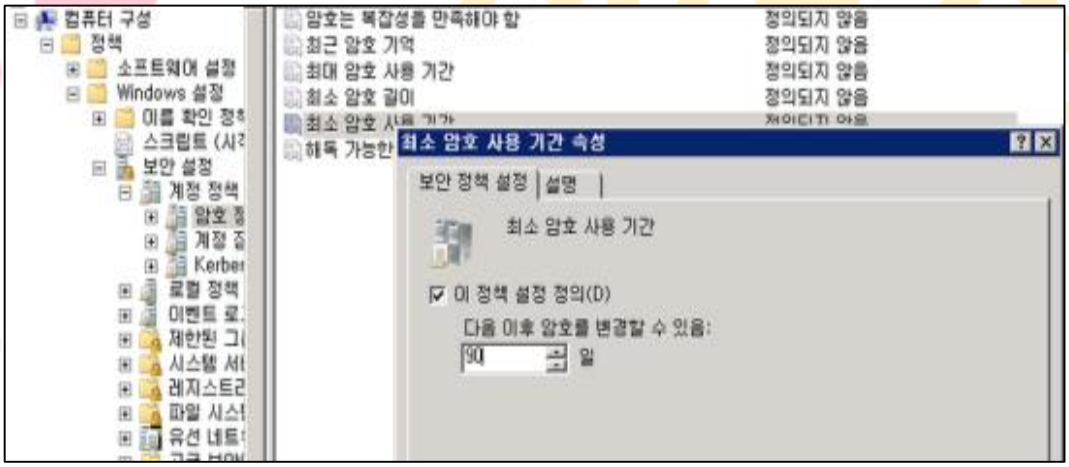
대구분	개인정보 기술적 보호조치	항목코드	4.1.4
중구분	개인정보처리시스템 접근관리	중요도	H
항목 개요	비밀번호 작성규칙을 규정하고 있고, 이를 준수하고 있어야 함.		
평가기준			
판단 기준	Y - 비밀번호 작성 규칙을 모두 준수하고 있음 P - 비밀번호 작성 규칙을 일부 준수하고 있음 N - 비밀번호 작성을 미 준수하여 취약하게 설정되어 있음		
점검 방법	▶ 사용자 비밀번호 작성 규칙/지침 확인 (기준을 반드시 준수하는가 확인) ① 다음 각 목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성 가. 영문 대문자(26개) 나. 영문 소문자(26개) 다. 숫자(10개) 라. 특수문자(32개) ② 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고 ③ 동일한 비밀번호 사용 제한 ④ 비밀번호 초기화 시 부여 받은 임시 비밀번호(작성규칙 적용) 변경 관리 ⑤ 사용자 로그인 시도 시 잘못된 패스워드 입력 횟수를 제한(5회 이내) ※ 비밀번호 생성 예시 : Skshieldus! → 영대문자, 영소문자, 특수문자 총 3종류를 조합한 10자리 ※ 상위 내역은 사용자(개인정보취급자)대상이고, 이용자(대고객)의 필수준수사항은 아님		
관련	※ 개인정보보호법 <제29조> 안전조치의무		



※ 출처: 개인정보영향평가 수행안내서

<그림 54> 비밀번호 작성규칙

근거	※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보 조치 기준 <제5조> 접근 권한의 관리 ※ 정보보호 및 개인정보보호 관리체계 인증 <2.5.4> 비밀번호 관리 ※ 개인정보의 기술적·관리적 보호조치기준 <제4조> 접근통제
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

4.1.5 사용자 비밀번호를 주기적으로 변경하여 관리하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.1.5
중구분	개인정보처리시스템 접근관리	**중요도**	**H**
항목 개요	비밀번호 작성규칙을 규정하고 있고, 이를 준수하고 있어야 함.		
평가기준			
판단 기준	Y - 비밀번호를 주기적으로 변경 관리하고 있음. P - 비밀번호를 주기적으로 변경 관리하고 있으나 변경주기가 기준을 초과함 N - 비밀번호를 주기적으로 변경하지 않음		
점검 방법	▶ 사용자 비밀번호 주기적 변경 시행여부 확인 ① 비밀번호 정기적 변경 주기 (ex: 변경주기 - 분기별 1회) - OS/WEB/WAS/DB: 180일 - 비밀번호에 유효기간을 설정하여 반기 별 1회 이상 변경(자경단, ISMS-P기준) - 단, 주요정보통신 기반시설 관련 서비스의 경우 분기(90일) 별 1회 이상 변경  <그림 55> Windows 서버 비밀번호 변경주기 설정 예시		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보 조치 기준 <제5조> 접근 권한의 관리 ※ 정보보호 및 개인정보보호 관리체계 인증 <2.5.4> 비밀번호 관리 ※ 개인정보의 기술적·관리적 보호조치기준 <제4조> 접근통제		
과징금	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를		

및 벌칙	도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

4.2. 개인정보처리시스템 접근통제

4.2.1 내부관리용 응용프로그램 접속 시 인가 받지 않은 접근을 제한하기 위한 접근통제를 적용하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.2.1
중구분	개인정보처리시스템 접근통제	**중요도**	**H**
항목 개요	비 인가된 사용자가 개인정보처리시스템 응용프로그램에 접근할 수 없도록 보호조치를 취해야 함		
평가기준			
판단 기준	Y - 1) 내부망 특정 단말에서만 접근을 허용 2) 외부 공인망에서 특정 단말만 접근 허용 P - 내부망 IP대역으로 제한 N - 1) 내부망 전체에 접근 허용 2) 외부 공인망에 전체에 접근 허용 N/A - 1) 응용프로그램 없음 2) 서비스 특성상 외부 공인망 오픈필요		
점검 방법	▶ 응용프로그램(Back office-WEB/WAS, App 등) 접근 시 접근통제 적용 확인 ① 방화벽/라우터 ACL 등을 통해 특정 IP/MAC을 사용하는 단말만 접근 허용 여부 확인 - 개인정보처리시스템(내부 관리용 응용프로그램) 최소한의 개인정보 취급자 접속이 가능하도록 제한된 단말에서만 접근이 가능하도록 제한 - 단, 서비스의 특성 상 다수의 취급자 접속이 필요한 경우 특정 대역에 대한 접속 허용 정책 적용을 허용 가능함. - 위치정보서비스는 IP대역으로 ACL을 적용하여 해당 서비스의 취급자 外 접속이 가능한 경우 미적용으로 함. ※ 위치정보사업자는 위치정보취급자가 사용할 수 있는 단말기를 제한하고 외부로부터 접근을 차단하기 위하여 다음과 같이 단말기 주소 등의 식별과 인증을 실시하여야 함 1. 접근 권한자에 대한 식별인증(ID, 패스워드 등) 2. 단말기에 대한 식별인증(주소 등): 방화벽, 어플리케이션, PKI기반인증서, 생체인식 등		

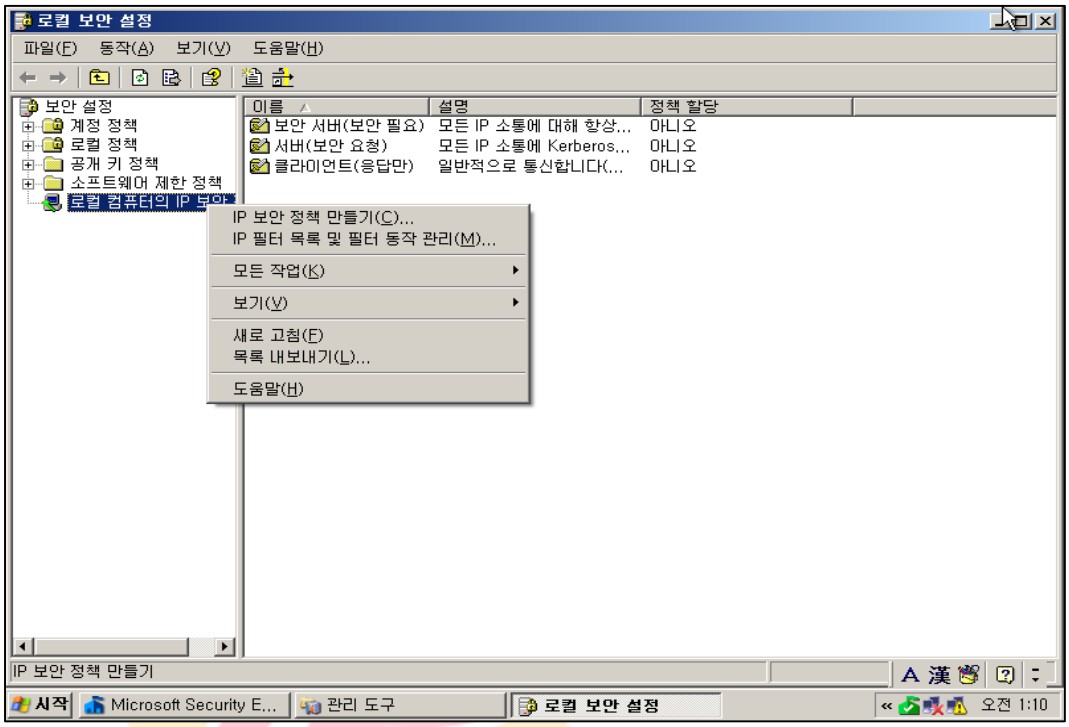
<table>
<tr>
<td></td>
<td>


※ 출처: 홈페이지 개인정보 노출방지 안내서
<그림 56> 관리자 페이지 접근제한(특정 IP만 접속허용)


※ 출처: 홈페이지 개인정보 노출방지 안내서
<그림 57> 관리자 페이지 2차 인증 예시
</td>
</tr>
<tr>
<td>관련
근거</td>
<td>※ 개인정보보호법 <제29조> 안전조치의무
※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치
※ 개인정보의 안전성 확보 조치 기준 <제6조> 접근통제
※ 개인정보의 기술적·관리적 보호조치기준 <제4조> 접근통제</td>
</tr>
<tr>
<td>과징금
및
벌칙</td>
<td>※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금
※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료</td>
</tr>
</table>

4.2.2 개인정보 취급자가 외부에서 내부관리용 응용프로그램 접속 시 공인인증서, OTP 등 안전한 접속수단을 적용하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.2.2
중구분	개인정보처리시스템 접근통제	**중요도**	**H**
항목 개요	외부에서 내부관리용 응용프로그램 접속이 가능할 경우 비 인가된 사용자의 접근 제한 및 정보유출 방지를 위해 가상사설망(VPN), 전용선, 공인인증서 등 안전한 접속수단을 사용하여야 함		
평가기준			
판단 기준	Y - 외부에서 접속 시 안전한 접속수단 적용 N - 외부에서 접속 시 안전한 접속수단 미 적용 (IP/MAC인증은 추가인증 수단 未 인정) N/A - 공인망 접근 없음		
점검 방법	▶ 개인정보처리시스템(Back office-WEB/WAS, App, 서버 등) 접근 시 접근통제 적용확인 ① 외부망에서 내부 개인정보처리시스템의 접속차단 여부 확인 ② 외부망에서 접속 시 관리자 승인 및 보호방안 적용 - ID/PW 외 추가인증 수단 존재여부 확인 (휴대폰 인증, 메일인증, I-PIN 인증, OTP 등) - VPN, 전용선 등 안전한 접속수단 사용 확인		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보조치 ※ 개인정보의 안전성 확보조치 기준 <제6조> 접근통제 ※ 개인정보의 기술적·관리적 보호조치기준 <제4조> 접근통제		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료		

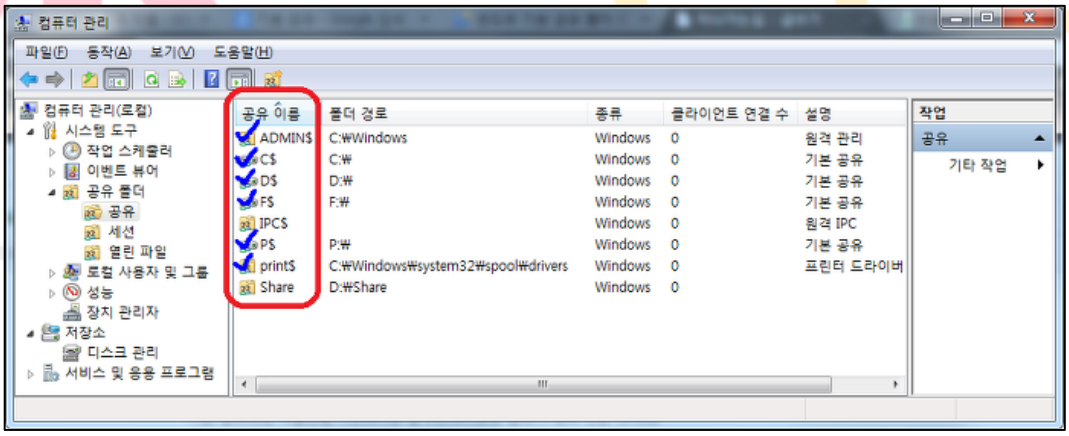
4.2.3 서버 접근 시 접근통제 적용되어 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.2.3
중구분	개인정보처리시스템 접근통제	**중요도**	**H**
항목 개요	개인정보처리시스템 서버에 접근 시 허용된 인력만 접근이 가능하게 통제하여야 함		
평가기준			
판단 기준	Y - 1) 내부망에서 서버 접근 시 특정 단말 접근허용 2) 외부 공인망에서 특정 단말만 접근 허용 P - 내부망 특정 IP대역에서 접근 가능 N - 1) 내부망 전체에서 접근 허용 2) 외부 공인망 전체에 접근 허용 N/A - 1) 서버 원격접속 없음 2) 서비스 특성상 외부 공인망 오픈필요		
점검 방법	▶ 서버 접근 시 접근통제 적용 확인 ① 망분리 후 방화벽/라우터 등을 통해 특정 IP/MAC 접근만 허용 ② 서버의 ACL 기능을 이용하여 특정 IP/MAC 접근만 허용 ③ 서버접근제어시스템을 통한 허용 ※ 원격지에서의 접속은 원칙적으로 금하나 부득이한 경우 서버 관리자의 승인 및 보호방안을 마련하여야 한다		

<table>
<tr><td></td><td> 

<그림 58> Windows 서버 ACL 설정 예시</td></tr>
<tr><td>관련
근거</td><td>※ 개인정보보호법 <제29조> 안전조치의무
※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보조치
※ 개인정보의 안전성 확보조치 기준 <제6조> 접근통제
※ 개인정보의 기술적·관리적 보호조치기준 <제4조> 접근통제</td></tr>
<tr><td>과징금
및
벌칙</td><td>※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금
※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료</td></tr>
</table>

4.2.4 서버 접근 시 안전한 통신 수단(ssh 등)을 적용하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.2.4
중구분	개인정보처리시스템 접근통제	**중요도**	**H**
항목 개요	개인정보처리시스템 서버에 접근 시 암호화된 통신 수단 등의 보호조치를 취하여야 함		
평가기준			
판단 기준	Y - 안전한 통신수단을 사용하여 접근 N - 안전한 통신수단 없이 서버에 접속 N/A - 서버 원격접속 없음		
점검 방법	▶ 서버 접근 시 안전한 통신수단을 사용 확인 ① 내부망에서 서버 접근 시 안전한 통신수단(ssh등) 사용 확인		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보조치 ※ 개인정보의 안전성 확보조치 기준 <제6조> 접근통제		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료		

4.2.5 서버의 불필요한 인터넷망을 차단하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.2.5
중구분	개인정보처리시스템 접근통제	**중요도**	**H**
항목 개요	개인정보처리시스템 서버의 인터넷망을 통제하여, 개인정보유출에 대한 차단이 되어야 함.		
평가기준			
판단 기준	Y - 1) 서버의 불필요한 인터넷망 차단하고 있음 2) 인터넷망의 접근이 가능하나 통제기준에 따른 통제절차 준수함 N - 서버에서 불필요한 인터넷망 접근이 가능함		
점검 방법	▶ 서버(내부망에 위치하고 개인정보를 보유한 서버, 예:DB서버)의 불필요한 인터넷망 차단 여부 확인 ① 방화벽 및 네트워크 장비를 통한 인터넷망 접근 통제 확인 ② 외부 인터넷망 접근이 필요할 경우(외부 API 연동 등) - 통제 절차 및 통제 기준 확인 - 외부 인터넷망 접근 허용의 목적 및 타당성 확인 ※ WhiteList 방식 차단 권고		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보조치 ※ 개인정보의 안전성 확보조치 기준 <제6조> 접근통제 ※ 개인정보의 기술적·관리적 보호조치기준 <제4조> 접근통제		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료		

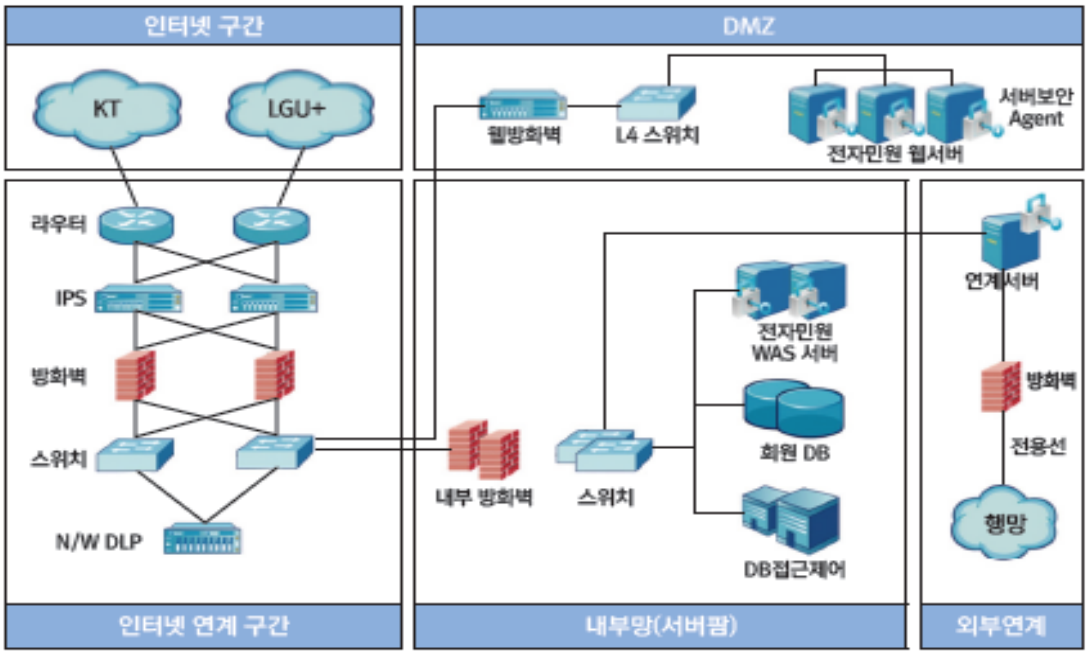
4.2.6 서버의 공유 폴더 및 Storage 사용 시 접근권한이 해당 서버로 제한되어 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.2.6
중구분	개인정보처리시스템 접근통제	**중요도**	**H**
항목 개요	개인정보처리 서버/단말에서 사용자 공유 폴더를 제한해야 하고, Storage 사용 시 Storage를 통한 파일 공유가 차단되어야 함.		
평가기준			
판단 기준	Y - 1) 공유 폴더 및 Storage를 사용하지 않고 있음 2) 공유 폴더 및 Storage 사용 시 타 서비스/시스템과 데이터 공유하지 않고 있음 N - 공유 폴더 및 Storage를 사용하고 있고, 타 서비스/시스템에서 목적 외에 공유 가능		
점검 방법	▶ 서버에서 사용자 공유 폴더 제한 ① 공유 폴더 사용하더라도, 해당 서버만 접근권한 부여 확인 ② 사용자 공유 폴더 존재여부 확인(Windows 서버) - [명령] 시작 > 실행 > cmd > net share - 폴더 또는 디렉터리 공유 금지 - 네트워크 드라이브 공유 금지 ▶ Storage 사용 시 타 서비스/시스템과의 데이터 공유 제한 확인  **<그림 59> Windows 기본 공유 폴더 설정된 화면**		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보조치 ※ 개인정보의 안전성 확보조치 기준 <제6조> 접근통제		
과징금 및	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금		

벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

4.2.7 데이터베이스 접근통제가 적용되어 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.2.7
중구분	개인정보처리시스템 접근통제	**중요도**	**H**
항목 개요	개인정보처리시스템 데이터베이스에 접근 시 관련 업무에 필요한 최소한의 권한만 차등 부여하고 관리자 외의 사용자에게 DBA 권한을 제한 시켜야 함		
평가기준			
판단 기준	Y - 데이터베이스 접근 시 특정 서버 및 단말 접근허용 P - 내부망 특정 네트워크 대역에서 접근 가능 N - 1) 내부망 전체에서 접근 허용 2) 외부망에서 접근 허용		
점검 방법	▶ 데이터베이스 접근통제 확인 ① 데이터베이스에 접속 시 접근통제(IP, MAC 등) 적용 확인 ② DMZ 구간에 위치한 웹서버에서 내부 데이터베이스로 접근할 경우 관련 포트 이외의 서비스포트(ftp, telnet, 터미널 등)의 차단 확인 ③ DB접근제어시스템 적용중인 경우, WAS서버 등 우회 경로의 존재 여부 ※ IP 접근통제 적용 시 192.168.0.1 ~ 192.168.0.50 등의 내부망 특정 대역으로 지정할 경우 미흡		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보조치 ※ 개인정보의 안전성 확보조치 기준 <제6조> 접근통제 ※ 개인정보의 기술적·관리적 보호조치기준 <제4조> 접근통제		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료		

4.2.8 데이터베이스는 내부망/비공개된 네트워크 영역에 위치하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.2.8
중구분	개인정보처리시스템 접근통제	**중요도**	**H**
항목 개요	개인정보를 저장하고 있는 데이터 베이스가 공개된 영역에 위치해 있을 경우 개인정보의 유출 가능성이 존재하므로 내부망/비공개된 네트워크 영역에 존재 해야함		
평가기준			
판단 기준	Y - 데이터베이스가 내부망/비공개된 네트워크 영역에 위치하고 있음 N - 데이터베이스가 공개된 네트워크 영역에 위치하고 있음		
점검 방법	▶ 데이터베이스의 네트워크 구성 위치 확인 ① 내부망/비공개된 네트워크에 위치하는지 확인 (공개 네트워크 영역(DMZ) 위치하여서는 안됨)		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보조치 ※ 정보보호 및 개인정보보호 관리체계 인증 <2.6.1> 네트워크 접근 ※ 정보보호 및 개인정보보호 관리체계 인증 <2.6.4> 데이터베이스 접근		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료		

4.2.9 침입/공격을 탐지/차단할 수 있는 보안 솔루션이 구성되어 있고, 관련 모니터링을 하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.2.9
중구분	개인정보처리시스템 접근통제	**중요도**	H
항목 개요	방화벽, IPS/IDS, 웹방화벽과 같은 보안 시스템의 구축되어 내부 시스템을 보호하고 있고, 이 보안장비들에 대해서 외부 침입시도에 대한 모니터링이나 주기적 분석이 진행되어야 함.		
평가기준			
판단 기준	Y - 1) 내부망에서 서비스 시 보안 솔루션의 보호받고 있음 2) 외부망에서 서비스 시 자체 보안 솔루션 통해 보호받고 모니터링 하고 있음 P - 보안 솔루션에 대한 별도 모니터링은 없음 N - 보안 솔루션이 구축되어 있지 않음		
점검 방법	▶ 침입탐지시스템, 침입차단시스템 구성 및 모니터링 확인 ① 내부망에서 대고객 서비스를 하는 경우 서비스 시스템(OS, DB, WAS 등)이 방화벽 및 WebSafeZone(IPS, WAF)/NetworkSafeZone(IPS, WAF)을 통해 보호를 받고 있는지 확인 ② 외부망에서 서비스하는 대고객 서비스일 경우 자체 보안솔루션 적용 및 모니터링 확인		
관련	※ 개인정보보호법 <제29조> 안전조치의무		



※ 출처: 개인정보영향평가 안내서

<그림 60> 정보보호시스템 구성도

근거	※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보조치 ※ 개인정보의 안전성 확보조치 기준 <제6조> 접근통제
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

4.3. 개인정보의 암호화

<table>
<tr><th colspan="4">4.3.1 주요 개인정보를 안전한 암호알고리즘으로 암호화하여 저장하고 있습니까?</th></tr>
<tr><th colspan="4">항목구분</th></tr>
<tr><td>대구분</td><td>개인정보 기술적 보호조치</td><td>항목코드</td><td>4.3.1</td></tr>
<tr><td>중구분</td><td>개인정보의 암호화</td><td>중요도</td><td>H</td></tr>
<tr><td>항목
개요</td><td colspan="3">개인정보처리 시스템의 중요 개인정보는 안전하게 암호화해야 함</td></tr>
<tr><th colspan="4">평가기준</th></tr>
<tr><td>판단
기준</td><td colspan="3">Y - 안전한 알고리즘으로 암호화 저장
P - 안전하지 않은 알고리즘으로 암호화 저장
N - 암호화하여 저장하지 않음
N/A - 암호화 대상 주요 개인정보 없음</td></tr>
<tr><td>점검
방법</td><td colspan="3">▶ 주요 개인정보 암호화 알고리즘 확인
① 주민등록번호, 계좌번호, 신용카드번호, 여권번호, 운전면허번호, 외국인등록번호, 위치정보 등에 대해 AES-128 등의 암호화 알고리즘으로 적용
※ DB 및 파일(Txt 등 DRM이 적용되지 않은 파일의 경우)내 저장된 정보 중 주요 개인정보는 암호화 알고리즘 적용 필요(주요 개인정보 컬럼 암호화)
<table>
<tr><th>구분</th><th>알고리즘</th></tr>
<tr><td>대칭키 암호
알고리즘</td><td>SEED
HIGHT
ARIA-128/192/256
AES-128/192/256
Camelia-128/192/256 등</td></tr>
<tr><td>공개키 암호
알고리즘</td><td>RSA
RSAES-OAEP 등</td></tr>
<tr><td>일방향 암호
알고리즘</td><td>SHA-224/256/384/512
Whirlpool 등</td></tr>
</table>
※ 출처: 개인정보의 암호화 조치 안내서
<표 5> 안전한 알고리즘(2020.12 기준)</td></tr>
<tr><td>관련
근거</td><td colspan="3">※ 개인정보보호법 <제24조> 고유식별정보의 처리 제한
※ 개인정보보호법 시행령 <제21조> 고유식별정보의 안전성 확보 조치
※ 개인정보보호법 시행령 <제21조의2> 주민등록번호 암호화 적용 대상
※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치</td></tr>
</table>

	※ 개인정보보호법 시행령 <제48조의2> 개인정보의 안전성 확보 조치에 관한 특례 ※ 개인정보의 안전성 확보조치 기준 <제7조> 개인정보의 암호화 ※ 개인정보의 기술적·관리적 보호조치기준 <제6조> 개인정보의 암호화
과징금 및 벌칙	※ 개인정보보호법 <제24조제3항> 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손된 경우 (암호화 등 안전성 확보에 필요한 조치를 하지 않은 경우) 5억원 이하의 과징금 ※ 개인정보보호법 <제24조> 고유식별정보 암호화 조치 아니한 경우 5년 이하의 징역 또는 5천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

4.3.2 비밀번호 등 인증관련 정보는 안전한 일방향 암호화 알고리즘으로 암호화하여 저장하고 있습니까?

항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.3.2
중구분	개인정보의 암호화	**중요도**	**H**
항목 개요	개인정보처리 시스템의 인증관련 정보는 일방향 암호화 알고리즘으로 암호화해야 함		

평가기준

판단 기준

Y - 안전한 일방향 알고리즘으로 암호화 저장
P - 안전하지 않은 알고리즘으로 암호화 저장
N - 암호화하여 저장하지 않음
N/A - 인증이 없는 단순 소개 페이지

점검 방법

▶ 인증관련 정보 암호화 적용 여부 확인
① 인증정보(비밀번호, 바이오 정보) 일방향 암호화(SHA-256 등) 적용여부 확인
② 주민등록번호 인증정보로 사용 시 일방향 암호화 적용 확인
※ DB 및 파일(txt 등 DRM이 적용되지 않은 파일의 경우)내 저장된 정보 중 인증정보는 암호화 알고리즘 적용 필요(인증정보 컬럼 암호화)

보안강도	해시 함수	안전성
80비트 미만	MD5, SHA-1	권고하지 않음.
80비트	HAS-160	
112비트	SHA-224	권고함
128비트	SHA-256	
192비트	SHA-384	
256비트	SHA-512	

※ 출처: 개인정보의 암호화 조치 안내서

<표 6> 보안강도에 따른 해시 함수 분류

관련 근거

※ 개인정보보호법 <제29조> 안전조치의무
※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치
※ 개인정보보호법 시행령 <제48조의2> 개인정보의 안전성 확보 조치에 관한 특례
※ 개인정보의 안전성 확보조치 기준 <제7조> 개인정보의 암호화
※ 개인정보의 기술적·관리적 보호조치기준 <제6조> 개인정보의 암호화

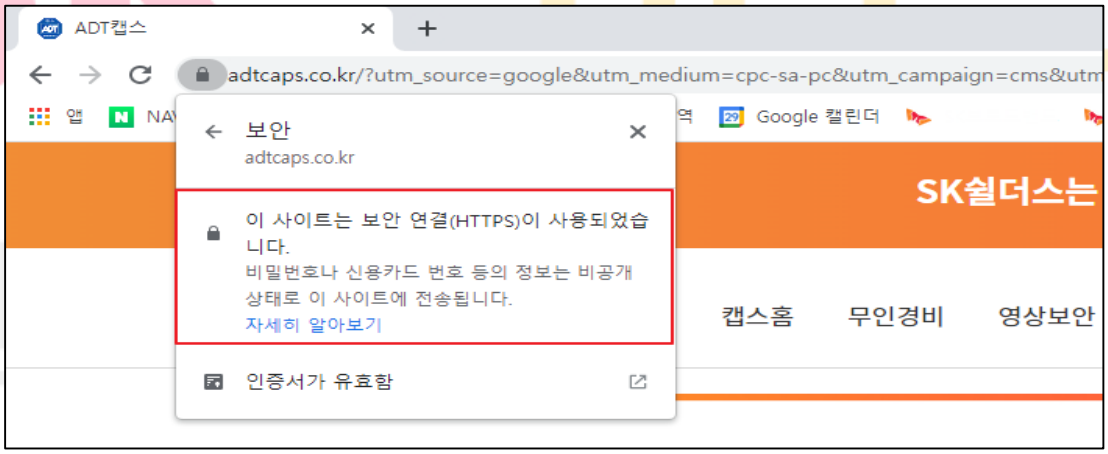
과징금

※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를

및 벌칙	도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

4.3.3 로그에 개인정보가 기록되는 경우 마스킹 또는 암호화를 적용하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.3.3
중구분	개인정보의 암호화	**중요도**	**H**
항목 개요	접속/작업로그 등에 개인정보가 저장되는 경우, 해당 개인정보 또한 마스킹 또는 암호화를 적용하여야 함		
평가기준			
판단 기준	Y - 로그 내 고객 주요 개인정보 암호화하고 있음 N - 로그 내 고객 주요 개인정보 암호화하지 않음		
점검 방법	▶ 접속/작업로그 기록 시 고객 개인정보 마스킹/암호화 여부 확인 ① 로그 내 고객 주요 개인정보 암호화 여부 확인 - 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드 번호, 위치정보 등 암호화가 의무화된 주요 고객 개인정보에 대한 암호화 ② 로그 내 고객 개인정보 마스킹 여부 확인(권고) - 성명, 생년월일, 세부 주소 등 마스킹이 필요한 고객 정보에 대한 마스킹 권고		
관련 근거	※ 개인정보보호법 <제24조> 고유식별정보의 처리 제한 ※ 개인정보보호법 시행령 <제21조> 고유식별정보의 안전성 확보 조치 ※ 개인정보보호법 시행령 <제21조의2> 주민등록번호 암호화 적용 대상 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보보호법 시행령 <제48조의2> 개인정보의 안전성 확보 조치에 관한 특례 ※ 개인정보의 안전성 확보조치 기준 <제7조> 개인정보의 암호화		
과징금 및 벌칙	※ 개인정보보호법 <제24조제3항> 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손된 경우 (암호화 등 안전성 확보에 필요한 조치를 하지 않은 경우) 5억원 이하의 과징금 ※ 개인정보보호법 <제24조제3항> 고유식별번호에 대해 안전성 확보에 필요한 조치(암호화 등)를 하지 않은 경우 3천만원 이하의 과태료 ※ 개인정보 마스킹은 "개인정보 안전조치 의무"의 권장사항		

4.3.4 인증정보 및 고유식별정보와 같은 주요 개인정보 전송 시 안전하게 암호화하여 전송하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.3.4
중구분	개인정보의 암호화	**중요도**	H
항목 개요	주요 개인정보는 안전한 알고리즘으로 암호화하여, 외부 공인망으로 전송되는 인증정보/주요 개인정보에 대해서는 확인이 불가능 하도록 구성되어야 함.		
평가기준			
판단 기준	Y - 인증정보/고유식별정보 전송 시 안전한 수단을 통해 전송하고 있음 N - 인증정보/고유식별정보 전송 시 안전한 암호화 전송 수단이 마련되어 있지 않음 N/A - 전송 구간에 암호화 필요한 주요정보 없음		
점검 방법	▶ 인증정보 및 고유식별정보 전송 시 암호화 통신 적용 확인 ① 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신 여부 확인 - 인증정보(ID, Password) 및 고유식별정보와 같은 주요 개인정보 전송 시 외부망 및 사내망 모두 암호화 적용 필요		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 <제24조> 고유식별정보의 처리 제한 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보보호법 시행령 <제48조의2> 개인정보의 안전성 확보 조치에 관한 특례 ※ 개인정보의 안전성 확보조치 기준 <제7조> 개인정보의 암호화 ※ 개인정보의 기술적·관리적 보호조치기준 <제6조> 개인정보의 암호화		



<그림 61> 웹페이지 HTTPS 적용 예시

과징금 및 벌칙	※ 개인정보보호법 <제24조제3항> 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손된 경우 (암호화 등 안전성 확보에 필요한 조치를 하지 않은 경우) 5억원 이하의 과징금 ※ 개인정보보호법 <제24조제3항> 고유식별번호에 대해 안전성 확보에 필요한 조치 (암호화 등)를 하지 않은 경우 3천만원 이하의 과태료 ※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

4.3.5 암호키는 별도의 안전한 장소에 보관하고 접근권한을 최소화하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.3.5
중구분	개인정보의 암호화	**중요도**	**H**
항목 개요	암호화를 할 경우 사용되어지는 암호화 키는 분실의 위험이 없는 안전한 장소에 보관되어야 하고, 암호화 키에 대한 접근권한도 관련 업무자에 한하여 최소한으로 부여되어야 함		
평가기준			
판단 기준	Y - 암호키에 대한 접근권한이 최소화되어 있고, 안전하게 보관되고 있음 N - 암호키에 대한 접근권한이 최소화되어 있지 않거나, 안전한 보관이 이루어지고 있지 않음		
점검 방법	▶ 암호키 안전보관 확인 ① 생성된 암호키는 별도 매체에 저장 후 안전한 장소(소산 백업 포함)에 보관 ② DB 시스템 적용 시 암/복호화 키 노출 금지 확인 (또는 솔루션(응용프로그램)을 통해 관리자 개입없이 배포 여부 확인) - 암호키는 소스단에 하드코딩 되어 사용되면 안 됨 ③ 암호키를 Network 전송 시, 암호화 여부 확인 ▶ 암호키에 대한 접근권한 최소화 여부 확인		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보조치 ※ 개인정보의 안전성 확보조치 기준 <제7조> 개인정보의 암호화		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료		

4.4. 접속기록 및 접근권한 기록 보관 및 점검

<table>
<tr><th colspan="4">4.4.1 응용프로그램/서버/DB의 접속기록 및 작업기록을 1년 이상 보관하고 있습니까?</th></tr>
<tr><th colspan="4">항목구분</th></tr>
<tr><td>대구분</td><td>개인정보 기술적 보호조치</td><td>항목코드</td><td>4.4.1</td></tr>
<tr><td>중구분</td><td>접속기록 및 접근권한 기록 보관 및 점검</td><td>중요도</td><td>H</td></tr>
<tr><td>항목
개요</td><td colspan="3">응용프로그램/서버/DB의 접속기록을 1년 이상 안전하게 보관해야 함</td></tr>
<tr><th colspan="4">평가기준</th></tr>
<tr><td>판단
기준</td><td colspan="3">Y - 개인정보처리시스템의 모든 접속 및 작업기록을 1년 이상 보관함
P - 개인정보처리시스템의 접속 및 작업기록 일부만 1년 이상 보관하고 있음
N - 개인정보처리시스템의 모든 접속 및 작업기록을 1년 이상 보관하지 않고 있음</td></tr>
<tr><td>점검
방법</td><td colspan="3">▶ 접속기록 보관확인
① 개인정보처리시스템 접속기록 1년 또는 2년 이상 보관 여부 확인
- 접속기록 보관
접속기록 보관·관리 기준
<table>
<tr><th>구 분</th><th>개인정보처리자</th><th>정보통신서비스 제공자등</th></tr>
<tr><td rowspan="2">보관기간</td><td>최소 1년 이상</td><td>최소 1년 이상</td></tr>
<tr><td>※ 단, 5만명이상의 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 경우 최소 2년 이상</td><td>※ 단,「전기통신사업법」제5조에 따른 기간통신사업자의 경우 최소 2년 이상</td></tr>
<tr><td>점검주기</td><td colspan="2">월 1회이상</td></tr>
<tr><td rowspan="5">기록항목</td><td>계정</td><td>계정(식별자)</td></tr>
<tr><td>접속일시</td><td>접속일시</td></tr>
<tr><td>처리한 정보주체 정보</td><td>-</td></tr>
<tr><td>접속지 정보</td><td>접속지를 알 수 있는 정보</td></tr>
<tr><td>수행업무</td><td>수행업무</td></tr>
<tr><td>다운로드 사유확인</td><td>내부 관리계획 등으로 정하는 바에 따라, 다운로드 사유확인</td><td>-</td></tr>
</table>
※ 출처: 개발자 대상 개인정보 보호조치 적용 안내서
<그림 62> 접속기록 보관 관리 기준
- 개인정보처리시스템 접근 관리 대장 보유 여부 확인
② 각 개인정보처리시스템 표준시간 동기화 확인
※ 접속기록 보관절차 수립
① 보존이 필요한 접속기록과 대상시스템의 식별</td></tr>
</table>

	② 각 시스템 및 장비별 접속기록 형태 및 보존기간 정의 ③ 접속기록 보존(백업) 방법 등 검색조건문(쿼리) 예시 ·◌ '김'씨 성을 가진 회원을 조회하는 경우 - 정보주체의 정보 : SELECT * FROM student WHERE name LIKE '김%'; ※ name: 학생이름(컬럼), student: 학생정보(테이블) ·◌ 영화를 연간 50회 이상 관람한 고객에게 VIP 등급부여 - 정보주체의 정보 : UPDATE member SET membership='VIP' WHERE movie_count_per_year>=50; ※ member: 회원정보(테이블), membership: 고객정보(컬럼), movie_count_per_year: 연간 영화관람 건수 (컬럼) ※ 출처: 개발자 대상 개인정보 보호조치 적용 가이드(2020) **<표 7> 검색조건문(쿼리) 예시**
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보조치 ※ 개인정보의 안전성 확보조치 기준 <제8조> 접속기록의 보관 및 점검
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

<table>
<tr><th colspan="4">4.4.2 응용프로그램/서버/DB의 접속 및 작업기록에 대한 주기적 검토 및 관련 대응을 하고 있습니까?</th></tr>
<tr><th colspan="4">항목구분</th></tr>
<tr><td>대구분</td><td>개인정보 기술적 보호조치</td><td>항목코드</td><td>4.4.2</td></tr>
<tr><td>중구분</td><td>접속기록 및 접근권한 기록 보관 및 점검</td><td>중요도</td><td>H</td></tr>
<tr><td>항목
개요</td><td colspan="3">개인정보처리시스템 사용자의 접속기록을 주기적으로 검토하여 정보유출, 해킹 등의 보안사고 발생 여부를 확인해야 함</td></tr>
<tr><th colspan="4">평가기준</th></tr>
<tr><td>판단
기준</td><td colspan="3">Y - 접속 및 작업기록을 주기적으로 검토하고 이상징후 발견 시 관련 책임자에게 보고하고 있음
P - 접속 및 작업기록을 주기적으로 검토하고 있으나, 이상징후 발견 시 관련 책임자에게 보고 절차가 없음
N - 접속 및 작업기록을 비주기적 혹은 미 검토하고 있고, 이상징후 발견 시 관련 책임자에게 보고하지 않음</td></tr>
<tr><td>점검
방법</td><td colspan="3">▶ 접속 및 작업기록의 주기적 검토 및 대응여부 확인
① 사용자 접속 및 작업기록을 검토한 후 이상징후 여부 등 그 결과를 관련 책임자에게 보고
② 이상징후 발견 시 정보유출, 해킹 등 발생 여부를 확인하기 위한 절차를 수립하고 절차에 따라 대응 필요

※ 주기적 검토방법
- 검토대상: 사용자 접속기록을 검토할 중요정보 및 주요 정보시스템 선정
- 검토주기: 월 1회 이상
- 검토기준 및 방법: 업무목적 이외의 중요정보 과다처리(조회, 변경, 삭제 등), 업무시간 외 접속, 비정상적인 접속(미 승인 계정 접속 등)등의 기준 및 확인 방법 수립
- 검토 담당자 및 책임자 지정
- 이상징후 대응절차 등

※ 접속기록 내 비정상 행위 예시
- 계정: 접근권한이 부여되지 않은 계정으로 접속한 행위 등
- 접속일시: 출근시간 전, 퇴근시간 후, 새벽시간, 휴무일 등 업무시간 외 접속한 행위 등
- 접속지 정보: 인가되지 않은 단말기 또는 지역(IP)에서 접속한 행위 등
- 처리한 정보주체 정보: 특정 정보주체에 대하여 과도하게 조회, 다운로드 등의 행위 등
- 수행업무: 대량의 개인정보에 대한 조회, 정정, 다운로드, 삭제 등의 행위 등
- 그 밖에 짧은 시간에 하나의 계정으로 여러 지역(IP)에서 접속한 행위 등
<table><tr><td>구분</td><td>이상징후(임계치)</td></tr></table></td></tr>
</table>

	Critical | 심야시간 접근 사용자 (22:00~07:00) Major | 반복 접근 사용자 (日 10회 이상) Critical | 다수IP 사용자 (日 3개 이상) Major | 동일IP의 다수사용자-구성원 (日 3개 이상) Critical | 동일IP의 다수사용자-BP사 (日 1개 이상) Major | 다수 로그인 실패 사용자 (月 3회 이상 계정 잠김) Critical | 개인정보 과다조회자-구성원 (日 20회 이상) Critical | 개인정보 과다조회자-콜센터 (日 50회 이상) Critical | 개인정보 과다조회자-기타BP사 (日 10회 이상) **<표 8> 이상징후 적용기준 예시** ※ 보고서, 메일등을 통한 검토/보고 증적 확인
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보조치 ※ 개인정보의 안전성 확보조치 기준 <제8조> 접속기록의 보관 및 점검
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

<table>
<tr><th colspan="4">4.4.3 개인정보를 기준 이상으로 다운로드 한 경우 그 사유를 확인하고 있습니까?</th></tr>
<tr><th colspan="4">항목구분</th></tr>
<tr><td>대구분</td><td>개인정보 기술적 보호조치</td><td>항목코드</td><td>4.4.3</td></tr>
<tr><td>중구분</td><td>접속기록 및 접근권한 기록 보관 및 점검</td><td>중요도</td><td>H</td></tr>
<tr><td>항목
개요</td><td colspan="3">개인정보를 기준이상으로 다운로드 하는 경우 그 사유를 확인해야 함</td></tr>
<tr><th colspan="4">평가기준</th></tr>
<tr><td>판단
기준</td><td colspan="3">Y - 개인정보 다운로드 기준 수립 및 사유 확인
P - 개인정보 다운로드 기준이 수립되어 있지 않거나, 사유를 확인하지 않음
N - 개인정보 다운로드 기준이 수립되어 있지 않으며, 사유도 확인하지 않음
N/A - 개인정보 다운로드 기능이 존재하지 않음</td></tr>
<tr><td>점검
방법</td><td colspan="3">▶ 개인정보 다운로드 기능 존재 시 기준 수립 및 사유 확인
① 고객 개인정보 다운로드 기준 수립
- 평균 다운로드 건수 기준 수립
- 일정 횟수 or 건수 이상의 다운로드 발생 시 사유를 확인해야 할 필요성이 존재
② 월 1회 작업기록 검토 시 다운로드 기준 초과 내역에 대한 사유 확인
- 일정 횟수 이상의 다운로드 발생 시 사유 확인
- 다량의 개인정보 다운로드 시 사유를 입력하는 기능 추가 권고
<table><tr><th>예시</th></tr><tr><td>(다운로드 정보주체의 수) 통상적으로 개인정보 처리 건수가 일평균 20건 미만인 소규모 기업에서 개인정보취급자가 100명 이상의 정보주체에 대한 개인정보를 다운로드 한 경우 사유 확인
(일정기간 내 다운로드 횟수) 개인정보취급자가 1시간 내 다운로드한 횟수가 20건 이상일 경우 단시간에 수차례에 걸쳐 개인정보를 다운로드 한 행위에 대한 사유 확인
(업무시간 외 다운로드 수행) 새벽시간, 휴무일 등 업무시간 외 개인정보를 다운로드 한 경우 사유 확인
※ 특정 서비스의 경우 개인정보처리시스템 운영 부서가 자체적으로 다운로드 사유확인이 필요한 기준을 책정할 수 있음</td></tr></table><표 9> 다운로드 사유확인이 필요한 기준 책정 예시</td></tr>
<tr><td>관련
근거</td><td colspan="3">※ 개인정보보호법 <제29조> 안전조치의무
※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보조치
※ 개인정보의 안전성 확보조치 기준 <제8조> 접속기록의 보관 및 점검</td></tr>
</table>

과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

4.4.4 접속 및 작업기록에 대한 백업자료는 별도의 물리적인 저장 장치에 저장하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.4.4
중구분	접속기록 및 접근권한 기록 보관 및 점검	**중요도**	**H**
항목 개요	개인정보처리시스템(응용프로그램/서버/DB)의 접속/작업 로그에 대한 백업자료는 별도의 물리적인 저장 장치에 보관해야 함		
평가기준			
판단 기준	Y - 접속 및 작업기록에 대한 백업자료를 별도의 물리적인 저장 장치에 보관 P - 접속 및 작업기록을 백업하고 있으나 최근 한 달 이내 백업하지 않음 N - 접속 및 작업기록에 대한 백업자료를 별도의 물리적인 저장 장치에 보관하지 않음		
점검 방법	▶ 접속 및 작업기록 물리적 분리 보관 확인 ① 백업 자료는 별도의 물리적 공간에 저장 - 최초 접속기록 및 마지막으로 저장된 기록 일자와 항목 확인 (최근 한 달 이내 백업 기록 확인) ② 접근권한 부여 최소화		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제8조> 접속기록의 보관 및 점검 ※ 개인정보의 기술적 관리적 보호조치 기준<제5조> 접속기록의 위·변조방지		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금		

4.4.5 접근권한의 부여, 변경, 또는 말소한 내역을 3년이상 보관하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.4.5
중구분	접속기록 및 접근권한 기록 보관 및 점검	**중요도**	**H**
항목 개요	개인정보처리시스템에 대한 접근권한 부여, 변경, 말소 시 관련 내역을 3년 이상 보관해야 함 (단, 정보통신서비스제공자 등은 경우 최소 5년간 보관)		
평가기준			
판단 기준	Y - 접근권한 부여/변경/말소 내역 3년 이상 보관하고 있음 P - 접근권한 부여/변경/말소 내역 3년 이하로 보관하고 있음 N - 접근권한 부여/변경/말소 내역 보관하지 않고 있음 N/A - 접근권한 부여/변경/말소 내역 없음		
점검 방법	▶ 계정 및 권한의 부여, 변경, 회수 이력 기록의 보관기간 확인 ① 접근권한 부여, 변경, 또는 말소한 내역의 기록 최소 5년간 보관 ② 성명, 소속, 시스템별 계정명, 사용기간, 권한 등 ※ 접근권한에 대한 기록 예시 - 접근권한 신청 정보(신청자 또는 대리신청자, 신청일시, 신청 목적, 사용기간 등) - 접근권한 승인 정보(승인자, 승인/거부 여부, 사유 및 일시 등) - 접근권한 등록 정보: 등록자(승인자), 등록일, 등록 방법(결재시스템, 계정/권한 대장 등) - 접근권한 정보: 권한명, 권한 내용 등		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보조치 ※ 개인정보의 안전성 확보조치 기준 <제5조> 접근 권한의 관리 ※ 개인정보의 기술적 관리적 보호조치 기준<제5조> 접속기록의 위·변조방지 ※ 개인정보의 기술적·관리적 보호조치기준 <제4조> 접근통제 ※ 정보보호 및 개인정보보호 관리체계 인증 <2.5.1> 사용자 계정 관리		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료		

4.5. 개인정보처리시스템 운영보안

4.5.1 모든 보유자산에 대한 취약점 진단을 정기적으로 진행하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.5.1
중구분	개인정보처리시스템 운영보안	**중요도**	**H**
항목 개요	보유한 자산에 대한 주기적인 검토/갱신을 통해 자산의 누락을 방지하여야 함		
평가기준			
판단 기준	Y - 모든 자산에 대해 연 1회 이상 취약점 진단 수행 P - 자산현황이 일부 누락되어 있음 N - 1) 취약점 진단 미수행 자산 존재 2) 자산현황이 작성되지 않음		
점검 방법	▶ 자산현황에 대한 파악여부 확인 ① 자산현황을 최신화 하여 유지 및 관리하고 있는지 확인 - 자산내역(IP, Hostname 등) 변경 시 반영필요 ▶ 정기적 취약점 진단(OS, WEB, WAS, DB) 진행 여부 점검 ① 연도별 취약점 진단 보고서를 확인하여 정기적으로 진행 여부 확인		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보조치 ※ 정보통신망법 <제47조의4> 이용자의 정보보호 ※ 개인정보의 기술적·관리적 보호조치 기준<제5조> 접속기록의 위·변조방지 ※ 정보보호 및 개인정보보호 관리체계 인증 <2.11.2> 취약점 점검 및 조치		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료		

4.5.2 웹사이트에 중요 개인정보 노출되지 않고 있고, 웹사이트에 게시하여야 할 경우 게시절차를 수립·이행하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.5.2
중구분	개인정보처리시스템 운영보안	**중요도**	**H**
항목 개요	웹사이트에 공지 및 기타 글을 게시할 때 관련 게시절차가 존재하지 않을 경우 고유식별정보 및 기타 개인정보가 노출될 수 있음		
평가기준			
판단 기준	Y - 공개된 게시판에 고객 개인정보가 노출되지 않고 있으며, 웹사이트에 중요 개인정보를 주기적으로 점검하고 있음 N - 개인정보가 노출되고 있거나, 게시할 경우에 따른 게시절차가 존재하지 않음 N/A - 개인정보 게시하지 않음		
점검 방법	▶ 공개된 게시판에 고객 개인정보 노출 여부 확인 ① 중요 개인정보 게시절차 위반사항에 대한 주기적인 검토 ② 웹사이트에 중요 개인정보를 게시해야 할 경우 허가 및 게시절차를 수립·이행 ③ 중요 개인정보 노출 여부 주기적으로 확인 ※ 중요 개인정보: 주민등록번호, 계좌정보, 신용카드정보 등		
관련	※ 개인정보보호법 <제29조> 안전조치의무		

※ 출처: 한국인터넷진흥원 홈페이지 개인정보 노출방지 안내서

<그림 63> 개인정보 노출 예시

근거	※ 개인정보보호법 <제39조의10> 노출된 개인정보의 삭제·차단 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보조치 ※ 개인정보보호 시행령 <제48조의8> 노출된 개인정보의 삭제·차단 요청 기관 ※ 정보보호 및 개인정보보호 관리체계 인증 <2.10.3> 공개서버 보안
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

4.5.3 공개된 서비스(검색엔진)을 차단하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.5.3
중구분	개인정보처리시스템 운영보안	**중요도**	**H**
항목 개요	검색엔진은 인터넷에 공개된 홈페이지의 정보를 수집하여 홈페이지 이용자들이 원하는 정보를 쉽게 찾아주는 기능을 제공하나 이로 인해 내부의 중요 정보가 노출될 수 있음		
평가기준			
판단 기준	Y - 검색엔진 기능 차단하고 있으며, 구글 등 외부 포탈에 내부/고객 정보가 노출되지 않음 N - 검색엔진 기능 차단하고 있지 않거나, 구글 등 외부 포탈에 내부/고객 정보가 노출되고 있음 N/A - 내부망 전용 사이트이므로 해당사항 없음		
점검 방법	▶ 내부 정보가 담긴 페이지나 게시물, 개인정보의 노출을 방치하기 위한 검색엔진 차단 여부 확인 ① robot 설정이 되어 검색엔진으로부터 정보 노출을 차단하고 있는지 확인 ② 구글링 점검 등을 통해 내부 정보의 외부 게시 노출 여부 확인 (검색조건 : 'site: 대상 URL', 'inurl: 대상 URL' 등)		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 <제39조의10> 노출된 개인정보의 삭제·차단 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보조치		

※ 출처: 한국인터넷진흥원 홈페이지 개인정보 노출방지 안내서

<그림 64> 검색엔진 노출 예시

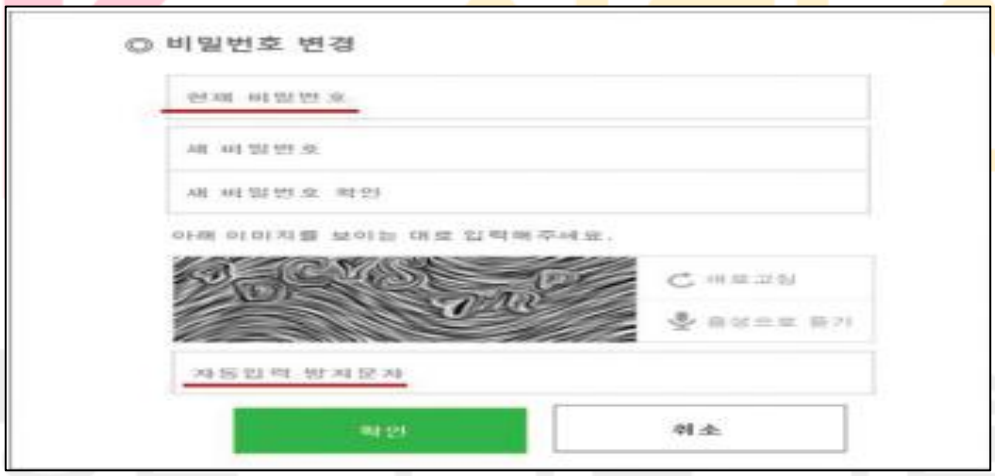
	※ 개인정보보호 시행령 <제48조의8> 노출된 개인정보의 삭제·차단 요청 기관 ※ 개인정보의 안전성 확보조치 기준 <제6조> 접근통제
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

4.5.4 서버에 백신이 설치되어 있고, 주기적으로 업데이트를 실시하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.5.4
중구분	개인정보처리시스템 운영보안	**중요도**	**H**
항목 개요	서버용 백신을 설치하여 정보유출, 악성프로그램 유입 등을 방지하여야 함		
평가기준			
판단 기준	Y - 백신이 설치되어 있으며 최신 업데이트 실시 및 주기적 점검 수행 P - 백신이 설치되어 있으나 업데이트 및 주기적 점검을 미수행 N - 백신이 설치되어 있지 않음 N/A - Windows 서버가 아님		
점검 방법	▶ 서버 백신 운영현황 확인 ① 백신소프트웨어 설치 여부 확인 - Windows Server는 필수 ② 최신 업데이트 적용 여부 확인 ③ 주기적인(월 1회 이상) 점검 여부 확인		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제9조> 악성프로그램 등 방지 ※ 개인정보의 기술적·관리적 보호조치기준 <제7조> 악성프로그램 방지		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료		

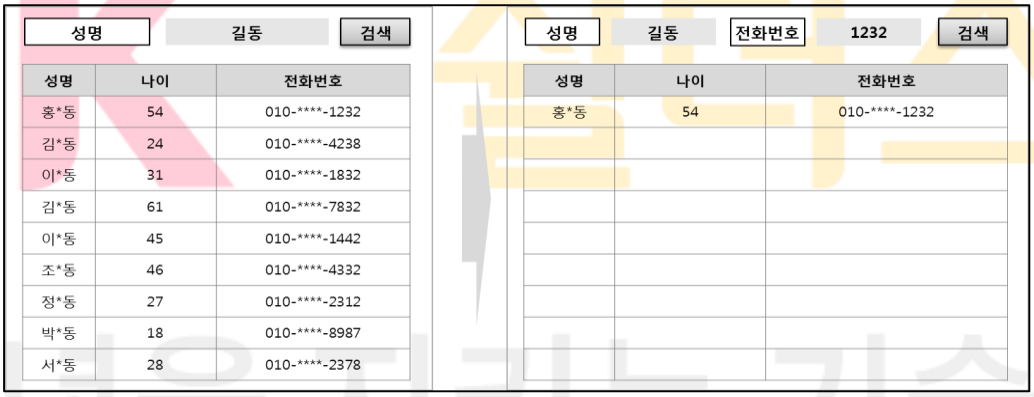
<table>
<tr><th colspan="4">4.5.5 개인정보 화면조회 및 출력물에 대한 보호조치(마스킹 등)를 하고 있습니까?</th></tr>
<tr><th colspan="4">항목구분</th></tr>
<tr><td>대구분</td><td>개인정보 기술적 보호조치</td><td>항목코드</td><td>4.5.5</td></tr>
<tr><td>중구분</td><td>개인정보처리시스템 운영보안</td><td>중요도</td><td>H</td></tr>
<tr><td>항목
개요</td><td colspan="3">개인정보의 처리 시 마스킹 등의 기술을 통해 개인정보의 표시를 제한하여야 함</td></tr>
<tr><th colspan="4">평가기준</th></tr>
<tr><td>판단
기준</td><td colspan="3">Y - 개인정보 화면조회 및 출력물 보호조치 수행
P - 개인정보 화면조회 및 출력물 보호조치는 미 수행하였으나, 우 클릭 방지/드래그 방지 적용
N - 개인정보 화면조회 및 출력물 보호조치 미수행
N/A - 화면조회 및 출력물에 개인정보 미포함</td></tr>
<tr><td>점검
방법</td><td colspan="3">▶ 개인정보의 화면조회 및 출력물 보호조치 적용 확인
① 화면 출력 시 보호조치(마스킹 등) 적용여부 확인
② 개인정보 출력물 보호조치(마스킹 등) 적용여부 확인
③ 서비스 운영 상 마스킹 적용이 불가할 경우 우 클릭 방지/드래그 방지 적용
<table><tr><th>개인정보</th><th>설명</th><th>예시</th></tr><tr><td>성명</td><td>성명 중 이름의 첫 번째 글자 이상</td><td>홍*동</td></tr><tr><td>주민번호</td><td>뒤에서부터 6자리</td><td>711231-1******</td></tr><tr><td>여권번호</td><td>뒤에서부터 4자리</td><td>12345****</td></tr><tr><td>연락처</td><td>전화번호 또는 휴대폰 뒤 4자리</td><td>010-1234-****</td></tr><tr><td>카드번호</td><td>7번째에서 12번째 자리</td><td>9430-82**-****-2393</td></tr><tr><td>계좌번호</td><td>뒤에서부터 5자리</td><td>430-20-1*****</td></tr></table>※ 출처: 개발자 대상 개인정보 보호조치 적용 가이드
<그림 65> 개인정보 출력 보호조치 방법 예시
※ 마스킹 처리는 화면상 출력되는 개인정보의 과도한 유출을 방지하기 위해, 화면상 리스팅 되는 내역 중 개인정보가 포함되어 있을 경우 처리되어야 함.
▶ 출력물 보호조치 확인
① 워터마크 적용 확인
② 응용프로그램에서 개인정보 출력 시 이력 조회가 되는지 확인</td></tr>
<tr><td>관련
근거</td><td colspan="3">※ 개인정보의 기술적 관리적 보호조치 기준<제10조> 개인정보 표시 제한 보호조치</td></tr>
<tr><td>과징금</td><td colspan="3">※ "개인정보 안전조치 의무"를 위한 기술적 보호조치 권장사항</td></tr>
</table>

및 벌칙	

4.5.6 표시 제한 해제 기능을 가지고 있고, 표시 제한 해제 시 로그생성 및 검토가 이루어지고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.5.6
중구분	개인정보처리시스템 운영보안	**중요도**	**M**
항목 개요	마스킹 된 개인정보를 해제하여 조회할 경우 해당 행위에 대한 승인절차와 기록을 통해 이를 검증, 확인하여야 함		
평가기준			
판단 기준	Y - 표시 제한 해제 권한을 적절하게 부여하고, 로그생성 및 주기적인 검토 수행 P - 표시 제한 해제 권한을 적절하게 부여하고, 로그생성이 이루어지고 있으나 주기적인 검토 미수행 N - 표시 제한 해제 권한의 부적절한 부여, 로그생성 및 주기적인 검토 미수행 N/A - 표시제한이 필요한 개인정보가 없음		
점검 방법	▶ 표시 제한된 개인정보에 대한 해제 내역 검토 확인 ① 개인정보(고유식별정보 등)의 표시 제한 해제 기능 확인 - 표시 제한 해제 권한의 발급 절차 및 관리여부 확인 ② 표시 제한 해제 시 로그 저장 및 주기적 검토 여부 확인		
관련 근거	※ 정보보호 및 개인정보보호 관리체계 인증 <3.2.3> 개인정보 표시제한 및 이용 시 보호조치		
과징금 및 벌칙	※ "개인정보 안전조치 의무"를 위한 기술적 보호조치 권장사항		

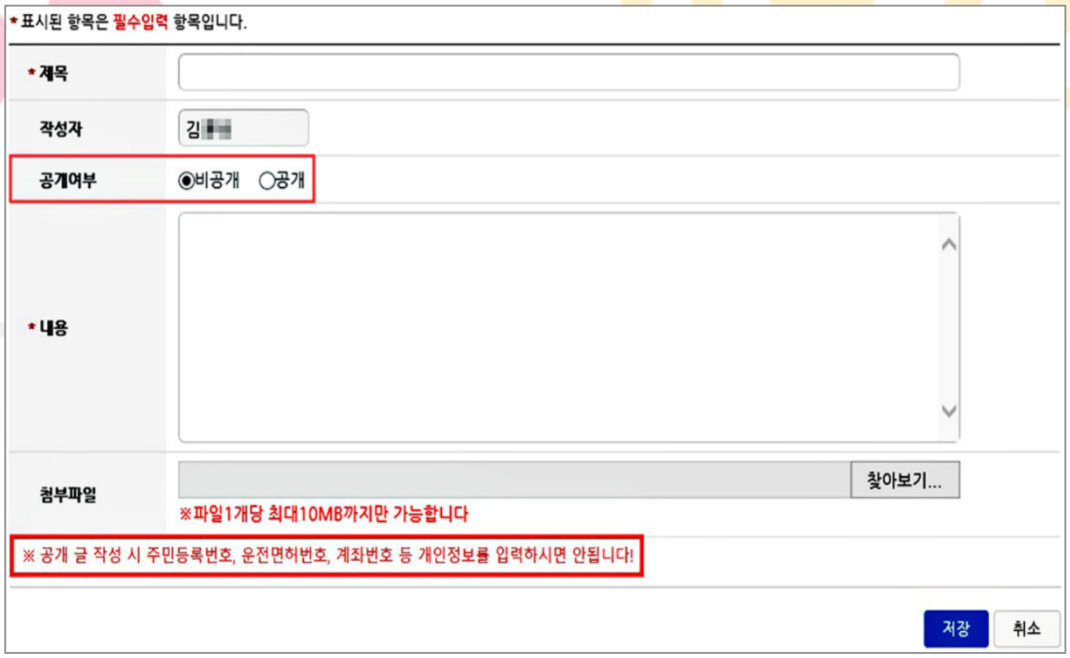
4.5.7 정보주체가 중요정보 조회 시 비밀번호 재확인 등의 추가 인증 수단이 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.5.7
중구분	개인정보처리시스템 운영보안	**중요도**	M
항목 개요	마스킹 된 개인정보를 해제하여 조회할 경우 해당 행위에 대한 승인절차와 기록을 통해 이를 검증, 확인하여야 함		
평가기준			
판단 기준	Y - 정보주체의 중요정보 변경 조회 시 비밀번호 재확인하고 있음 N - 정보주체의 중요정보 변경 조회 시 비밀번호 재확인하고 있지 않음 N/A - 주요 개인정보 없음		
점검 방법	▶ 정보주체 중요정보 조회 시 비밀번호 재확인 여부 확인 ① 주요 개인정보(고유식별정보, 민감정보, 금융정보)를 조회할 경우 비밀번호나 본인여부 재확인 여부 ② 비밀번호 변경 시 비밀번호 재입력 또는 자동입력 방지 문자(캡쳐) 적용 유무  ※ 출처: 개인정보영향평가 수행안내서 **<그림 66> 중요정보 변경 예시**		
관련 근거	※ 개인정보 영향평가 수행 안내서 <4.1.3> 추가인증 확인		
과징금 및 벌칙	※ "개인정보 안전조치 의무"를 위한 기술적 보호조치 권장사항		
4.5.8 응용프로그램을 통한 개인정보 검색 시 일치검색(equal검색)이나 두가지 조건 이상의			

검색조건을 사용하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.5.8
중구분	개인정보처리시스템 운영보안	**중요도**	M
항목 개요	응용프로그램을 통한 개인정보 검색 시 필요한 정보 외의 정보의 노출을 방지하여야 함		
평가기준			
판단 기준	Y - 일치검색(equal검색)이나 두가지 조건 이상의 검색조건 사용 N - 일치검색(equal검색)이나 두가지 조건 이상의 검색조건 미 적용 N/A - 1) 개인정보 검색기능이 존재하지 않음 2) 개인정보가 모두 마스킹 되어 있음		
점검 방법	▶ 응용프로그램(Web, App, C/S 등) 통한 개인정보 검색 시 보호조치 적용 확인 ① 일치검색(equal검색)이나 두가지 조건 이상의 검색조건을 사용 ex) 두가지 조건 이상의 검색조건 : 이름, 생년월일로 검색		
관련 근거	※ 정보보호 및 개인정보보호 관리체계 인증 <3.2.3> 개인정보 표시제한 및 이용 시 보호조치		
과징금 및 벌칙	※ "개인정보 안전조치 의무"를 위한 기술적 보호조치 권장사항		



<그림 67> 검색조건 변경 예시

4.5.9 게시판에 경고문구를 게재하여 고객이 글 작성 전 확인하게 하고, 본인만 확인/삭제 가능하게 구성되어 있습니까?

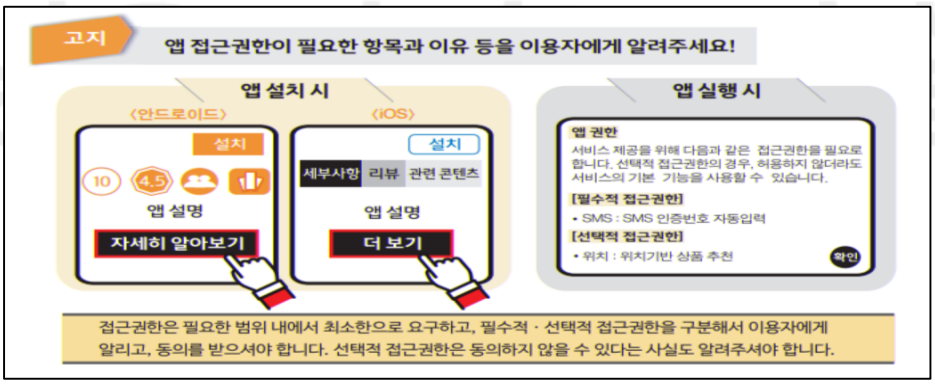
<table>
<tr><th colspan="4">항목구분</th></tr>
<tr><td>대구분</td><td>개인정보 기술적 보호조치</td><td>항목코드</td><td>4.5.9</td></tr>
<tr><td>중구분</td><td>개인정보처리시스템 운영보안</td><td>중요도</td><td>M</td></tr>
<tr><td>항목
개요</td><td colspan="3">게시판 이용자가 개인정보를 직접 게시할 경우 발생할 수 있는 개인정보 노출에 대한 보호조치가 되어야 함</td></tr>
<tr><th colspan="4">평가기준</th></tr>
<tr><td>판단
기준</td><td colspan="3">Y - 게시판에 경고문구가 게재되고, 본인만 확인/삭제 가능
P - 게시판에 경고문구가 미 게재되거나, 타인에 의한 접근 가능
N - 게시판에 경고문구가 미 게재되고, 타인에 의한 접근 가능</td></tr>
<tr><td>점검
방법</td><td colspan="3">▶ 게시판 보호조치 확인
① 게시판(회원/비회원 용)에 경고문구(예시: "개인정보의 포함 유무 확인 및 개인정보 노출로 인한 피해") 게재 확인
② 게시물에 대해 본인만 확인/삭제할 수 있게 설정여부 확인 (비밀 글 등)
- 이용자가 게시한 게시물을 삭제할 수 있도록 구현 확인
이용자 스스로 삭제하지 못하는 경우, 자기 게시물 접근배제 요청 시 고객센터 등을 통한 접수/처리 절차 수립/운영 되고 있는지 확인
 

※ 출처: 홈페이지 개인정보 노출방지 안내서
<그림 68> 개인정보 게시에 대한 주의 안내 예시</td></tr>
<tr><td>관련
근거</td><td colspan="3">※ 정보통신망법 <제44조의5> 게시판이용자의 본인확인
※ 홈페이지 개인정보 노출방지 가이드라인</td></tr>
</table>

과징금 및 벌칙	※ "개인정보 안전조치 의무"를 위한 기술적 보호조치 권장사항

4.6. Mobile 기기의 소프트웨어관리

4.6.1 Mobile 기기의 소프트웨어가 접근하는 권한의 관련 고지를 띄우고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.6.1
중구분	Mobile 기기의 소프트웨어관리	**중요도**	H
항목 개요	Mobile 기기(Smart Phone, Tablet 단말 등)의 소프트웨어가 접근하는 권한에 대해서 이용자들이 인지할 수 있게 고지하여야 함		
평가기준			
판단 기준	Y - Mobile 기기의 소프트웨어의 최초 설치 혹은 실행 시 접근권한에 대해 고지하고 있음 P - Mobile 기기의 소프트웨어의 최초 설치 혹은 실행 시 접근권한에 대해 일부만 고지하고 있음 N - Mobile 기기의 소프트웨어의 최초 설치 혹은 실행 시 접근권한에 대해 고지하지 않음 N/A - Mobile 기기 소프트웨어가 존재하지 않음		
점검 방법	▶ Mobile 기기(Smart Phone, Tablet 단말 등)의 소프트웨어의 최초 설치 혹은 실행 시 접근권한에 대해 고지하는지 확인 ① (앱 설치 시) 이용자는 앱 마켓에서 설치하려는 앱을 검색한 후, '자세히 알아보기(구글 플레이)', '설명→더보기(애플 앱스토어)' 또는 별도 접근권한 안내창* (원스토어)'란 등에서 상기 고지 내용을 확인 ※ 별도 접근권한 안내창은 안드로이드 6.0 미만 버전의 경우에 해당함 ② (앱 실행 시) 서비스를 최초로 이용하고자 할 때, 팝업 창 등을 통해 앱이 접근하려는 정보와 기능에 대한 고지 내용을 확인		



※ 출처: 방송통신위원회 스마트폰 앱 접근권한 개인정보보호 안내서

<그림 69> 접근권한 고지 예시

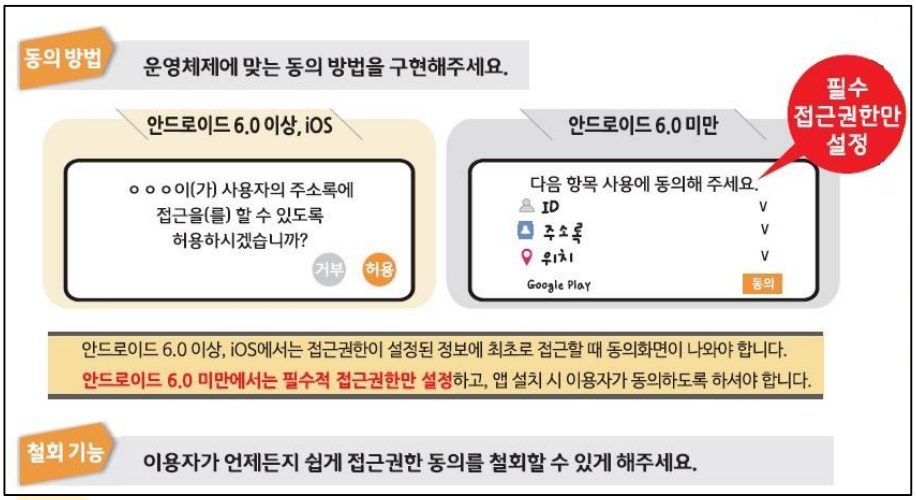
③ 필수적/선택적 접근권한 구분 시 필요한 항목 확인

가. 필수적 접근권한

- 접근권한이 필요한 정보 및 기능의 항목

	- 해당 정보 및 기능이 필요한 이유 나. 선택적 접근권한 - 접근권한이 필요한 정보 및 기능의 항목 - 해당 정보 및 기능이 필요한 항목 - 접근권한 허용에 동의하지 않을 수 있다는 사실
관련 근거	※ 정보통신망법 <제22조의2> 접근권한에 대한 동의 ※ 정보통신망법 시행령 <제9조의2> 접근권한의 범위 등 ※ 스마트폰 앱 개인정보보호 가이드라인
과징금 및 벌칙	※ 정보통신망법 <제22조의2제3항> 동의 및 철회방법을 마련하는 등 이용자 정보보호를 위하여 필요한 조치를 하지 않은 경우 3천만원 이하 과태료

4.6.2 Mobile 기기의 소프트웨어가 접근하는 정보에 대해서 필수권한, 선택권한으로 구분하여 동의를 받고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.6.2
중구분	Mobile 기기의 소프트웨어관리	**중요도**	**H**
항목 개요	Mobile 기기(Smart Phone, Tablet 단말 등)의 소프트웨어 사용 시 필요한 필수권한과 선택권한을 구분하여야 함		
평가기준			
판단 기준	Y - Mobile 기기의 소프트웨어의 접근권한이 필수 및 선택항목으로 구분되어 있으며, 이에 대한 동의·철회 기능이 구현되어 있음 N - Mobile 기기의 소프트웨어의 접근권한이 필수 및 선택항목으로 구분되어 있지 않거나, 이에 대한 동의·철회 기능이 구현되어 있지 않음 N/A - Mobile 기기 소프트웨어가 존재하지 않음		
점검 방법	▶ 필수권한, 선택권한 구분하여 동의 받는지 확인 ① 필수권한 미 동의 시 서비스 사용 불가 ② 선택권한 미 동의 시 서비스는 사용 가능하고, 미 동의한 정보 관련 기능만 사용 불가 ③ (설치한 앱 실행) 접근권한별 동의 내역 확인 - 앱 설치 또는 실행 시 앱이 접근하려는 정보 내용과 해당 앱의 설정 및 제어와 동일한지 확인 ※ Mobile 기기의 소프트웨어는 운영체제가 제공하는 범위 내에서 접근하는 정보에 대해서 동의·철회 기능이 구현되어야 함. ※ 애플(iOS)와 안드로이드 마시멜로(6.0) 이상은 운영체제 단에서 선택동의 기능을 제공하나, 안드로이드 마시멜로(6.0) 이하는 제공하지 않음. 이 경우는 필수적 접근권한만 설정하여 앱 설치 시 또는 최초 실행과정에서 이용자에게 알리고 동의 여부를 결정하게 구성해야 함.		

<table>
<tr><td></td><td> 

※ 출처: 방송통신위원회 스마트폰 앱 접근권한 개인정보보호 안내서
<그림 70> 동의 방법 및 철회 기능</td></tr>
<tr><td>관련 근거</td><td>※ 정보통신망법 <제22조의2> 접근권한에 대한 동의
※ 정보통신망법 시행령 <제9조의2> 접근권한의 범위 등
※ 스마트폰 앱 개인정보보호 가이드라인</td></tr>
<tr><td>과징금 및 벌칙</td><td>※ 정보통신망법 <제22조의2제3항> 동의 및 철회방법을 마련하는 등 이용자 정보보호를 위하여 필요한 조치를 하지 않은 경우 3천만원 이하 과태료</td></tr>
</table>

4.6.3 필수권한 거절/철회 시 서비스 사용이 불가하고, 선택권한 동의 거절/철회 시 서비스를 정상 제공하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.6.3
중구분	Mobile 기기의 소프트웨어관리	**중요도**	**H**
항목 개요	Mobile 기기의 소프트웨어 사용 시 필수권한 미 동의 시 서비스가 제공되지 않고 선택권한 미 동의 시에는 관련 기능만 제공이 안되고 타 서비스 기능은 제공되어야 함		
평가기준			
판단 기준	Y - Mobile 기기의 소프트웨어의 필수권한 미 동의 시 서비스 제공이 불가하며, 선택권한 동의 거절/철회 시 서비스를 정상제공 하고 있음 N - Mobile 기기의 소프트웨어의 필수권한 미 동의 시 서비스 제공이 가능하거나, 선택권한 동의 거절/철회 시 서비스를 정상제공 하지 않고 있음 N/A - Mobile 기기 소프트웨어가 존재하지 않음		
점검 방법	▶ 필수권한에 대해서는 동의 거절/철회 시 서비스 실행이 불가하고, 선택권한에 대해서는 동의 거절/철회 시 해당 기능만 사용되지 않고, 기타 기능은 정상 사용되어야 함. ※ Mobile 기기의 소프트웨어는 운영체제가 제공하는 범위 내에서 접근하는 정보에 대해서 동의·철회 기능이 구현되어야 함.		
관련 근거	※ 정보통신망법 <제22조의2> 접근권한에 대한 동의 ※ 스마트폰 앱 개인정보보호 가이드라인		
과징금 및 벌칙	※ 정보통신망법 <제22조의2제2항> 반드시 필요하지 아니한 접근권한을 설정하는데 이용자가 동의하지 아니한다는 이유로 해당 서비스의 제공을 거부하는 경우 3천만원 이하 과태료		

4.6.4 필수권한과 선택권한은 해당 서비스에 적절합니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.6.4
중구분	Mobile 기기의 소프트웨어관리	**중요도**	**H**
항목 개요	개인정보 수집 시 각 권한은 해당상품의 서비스 특성을 고려한 합리적인 범위 내로 수집해야 함		
평가기준			
판단 기준	Y - Mobile 기기의 소프트웨어의 필수/선택권한이 합리적으로 선정되어 있음 N - Mobile 기기의 소프트웨어의 필수/선택권한에 불필요한 권한이 포함되어 있음 N/A - Mobile 기기 소프트웨어가 존재하지 않음		
점검 방법	▶ 불필요한 필수/선택권한 수집여부 확인 ① 이용약관·개인정보 처리방침 등에 공개된 해당 서비스의 범위 ② 실제 제공하는 서비스 ③ 해당 서비스에 대한 이용자의 합리적 예측 가능성 ④ 해당 서비스와 접근권한의 기술적 관련성		
관련 근거	※ 정보통신망법 <제22조의2> 접근권한에 대한 동의 ※ 정보통신망법 시행령 <제9조의2> 접근권한의 범위 등 ※ 스마트폰 앱 개인정보보호 가이드라인		
과징금 및 벌칙	※ 정보통신망법 <제22조의2제3항> 동의 및 철회방법을 마련하는 등 이용자 정보보호를 위하여 필요한 조치를 하지 않은 경우 3천만원 이하 과태료		

4.6.5 Mobile 기기의 소프트웨어를 삭제하여도 개인정보가 서비스 사업자에게 남아있을 경우, 이를 정보주체에게 알리고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.6.5
중구분	Mobile 기기의 소프트웨어관리	**중요도**	**H**
항목 개요	Mobile App을 삭제하여도 회원탈퇴 등의 별도 요청이 필요함을 개인정보 처리방침에 명시하여야 함		
평가기준			
판단 기준	Y - Mobile 기기의 소프트웨어 삭제 시 별도 요청 필요사항 명시함 N - Mobile 기기의 소프트웨어 삭제 시 별도 요청 필요사항 명시하지 않음 N/A - 1) Mobile 기기 소프트웨어가 존재하지 않음 2) 삭제가 필요한 개인정보 없음		
점검 방법	▶ Mobile 기기의 소프트웨어 삭제 시 별도 요청 필요사항 명시여부 확인 ① 개인정보 처리방침 등에 내 App을 삭제하더라도 회원탈퇴 등 별도 요청해야 한다는 내용을 명시하고 있는지 확인 제5조(개인정보의 분리보관 또는 파기) ① SK쉴더스는 개인정보 수집 및 이용목적이 달성된 후에는 해당 정보를 지체 없이 파기합니다. 단, 분쟁 해결, 민원처리, 법령상 의무이행 및 리스크 관리업무 등을 위하여 개인정보의 보존이 필요한 경우에는 다른 정보주체의 개인정보와 분리하여 별도로 저장·관리 할 수 있습니다. ② SK쉴더스는 개인정보가 기록된 출력물, 서면 등은 파쇄 또는 소각의 방법으로 파기하고, 전자적 파일형태의 개인정보는 복원이 불가능한 방법으로 영구 삭제하는 방법으로 파기합니다. ③ 설치된 모바일 어플리케이션을 삭제하더라도 실제 개인정보는 회사가 보유하고 있으며, 개인정보의 삭제를 원하는 경우 별도의 회원탈퇴 또는 개인정보 수집, 이용동의 철회 과정이 필요합니다. ④ [illegible] 30일내에로그인(log in)하지 않을 경우 App의사용권한을해지합니다. **<그림 71> Mobile App 삭제 시 별도요청 필요 예시** 개인정보처리방침 상세 문구 설치된 모바일 어플리케이션을 삭제하더라도 실제 개인정보는 회사가 보유하고 있으며, 개인정보의 삭제를 원하는 경우 별도의 회원탈퇴 또는 개인정보 수집, 이용동의 철회 과정이 필요합니다.		
관련 근거	※ 정보통신망법 <제22조의2> 접근권한에 대한 동의 ※ 정보통신망법 시행령 <제9조의2> 접근권한의 범위 등 ※ 스마트폰 앱 개인정보보호 가이드라인		
과징금 및 벌칙	※ 정보통신망법 <제22조의2제3항> 동의 및 철회방법을 마련하는 등 이용자 정보보호를 위하여 필요한 조치를 하지 않은 경우 3천만원 이하 과태료		

4.6.6 가입해지 또는 동의철회를 쉽게 할 수 있도록 Mobile 기기의 소프트웨어 내에 탈퇴 또는 동의철회 메뉴를 구성하고 있는가?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.6.6
중구분	Mobile 기기의 소프트웨어관리	**중요도**	**H**
항목 개요	Mobile App 이용자가 쉽게 가입해지 또는 동의철회 할 수 있도록 탈퇴 또는 동의철회 메뉴를 구성하고 있어야 함.		
평가기준			
판단 기준	Y - Mobile 기기 소프트웨어 내에 가입해지 및 동의철회 메뉴가 쉽게 찾을 수 있음 N - Mobile 기기 소프트웨어 내에 가입해지 및 동의철회 메뉴가 없음 N/A - Mobile 기기 소프트웨어가 존재하지 않음		
점검 방법	▶ Mobile 기기의 소프트웨어 가입해지 또는 동의철회 메뉴 존재확인 ① 이용자가 쉽게 탈퇴 또는 동의철회 메뉴를 찾을 수 있도록 2 Depth 이내에 배치하고, 개인정보 처리방침에 연락 가능한 연락처를 명시하여야 함		
관련 근거	※ 정보통신망법 <제22조의2> 접근권한에 대한 동의 ※ 정보통신망법 시행령 <제9조의2> 접근권한의 범위 등 ※ 스마트폰 앱 개인정보보호 가이드라인		
과징금 및 벌칙	※ 정보통신망법 <제22조의2제3항> 동의 및 철회방법을 마련하는 등 이용자 정보보호를 위하여 필요한 조치를 하지 않은 경우 3천만원 이하 과태료		

4.7. 개인정보취급자 단말보안

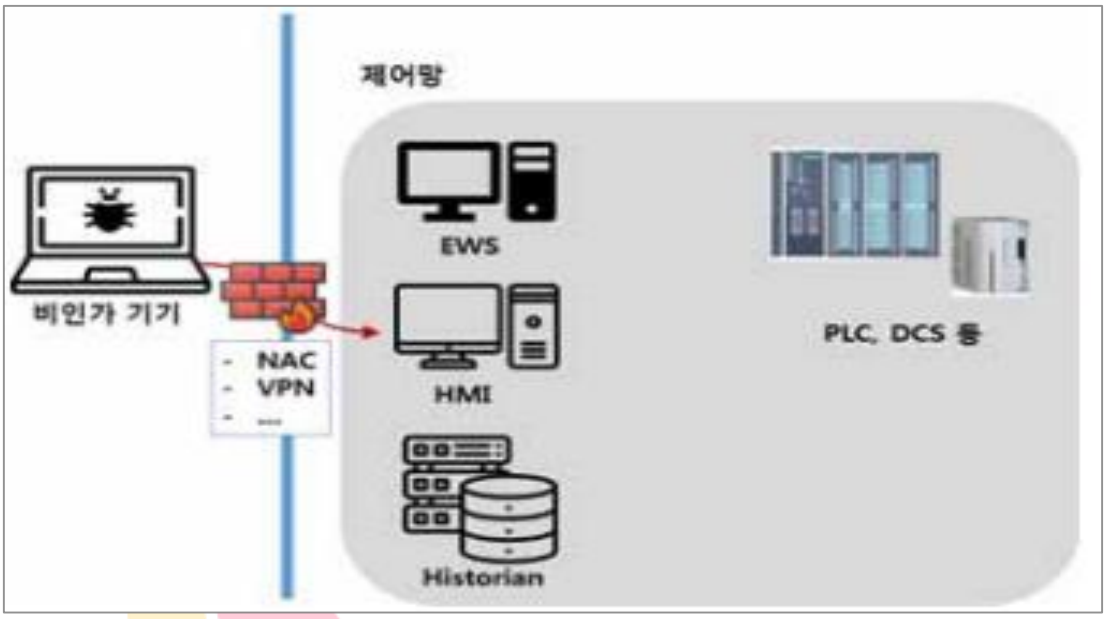
4.7.1 개인정보취급자 단말에 최신 보안 패치가 적용되고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.7.1
중구분	개인정보취급자 단말보안	**중요도**	**H**
항목 개요	개인정보취급자 단말에는 최신 보안 패치의 적용을 통해 악성코드 유입, 알려진 취약점을 통한 공격 등에 대비하여야 함		
평가기준			
판단 기준	Y - 단말에 최근 1개월내의 보안 패치가 적용되어 있음 N - 단말에 최근 1개월내의 보안 패치가 적용되어 있지 않음		
점검 방법	▶ 개인정보취급자 단말 최신 보안 패치 적용여부 확인 ① 주기적인 보안 패치 적용 확인(월 1회 이상)  **<그림 72> 단말 최신 보안패치 예시**		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제10조> 관리용 단말기의 안전조치		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료		

4.7.2 단말에 최신 업데이트된 백신이 설치되어 있고, 주기적으로 검사를 실시하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.7.2
중구분	개인정보취급자 단말보안	**중요도**	**H**
항목 개요	개인정보처리시스템 서버에 서버용 백신이 설치하여 정보유출, 악성프로그램 유입 등을 방지하여야 함		
평가기준			
판단 기준	Y - 백신이 설치되어 있으며 최신 업데이트 실시, 실시간 감시기능 사용, 주기적 점검 수행 P - 최신 업데이트 실시, 실시간 감시기능 사용, 주기적 점검 중 일부 미수행 N - 1) 백신에 대한 업데이트, 실시간 감시기능, 주기적 점검을 실시하지 않음 2) 백신이 설치되어 있지 않음		
점검 방법	▶ 개인정보취급자단말 백신 운영현황 확인 ① 백신소프트웨어 설치 여부 확인. ② 최신 업데이트 적용 여부 확인 ③ 월 1회 이상 주기적 점검 확인 ④ 실시간 감시기능 활성화 여부 확인		
관련	※ 개인정보보호법 <제29조> 안전조치의무		

<그림 73> 백신 자동업데이트 설정 예시

근거	※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제9조> 악성프로그램 등 방지
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

4.7.3 비인가 단말이 내부 네트워크(업무망)에 접속하지 못하도록 하는 방안이 적용되어 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.7.3
중구분	개인정보취급자 단말보안	**중요도**	**H**
항목 개요	취급자 단말기(단말, 모바일기기, 관리용 단말기 등)가 개인정보 처리시스템 네트워크에 접근이 가능할 경우, 단말기를 통한 개인정보 처리시스템의 감염이 발생할 수 있음		
평가기준			
판단 기준	Y - 취약한 단말의 네트워크 접근 제한 적용 N - 취약한 단말의 네트워크 접근 제한 미 적용		
점검 방법	▶ 내부 네트워크 접근을 위한 네트워크 통제 솔루션 운영 확인 ① 내부 네트워크 사용 시 IP를 통제할 수 있는 방법을 사용하는지 확인 ② (NAC 부재 시) 외부자 PC를 내부망에 연결하기 전에 담당자가 PC의 안전조치 여부를 확인하는 절차가 있으면 양호 - 필수보안 S/W 설치 여부(백신, 문서보안, 이글아이 등) - OS, 상용 프로그램 최신 업데이트 적용 여부 - 무선 네트워크 사용 신청 절차에 따른 접속 등 ※ 점검 확인 사항 - AD정책, NAC 등의 정책 - 내부 네트워크 접근통제방안 지침 - 보안솔루션(NAC 등) 차단 정책 - 네트워크장비 IP/MAC 필터링 설정 정책 - 무선 네트워크 사용 신청 및 승인 내역		

	 ※ 출처: 주요통신기반시설 기술적 취약점 분석 평가 방법 상세가이드 **<그림 74> 네트워크 접근통제 구성**
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

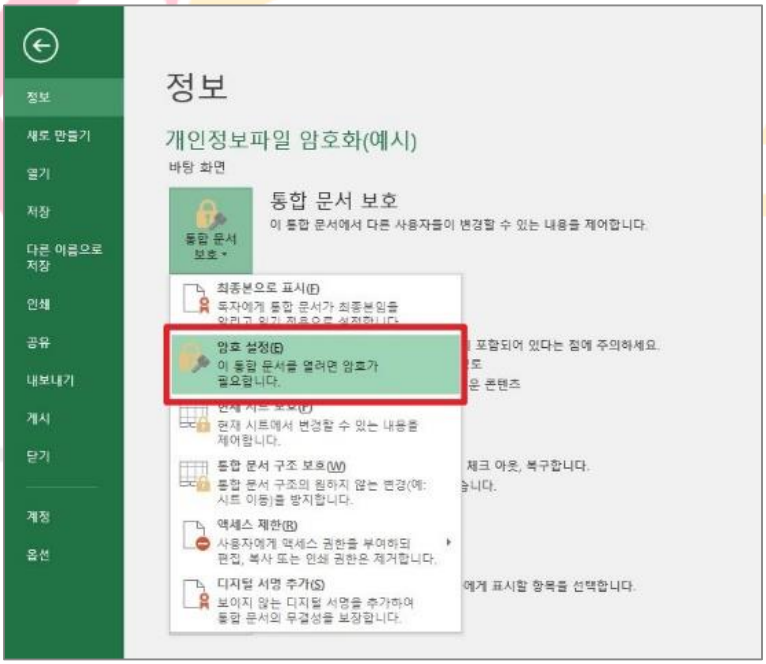
4.7.4 취급자 단말에 유해 사이트(성인, 오락 등) 통제가 되어 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.7.4
중구분	개인정보취급자 단말보안	**중요도**	**H**
항목 개요	취급자 단말에서 유해 사이트에 접근이 가능할 경우, 바이러스 감염, 유해 소프트웨어 설치 등의 2차 피해가 발생할 수 있음		
평가기준			
판단 기준	Y - 유해 사이트 차단 정책이 적용되어 있음 N - 유해 사이트 차단 정책이 적용되어 있지 않음 N/A - 인터넷 접속 불가함		
점검 방법	▶ 취급자 단말의 인터넷 접속정책 수립·이행 여부 확인 ① 정보 유출 가능 사이트(웹하드, P2P, 웹메일, 드라이브 등) 접속 차단 정책 ② 유해사이트(성인, 오락 등) 접속 차단 정책 ③ 이메일, 인터넷 사이트의 접속, 소프트웨어 다운로드 및 전송 등의 사용자 접속정책 ④ 인터넷 연결 시 네트워크 구성 정책 ⑤ 인터넷 접속내역 검토(모니터링) 정책 등		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제6조> 접근통제		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료		

ACL_15	전체	INTERNAL	차단사이트 바이러스공격 북한차단IP	ALL	none	ANY	Deny							
ACL_16	전체	INTERNAL	차단사이트_추가	ALL	none	ANY	Deny							
ACL_17	전체	INTERNAL	불법사이트 차단사이트추가1	ALL	none	ANY	Deny							
ACL_18	전체	INTERNAL	차단사이트추가2 증권사이트	ALL	none	ANY	Deny							
↳ 설명: 20110304_DDoS_상용메일														
ACL_19	전체	INTERNAL	차단사이트추가3 상용클라우드	ALL	none	ANY	Deny							
ACL_20	전체	INTERNAL	원격제어사이트	HTTPS NateOn HTTP	none	ANY	Deny							
ACL_21	전체	INTERNAL	모바일사이트	ALL	none	ANY	Deny							
ACL_22	전체	INTERNAL	P2P	ALL	none	ANY	Deny							

<그림 75> 방화벽 ACL을 통한 유해사이트 차단 설정 예시

4.7.5 취급자 단말의 외부저장매체 쓰기권한을 차단하고 있습니까?

항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.7.5
중구분	개인정보취급자 단말보안	**중요도**	**H**
항목 개요	개인정보의 외부 저장매체 사용 시 이에 대한 보호조치를 통해 정보유출을 예방해야 함		
평가기준			
판단 기준	Y - 외부 저장매체(USB, CD 등)의 쓰기(write) 권한 차단 N - 외부 저장매체(USB, CD 등)의 쓰기(write) 권한 허용		
점검 방법	▶ 외부 저장매체 사용에 대한 보호조치 적용여부 ① 외부저장매체 사용 시 읽기(Read) 권한만 허용하고 쓰기(write) 권한은 차단  ※ 출처: 중소기업 정보보호 실무 가이드 **<그림 76> 휴대용 저장매체 예시**		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료		

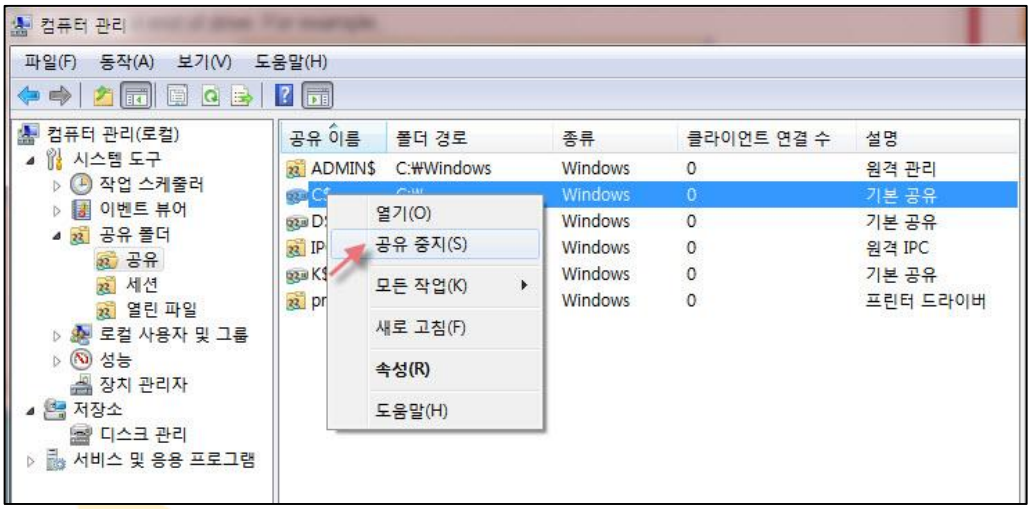
4.7.6 취급자 단말에 개인정보 파일 저장 시 보안 조치가 마련되어 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.7.6
중구분	개인정보취급자 단말보안	**중요도**	**H**
항목 개요	개인정보취급자 단말에서 개인정보파일의 저장하는 경우 비밀번호 설정 후 저장이 필요함.		
평가기준			
판단 기준	Y - 파일 암호화 소프트웨어 적용 P - 파일 비밀번호 설정 적용 N - 파일 암호화 소프트웨어, 파일 비밀번호 미 적용		
점검 방법	▶ 개인정보 파일에 대한 보안 조치 확인 ① 파일 암호화 소프트웨어(DRM) 적용 - 파일 암호화 소프트웨어 미 적용 시 파일 자체 비밀번호 설정 필요  **<그림 77> 개인정보파일 비밀번호 설정**		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제7조> 개인정보의 암호화		
과징금	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를		

및 벌칙	도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

<table>
<tr><th colspan="4">4.7.7 취급자 단말에 공유 폴더 사용을 제한하고 있습니까?</th></tr>
<tr><th colspan="4">항목구분</th></tr>
<tr><td>대구분</td><td>개인정보 기술적 보호조치</td><td>항목코드</td><td>4.7.7</td></tr>
<tr><td>중구분</td><td>개인정보취급자 단말보안</td><td>중요도</td><td>H</td></tr>
<tr><td>항목
개요</td><td colspan="3">개인정보 취급자 단말에서 공유 폴더를 사용 중일 경우 이를 통한 개인정보 접근 및 유출 가능성이 존재함</td></tr>
<tr><th colspan="4">평가기준</th></tr>
<tr><td>판단
기준</td><td colspan="3">Y - 취급자 단말에서 공유 폴더 사용하지 않음
N - 취급자 단말에서 공유 폴더 사용하고 있음</td></tr>
<tr><td>점검
방법</td><td colspan="3">▶ 취급자 단말의 공유폴더 제한
① 공유폴더 및 네트워크 드라이브 공유 금지
- 공유폴더 설정 확인 : [명령] 시작 > 실행 > cmd > net share

※ 공유폴더 확인 예시(Windows 단말)
 

<그림 78> 공유폴더 확인 예시
※ 설정 방법(Windows XP, 7, 8.1, 10
1) 기본 공유 폴더 상태 확인 및 공유 중지
- 제어판 > 관리 도구 > 컴퓨터 관리 > 공유 폴더 > 공유 (시작 > 실행 > 'fsmgmt.msc' 입력 > 공유)
- 불필요한 공유 폴더 확인 > 해당 공유 폴더 우클릭 > 공유 중지</td></tr>
</table>

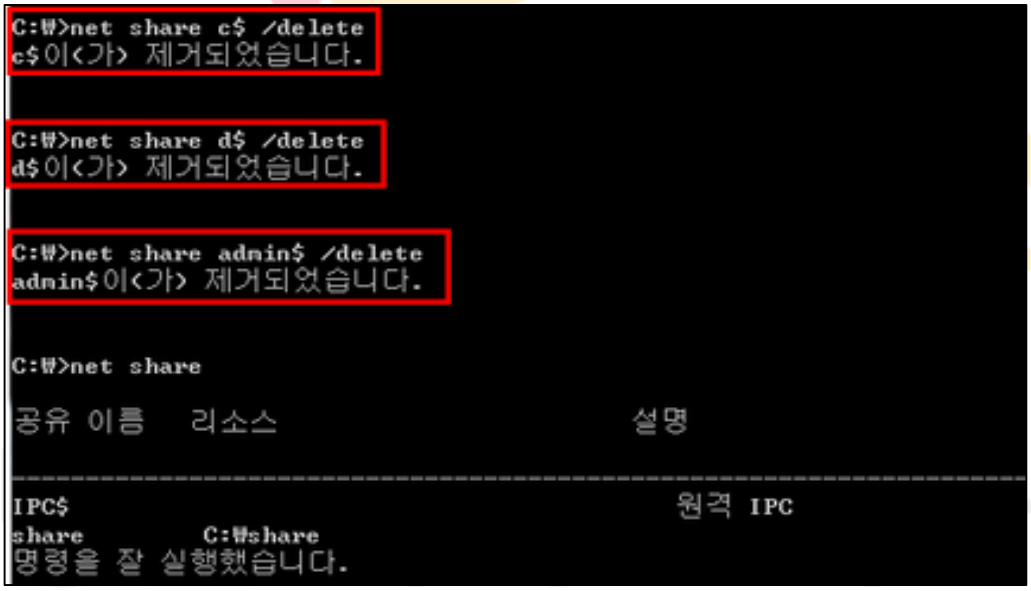


<그림 79> 기본 공유 폴더 삭제 예시

2) CMD 명령어를 이용한 설정 변경

- 관리자 권한으로 CMD.EXE 실행 후, 'net share' 입력
- 공유 폴더 중 삭제할 공유 폴더 확인

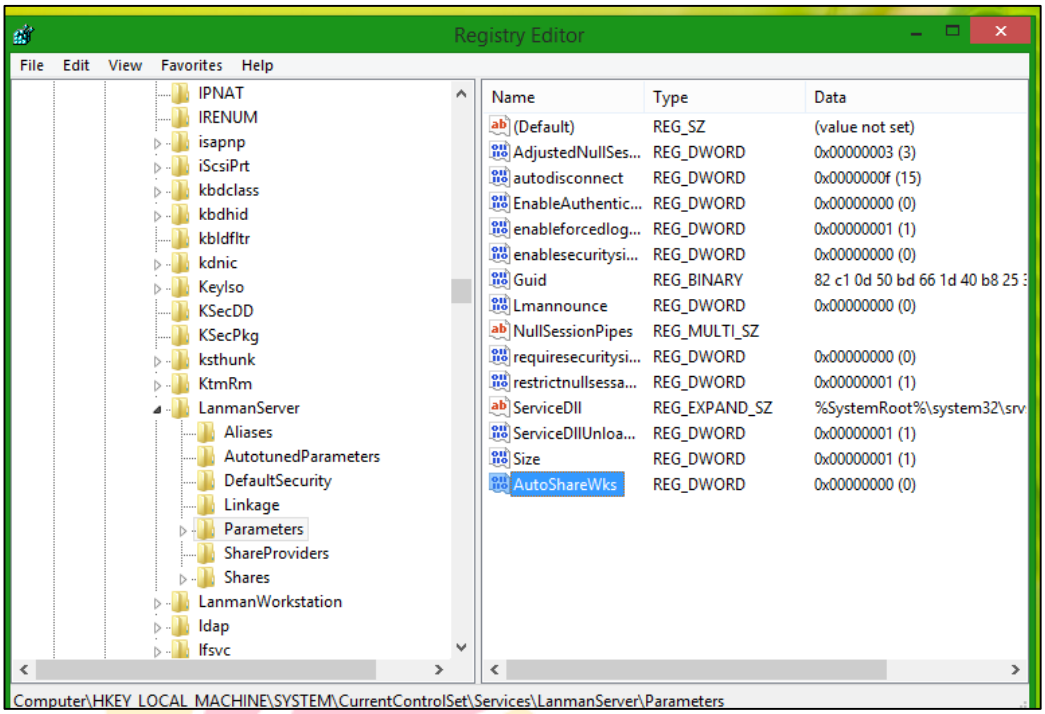
C:₩net share '삭제할 공유 폴더명' /delete 명령을 통해 공유 폴더 삭제



<그림 80> 기본 공유 폴더 삭제 예시

3) 시스템 재부팅 후 기본 공유 폴더 자동 공유 방지 설정(필수)

- 시작 > 실행 > 'regedit' 입력
- HKLM₩System₩currentControlSet₩Services₩LanmanServer₩Parameters 이동
- 설정 값 입력
- 값이 없는 경우, 새로 만들기 > AutoShareServer(또는, AutoShareWKS)를 추가하고 값을 '0'으로 입력

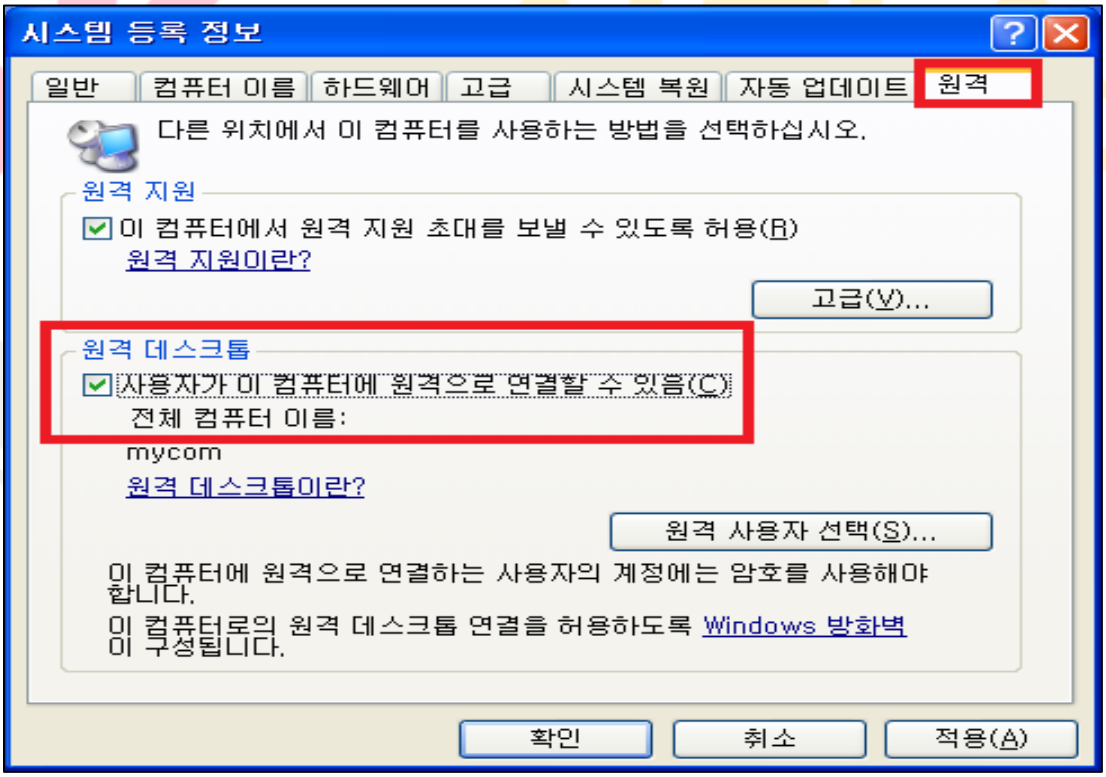


<그림 81> 레지스트리 등록/수정

관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제6조> 접근통제 ※ 개인정보의 안전성 확보조치 기준 <제10조> 관리용 단말기의 안전조치
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

4.7.8 주요 개인정보취급자 관리용 단말은 인터넷 망분리가 적용되어 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.7.8
중구분	개인정보취급자 단말보안	**중요도**	**H**
항목 개요	개인정보처리시스템에 접근하는 주요 개인정보 취급자 단말의 인터넷을 통제하여 개인정보유출을 차단하여야 함.		
평가기준			
판단 기준	Y - 주요 개인정보취급자 단말 인터넷 망분리 적용 N - 주요 개인정보취급자 단말 인터넷 망분리 미적용		
점검 방법	▶ 주요 개인정보 취급자 관리용 단말이 외부망과 분리되어 있는지 확인 ① 방화벽 및 스위치를 통한 인터넷 망분리 확인 - 솔루션(예: 망분리)을 통해 인터넷을 차단하고 있는지 확인 ※ 망분리 의무 대상자(주요 개인정보 취급자 기준) 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제6조> 접근통제 ※ 개인정보의 안전성 확보조치 기준 <제10조> 관리용 단말기의 안전조치		
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료		

4.7.9 개인정보취급자 관리용 단말의 원격접속을 차단하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.7.9
중구분	개인정보취급자 단말보안	**중요도**	**H**
항목 개요	개인정보취급자 단말에 원격접속이 가능할 시 해당 단말 외의 단말이나 서버에서 개인정보취급자 단말에 접근하여 개인정보를 탈취할 수 있으므로, 기능이 차단되어 있어야 함.		
평가기준			
판단 기준	Y - 개인정보취급자 단말 원격접속의 차단 및 관련 프로그램이 미 설치되어 있음 N - 개인정보취급자 단말 원격접속이 허용되어 있거나 관련 프로그램이 설치되어 있음		
점검 방법	▶ 개인정보취급자 단말의 원격접속 차단 여부 확인 ① 내컴퓨터 - 속성 - 원격 접속 차단 여부 확인 - 원격 접속 설정 후 실제 접속이 가능한지 확인(내부망, 외부망 테스트) ② 기타 원격접속이 가능한 프로그램(팀뷰어 등)이 설치되어 있는지 확인		

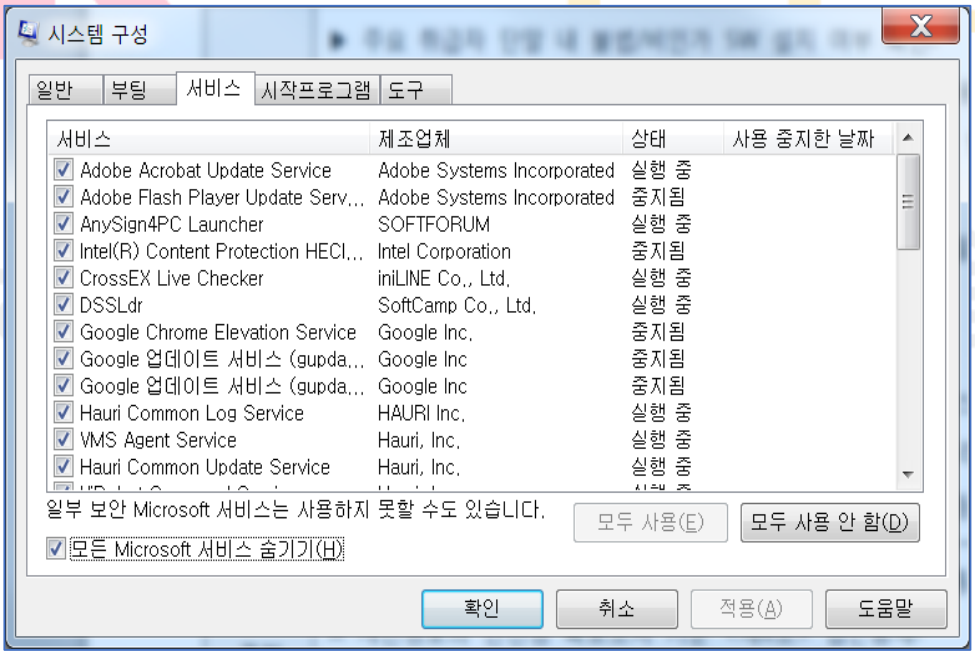


<그림 82> Windows 취급자 단말 원격 데스크톱 설정 예시

※ 외부망에서 내부 취급자 단말(일반단말, 모바일기기, 관리용 단말기 등) 원격접속 시 안전한 접속수단(추가인증 or IP통제) 및 구간 암호화 등이 적용되어야 함.

관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제6조> 접근통제 ※ 개인정보의 안전성 확보조치 기준 <제10조> 관리용 단말기의 안전조치
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

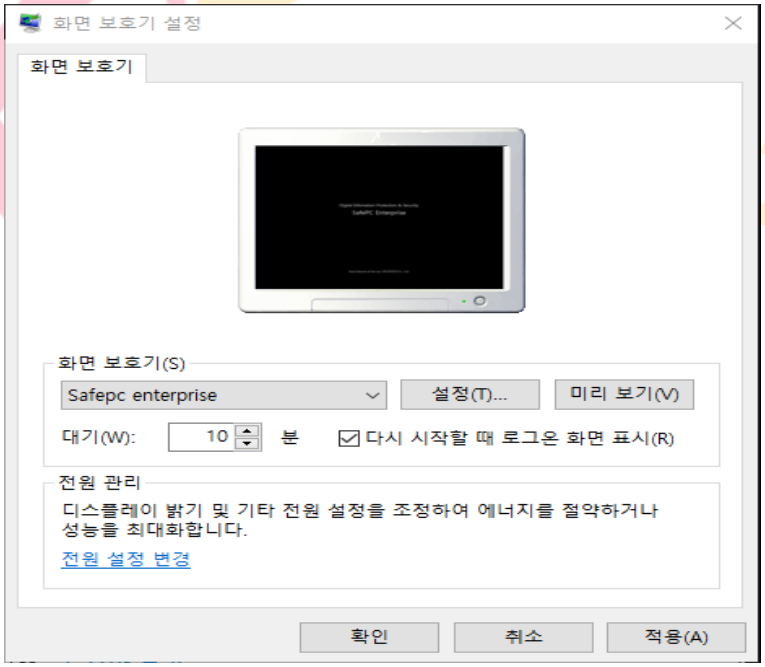
4.7.10 주요 취급자 단말 내 불법/비인가 소프트웨어나, 불필요한 서비스가 금지되어 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.7.10
중구분	개인정보취급자 단말보안	**중요도**	**H**
항목 개요	개인정보취급자 단말에 불법/비인가 소프트웨어나 불필요한 서비스가 존재할 경우, 해당 경로를 통해 개인정보 유출이나 침해사고가 발생할 수 있음		
평가기준			
판단 기준	Y - 주요 취급자 단말 내 불법/비인가 SW/불필요한 서비스가 존재하지 않음 N - 주요 취급자 단말 내 불법/비인가 SW/불필요한 서비스가 설치되어 있음 N/A - 주요 취급자 단말의 인터넷이 차단되어 있음		
점검 방법	▶ 주요 취급자 단말 내 불법/비인가 SW 설치 여부 확인 ① 개인정보 주요 취급자 단말(OS/DB, 관리자 페이지 접근용 단말) 내 비인가 메신저, 기타 SW 설치 여부 확인 ② 불필요 서비스 실행여부 확인 - 실행 -> msconfig -> 서비스, 시작프로그램 구성 내 불필요 서비스, 시작프로그램 확인 ③ 비인가 무선랜 사용여부 확인		
관련	※ 개인정보보호법 <제29조> 안전조치의무		



<그림 83> 실행 중인 서비스 확인

근거	※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제6조> 접근통제
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

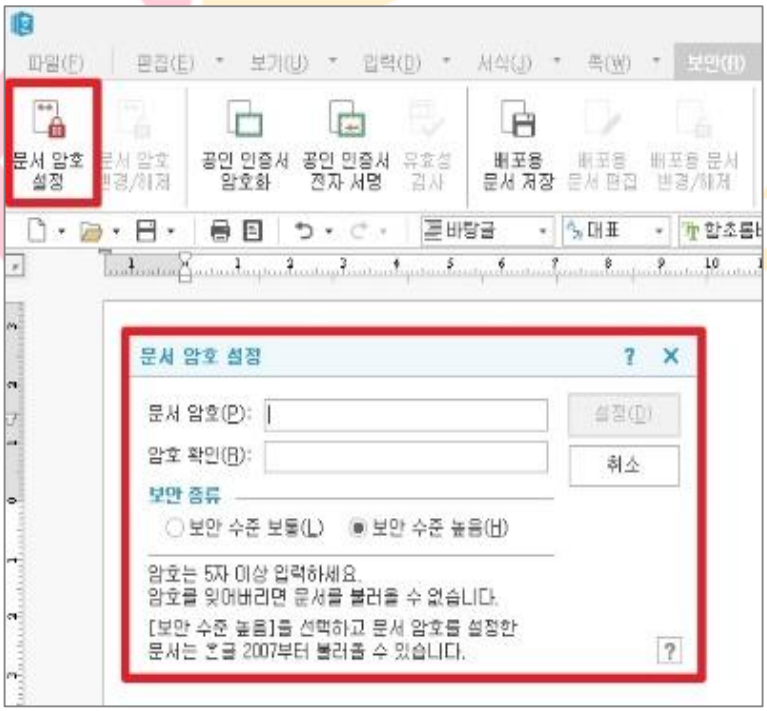
4.7.11 취급자 단말 내 화면보호기 설정이 되어 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.7.11
중구분	개인정보취급자 단말보안	**중요도**	**H**
항목 개요	화면보호기 설정이 되어 있지 않거나 10분 이상 부재 시 잠금 설정이 되지 않은 경우		
평가기준			
판단 기준	Y - 화면보호기 설정되어 있음 N - 화면보호기 설정이 되어 있지 않거나, 10분 이상으로 설정되어 있음		
점검 방법	▶ 10분이상 부재 시 자동으로 화면보호기 설정 여부 확인 ① 단말 내 설정을 통해 화면보호기 적용(10분 이내 권고) ② 화면보호기 설정 시 비밀번호 입력 필수적용 - 제어판 -> 개인설정 -> 잠금화면 -> 화면 보호기 설정		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제10조> 관리용 단말기의 안전조치		
과징금	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를		



<그림 84> 화면보호기 설정

및 벌칙	도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

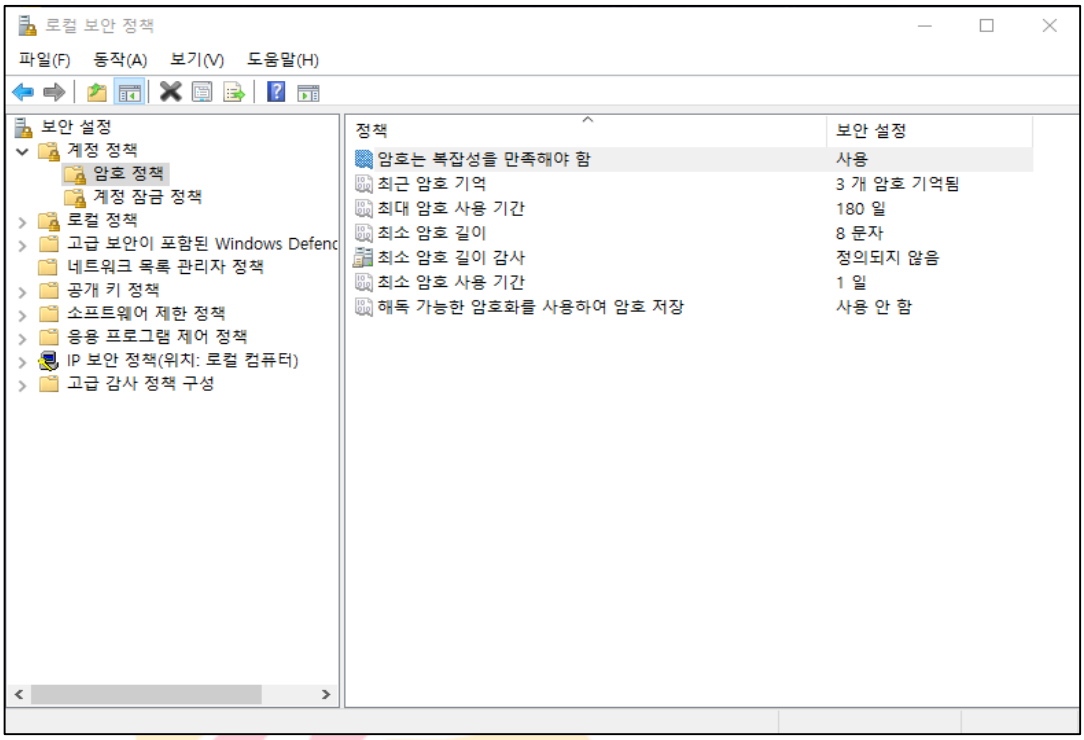
4.7.12 취급자 단말 내 비밀번호 관리대장이 암호화되어 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.7.12
중구분	개인정보취급자 단말보안	**중요도**	**H**
항목 개요	취급자 단말에 비밀번호 관리대장을 보관할 경우 암호화 등의 안전성 확보조치가 필요함		
평가기준			
판단 기준	Y - 비밀번호 관리대장을 보유하지 않거나, DRM or 파일 비밀번호가 설정되어 있음 N - 비밀번호 관리대장이 DRM or 파일 비밀번호 설정 없이 보관되고 있음		
점검 방법	▶ 개인정보 처리시스템 관리를 위한 비밀번호 관리대장 보유여부 확인 ① 단말 내 비밀번호 관리대장 보유 여부 확인 - 비밀번호 관리대장의 DRM or 파일 비밀번호 설정여부 확인		
관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제7조> 개인정보의 암호화		
과징금	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를		



<그림 85> 한글파일 암호화 예시

및 벌칙	도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료

4.7.13 취급자 단말의 비밀번호 설정 및 작성규칙이 적용되어 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.7.13
중구분	개인정보취급자 단말보안	**중요도**	**H**
항목 개요	취급자 단말에 비밀번호 설정 및 작성 시 예측이 어려운 문자 구성이 필요함.		
평가기준			
판단 기준	Y - 취급자 단말의 로그인 시 비밀번호 입력 및 관련 규칙이 적용되어 있음 N - 취급자 단말의 로그인 시 비밀번호를 입력하지 않거나, 관련 규칙이 적용되지 않음		
점검 방법	▶ 취급자 단말의 비밀번호 설정/작성규칙 여부 확인 ① 다음 각 목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성 ② 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고 ③ 동일한 비밀번호 사용 제한 ④ 비밀번호 초기화 시 부여받은 임시 비밀번호(작성규칙 적용) 변경 관리 ⑤ 사용자 로그인 시도 시 잘못된 패스워드 입력 횟수를 제한(5회 이내) ⑥ PCSS 등 로컬보안프로그램 사용 시 해당 설정 확인 필요 ※ Windows10 기준 규칙 - 암호는 복잡성을 만족해야 함 - 최근 암호 기억 3개(권고) - 최대 암호 사용기간 180일 - 최소 암호 길이 8문자 - 최소 암호 사용 기간 1일		

<table>
<tr><td></td><td> 

<그림 86> 단말 비밀번호 관련 설정 확인</td></tr>
<tr><td>관련
근거</td><td>※ 개인정보보호법 <제29조> 안전조치의무
※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치
※ 개인정보의 안전성 확보조치 기준 <제5조> 접근 권한의 관리</td></tr>
<tr><td>과징금
및
벌칙</td><td>※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금
※ 개인정보보호법 <제29조> 안전성 확보 조치 의무를 위반한 경우 3천만원 이하 과태료</td></tr>
</table>

4.8. 개발 환경 통제

4.8.1 테스트 데이터는 임의의 데이터를 생성하거나 운영데이터를 가공하여 사용하고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.8.1
중구분	개발 환경 통제	**중요도**	M
항목 개요	응용프로그램 개발 및 변경을 위한 테스트 시 실 운영 데이터를 변조하거나 임의의 데이터를 사용하여 개인정보 유출을 방지하여야 함		
평가기준			
판단 기준	Y - 1) 임의의 데이터를 생성하거나 운영 데이터를 가공하여 사용하고 있음. 2) 운영 데이터 사용 시 내부 승인 후 사용하고, 테스트 후 즉시파기 함. N - 임의의 데이터를 생성하지 않고, 운영 데이터 원본을 사용하고 있음 N/A – 서비스 구축 후 응용프로그램 개발 및 변경을 하지 않아, 관련 사례가 없음		
점검 방법	▶ 응용프로그램 개발 및 변경을 위한 테스트 시 운영 데이터 사용 여부 확인 ① 테스트 데이터는 임의의 데이터를 생성하여 사용하거나, 운영데이터를 가공하여 사용 ※ 운영 데이터를 변조하여 사용하더라도, 실제 고객정보(고객명, 핸드폰번호, 전화번호, 이메일, 고객번호, 서비스번호 등)이 테스트 데이터에 포함되면 안됨. ※ 임의로 생성되는 가상정보라도 실제와 연관성이 없게 생성되어야 함. - 핸드폰 번호도 123-4567-8989 과 같이 실제와 연관되지 않게 생성 - 실제 핸드폰 번호 입력 테스트 필요 시 테스트 진행 자의 핸드폰 번호 정도만포함 사용할 수 있고, 테스트 이후에는 즉시 삭제해야 함. ② 운영 데이터의 사용 시 팀장 승인 후 사용하고, 테스트 후 즉시 파기		
관련 근거	※ 정보보호 및 개인정보보호 관리체계 인증 <2.8.4> 시험 데이터 보안		
과징금 및 벌칙	※ "개인정보 안전조치 의무"를 위한 기술적 보호조치 권장사항		

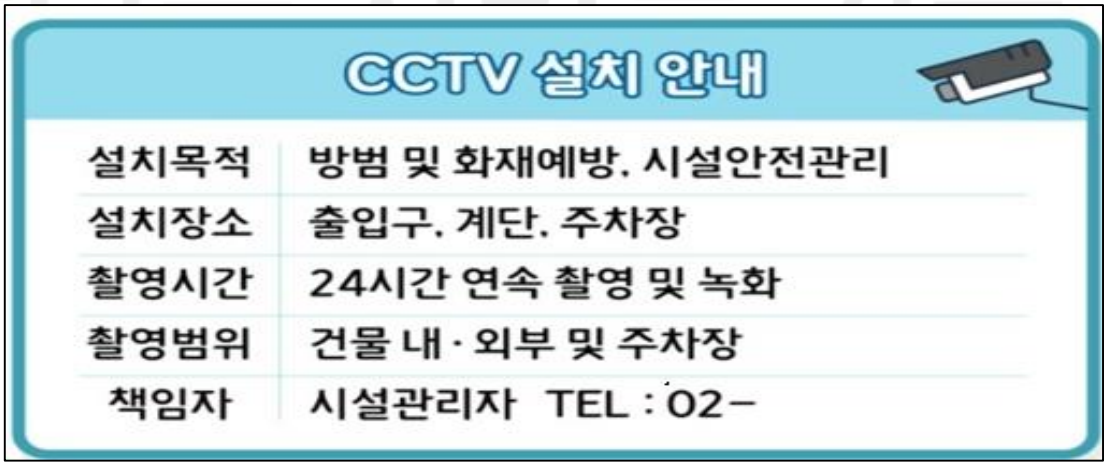
4.8.2 프로그램 소스의 형상관리가 이루어지고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.8.2
중구분	개발 환경 통제	**중요도**	**M**
항목 개요	프로그램 소스에 대한 변경절차를 수립·이행하여 변경 이력에 대한 관리를 이행하여야 함		
평가기준			
판단 기준	Y - 프로그램 소스의 형상관리가 이루어 짐 N - 프로그램 소스의 형상관리 없음		
점검 방법	▶ 프로그램 소스의 형상관리 절차를 수립·이행하고 변경이력 관리 확인 ① 별도 형상관리 프로그램 사용여부 확인 ② 형상관리 프로그램 미 사용 시 정기적 백업여부 확인 ※ 형상관리 프로그램 사용화면 증적 확인 필요		
관련 근거	※ 정보보호 및 개인정보보호 관리체계 인증 <2.8.4> 시험 데이터 보안		
과징금 및 벌칙	※ "개인정보 안전조치 의무"를 위한 기술적 보호조치 권장사항		

4.8.3 프로그램 소스에 인가된 사용자만 접근가능토록 구성되고 운영환경에 보관하지 않고 있습니까?			
항목구분			
대구분	개인정보 기술적 보호조치	**항목코드**	4.8.3
중구분	개발 환경 통제	**중요도**	**M**
항목 개요	프로그램 소스의 분석을 통해 취약점 및 개인정보의 노출이 가능하므로 이에 대한 접근통제를 이행하여야 함		
평가기준			
판단 기준	Y - 프로그램 소스는 인가된 사용자만이 접근하도록 통제하고, 프로그램 소스를 운영환경에 보관하지 않음 N - 프로그램 소스가 비 인가된 사용자가 접근 가능하고, 프로그램 소스를 운영환경에 보관함		
점검 방법	▶ 시스템 운영 장애 등 비상시를 대비한 이전 시스템의 프로그램 소스 및 관련 정보 보관 여부 확인 ▶ 형상관리 Tool 접근권한 관리 및 접근통제 여부 확인 ① 접근권한 관리 - 형상관리 Tool 사용자를 모두 식별하고, 관리자 권한은 최소한으로 부여함 ② 접근통제 - 형상관리 Tool 접속 時 PW를 설정하고, PW는 암호화함 - 형상관리 Tool 접속 時 IP기반 접속을 통제함		
관련 근거	※ 정보보호 및 개인정보보호 관리체계 인증 <2.8.5> 소스 프로그램 관리		
과징금 및 벌칙	※ "개인정보 안전조치 의무"를 위한 기술적 보호조치 권장사항		

5. 영상정보 보호조치

5.1. 영상정보처리기기 관리적 보호조치

5.1.1 영상정보처리기기를 설치·운영하는 경우 목적을 확인하고 안내판을 설치하였습니까?			
항목구분			
대구분	영상정보보호 조치	**항목코드**	5.1.1
중구분	영상정보처리기기 관리적 보호조치	**중요도**	**H**
항목 개요	영상정보처리기기 설치 후 정보주체가 이를 쉽게 인식할 수 있도록 안내판을 설치하거나, 홈페이지 이메일 등을 통해 안내해야 함.		
평가기준			
판단 기준	Y - 설치목적이 분명하고 안내판 필수 기재사항을 모두 기재함 p - 설치목적이 분명하지 않거나, 안내판 필수 기재사항을 일부/전부 누락함 N - 안내 표지판을 설치하지 않음.		
점검 방법	▶ 누구나 접근 가능한 공개된 장소에 법령, 범죄예방, 화재예방 등의 목적으로만 영상정보처리기기를 설치하였는지 확인 ① CCTV, 네트워크카메라 등 영상정보처리기기의 경우, 불특정 다수가 이용하는 공중화장실, 탈의실, 목욕실 등 개인의 사생활을 침해할 우려가 큰 장소는 영상정보처리기기 설치 금지 ② 안내판의 기재내용 - 설치 목적 및 장소 - 촬영범위 및 시간 - 관리책임자의 성명, 직책 및 연락처 - 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 수탁자의 명칭 및 연락처		



※ 출처: 개인정보보호 위원회 공식블로그 공개된 장소의 CCTV편

<그림 87> 영상정보처리기기 안내판

관련 근거	※ 개인정보보호법 <제25조제4항> 영상정보처리기기의 설치·운영 제한
과징금 및 벌칙	※ 개인정보보호법 <제25조제4항>안내판 설치 등 필요한 조치를 하지 아니한 경우 1천만원 이하 과태료

5.1.2 영상정보처리기기 운영·관리 방침을 마련하고 있습니까?			
항목구분			
대구분	영상정보보호 조치	**항목코드**	5.1.2
중구분	영상정보처리기기 관리적 보호조치	**중요도**	**H**
항목 개요	영상정보처리기기 운영 시 영상정보처리기기에 대한 운영 관리 방침을 수립하도록 하여야 함.		
평가기준			
판단 기준	Y - 운영·관리 방침이 마련되어 있음 P - 운영·관리 방침이 일부 누락되어 있음 N - 운영·관리 방침이 존재하지 않음		
점검 방법	▶ 다음 각 호의 사항이 포함된 영상정보처리기기 운영·관리 방침을 마련하였는지 확인 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 영상정보처리기기운영자의 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		

영상정보처리방침

Home > 영상정보처리방침

뷰가드 멤버십을 찾으세요?

TOP

이전조항보기

에스케이 쉴더스 주식회사 (이하 본사라 함)는 영상정보처리기기 운영.관리 방침을 통해 본사에서 처리하는 영상정보가 어떠한 용도와 방식으로 이용.관리되고 있는지 알려드립니다.

1.영상정보처리기기의 설치 근거 및 설치 목적

본사는 개인정보보호법 제25조 제1항에 따라 다음과 같은 목적으로 영상정보처리기기를 설치.운영 합니다.

- 시설안전 및 화재 예방
- 고객의 안전을 위한 범죄 예방
- 차량 도난 및 파손 방지 (지하 2.3 층 주차장 및 1층 옥외 주차장)

2. 설치 대수, 설치 위치 및 촬영범위

설치 대수	설치 위치 및 촬영 범위
42대	건물로비, 사무실 입구, 지하 주차장 및 옥외 주차장 입구

캡틴이에게 물어보세요

TOP

3. 관리책임자 및 접근권한자

	이름	직위	소속	연락처
관리책임자	배정기	팀장	HR지원팀	02-3485-9034
접근권한자	강민수	담당장	HR지원팀	02-3485-9073

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.

5. 영상정보처리기기 관리 등의 위탁에 관 한 사항

본사는 아래와 같이 영상정보처리기기 관리 등을 위탁하고 있으며, 관계 법령에 따라 위탁계약 시 개인정보가 안전하게 관리될 수 있도록 필요한 사항을 규정하고 있습니다.

수탁업체	담당자	연락처
캡스텍	이규창	02-3485-9179

6. 개인영상정보의 확인 방법 및 장소에 관한 사항

개인영상정보에 관하여 열람, 확인, 삭제를 원하는 경우 영상정보 관리책임자에게 미리 연락하고 담당 부서를 방문하시면 확인 가능합니다.

간편한 상담 신청이 필요하신가요?

TOP

7. 정보주체의 영상정보 열람 등 요구에 대한 조치

귀하는 개인영상정보에 관하여 열람 또는 존재확인.삭제를 원하는 경우 언제든지 영상정보리기기 운영자에게 요구하실 수 있습니다. 단, 귀하가 촬영된 개인영상정보 및 명백히 정보주체의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 개인영상정보에 한정됩니다.본사는 개인영상정보에 관하여 열람 또는 존재확인.삭제를 요구한 경우 지체 없이 필요한 조치를 하겠습니다.

8. 영상정보의 안전성 확보조치

본사는 처리하는 영상정보는 암호화 조치 등을 통하여 안전하게 관리되고 있습니다. 또한 본사는 개인영상정보보호를 위한 관리적 대책으로서 개인정보에 대한 접근 권한을 차등부여하고 있고, 개인영상정보의 위.변조 방지를 위하여 개인영상정보의 생성 일시, 열람 시 열람 목적.열람자.열람 일시 등을 기록하여 관리하고 있습니다. 이 외에도 개인영상정보의 안전한 물리적 보관을 위하여 잠금장치를 설치하고 있습니다.

9. 개인정보 처리방침 변경에 관한 사항

이 영상정보처리기기 운영.관리방침은 2019년 04월 11일에 제정되었으며 법령 · 정책 또는 보안기술의 변경에 따라 내용의 추가 · 삭제 및 수정이 있을 시에는 시행하기 최소 7일전에 본 사 홈페이지를 통해 변경사유 및 내용 등을 공지하도록 하겠습니다.

- 공고일자 : 2019년 4월 12일 / 시행일자 : 2019년 4월 12일

공고일	시행일	버전
2019.04	2019.04	Rev. 1

<그림 88> 영상정보처리기기 운영·관리 방침

관련 근거	※ 개인정보보호법 <제25조> 영상정보처리기기의 설치·운영 제한 ※ 개인정보보호법 시행령 <제24조> 안내판의 설치 등
과징금 및 벌칙	※ 개인정보보호법 <제25조> 영상정보처리기기의 설치·운영 제한 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자 3년 이하의 징역 또는 3천만원 이하의 벌금

5.1.3 영상정보처리기기 설치 운영에 관한 사무를 위탁하는 경우 절차 및 요건에 따라 계약서에 반영하고 있습니까?

항목구분			
대구분	영상정보보호 조치	**항목코드**	5.1.3
중구분	영상정보처리기기 관리적 보호조치	**중요도**	H
항목 개요	영상정보처리기기 위탁 시 개인정보보호와 관련 내용이 포함되도록 하여야 함.		
평가기준			
판단 기준	Y - 위탁 계약서 개인정보보호 관련 내용을 모두 포함하여 징구 하고 있음 P - 위탁 계약서 개인정보보호 관련 내용이 일부 누락되어 있음 N - 위탁 계약서 징구를 하지 않은 경우		
점검 방법	▶ 영상정보처리기기 관리 업무를 위탁하는 경우 위탁 계약사 등에 개인정보보호 관련 내용이 포함되도록 하여야 한다. ① 위탁하는 사무의 목적 및 범위 ② 재 위탁 제한에 관한 사항 ③ 영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한사항 ④ 영상정보의 관리 현황 점검에 관한 사항 ⑤ 위탁 받는 자가 준수하야 할 의무를 위반한 경우 손해배상 등 책임에 관한 사항		

표준 개인정보처리위탁 계약서

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)
1.
2.

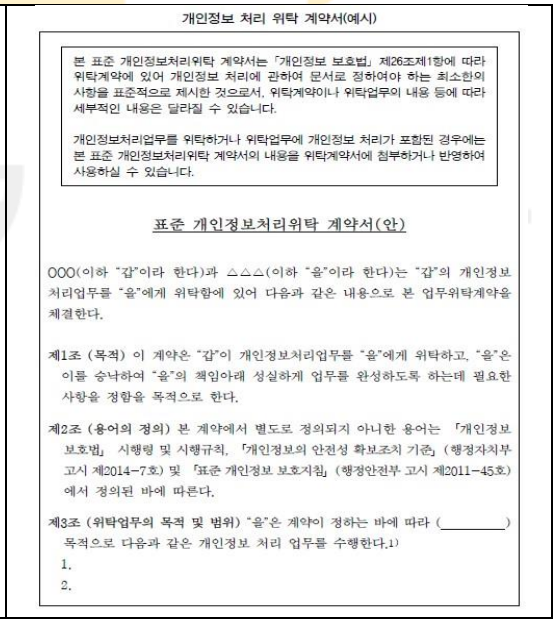
제4조 (위탁업무 기간) 이 계약서에 의한 개인정보 처리업무의 기간은 다음과 같다.
계약 기간 : 20oo년 o월 o일 ~ 20oo년 o월 o일

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.

제6조 (개인정보의 안전성 확보조치) "을"은 「개인정보 보호법」 제23조제2항 및 제24조제3항 및 제29조, 같은 법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(개인정보 보호위원회 고시 제2020-2호)에 따라 개인정보의 안전성 확보에 필요한 기술적·관리적 조치를 취하여야 한다.

제7조 (개인정보의 처리제한) ① "을"은 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.
② "을"은 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유

SK 쉴더스



개인정보 처리 위탁 계약서(예시)

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.

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

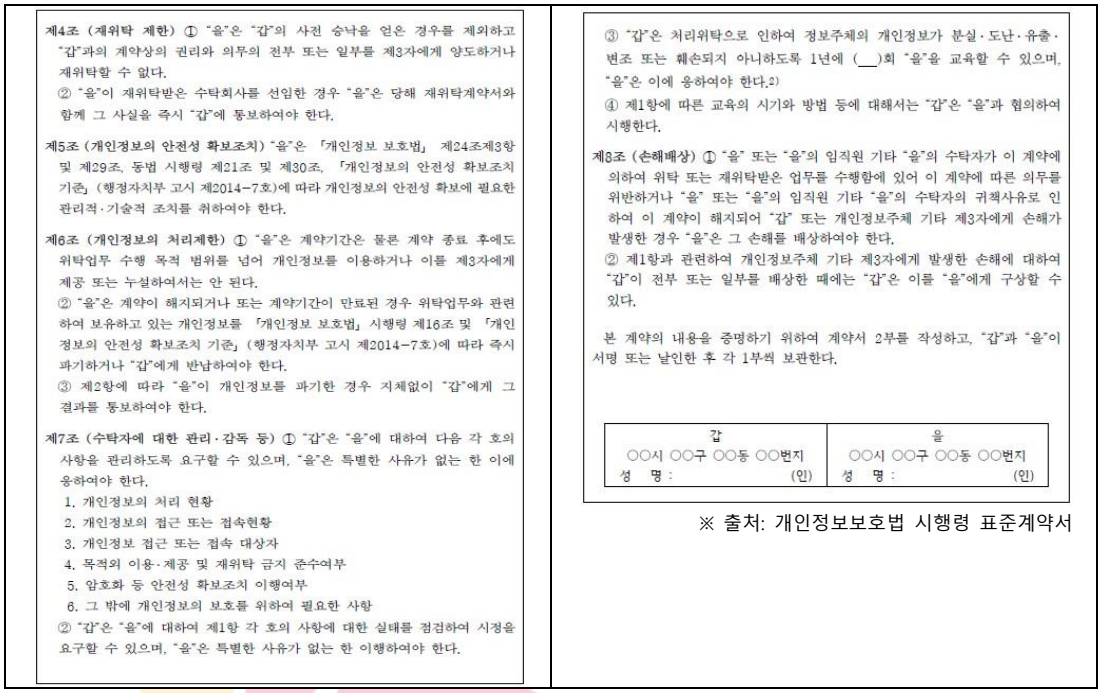
표준 개인정보처리위탁 계약서(안)

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」 시행령 및 시행규칙, 「개인정보의 안전성 확보조치 기준」(행정자치부 고시 제2014-7호) 및 「표준 개인정보 보호지침」(행정안전부 고시 제2011-45호)에서 정의된 바에 따른다.

제3조 (위탁업무의 목적 및 범위) "을"은 계약이 정하는 바에 따라 (_____) 목적으로 다음과 같은 개인정보 처리 업무를 수행한다.1)
1.
2.



제4조 (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 재위탁받은 수탁회사를 선임한 경우 "을"은 당해 재위탁계약서와 함께 그 사실을 즉시 "갑"에 통보하여야 한다.

제5조 (개인정보의 안전성 확보조치) "을"은 「개인정보 보호법」 제24조제3항 및 제29조, 동법 시행령 제21조 및 제30조, 「개인정보의 안전성 확보조치 기준」(행정자치부 고시 제2014-7호)에 따라 개인정보의 안전성 확보에 필요한 관리적·기술적 조치를 취하여야 한다.

제6조 (개인정보의 처리제한) ① "을"은 계약기간은 물론 계약 종료 후에도 위탁업무 수행 목적 범위를 넘어 개인정보를 이용하거나 이를 제3자에게 제공 또는 누설하여서는 안 된다.
② "을"은 계약이 해지되거나 또는 계약기간이 만료된 경우 위탁업무와 관련하여 보유하고 있는 개인정보를 「개인정보 보호법」 시행령 제16조 및 「개인정보의 안전성 확보조치 기준」(행정자치부 고시 제2014-7호)에 따라 즉시 파기하거나 "갑"에게 반납하여야 한다.
③ 제2항에 따라 "을"이 개인정보를 파기한 경우 지체없이 "갑"에게 그 결과를 통보하여야 한다.

제7조 (수탁자에 대한 관리·감독 등) ① "갑"은 "을"에 대하여 다음 각 호의 사항을 관리하도록 요구할 수 있으며, "을"은 특별한 사유가 없는 한 이에 응하여야 한다.
1. 개인정보의 처리 현황
2. 개인정보의 접근 또는 접속현황
3. 개인정보 접근 또는 접속 대상자
4. 목적외 이용·제공 및 재위탁 금지 준수여부
5. 암호화 등 안전성 확보조치 이행여부
6. 그 밖에 개인정보의 보호를 위하여 필요한 사항
② "갑"은 "을"에 대하여 제1항 각 호의 사항에 대한 실태를 점검하여 시정을 요구할 수 있으며, "을"은 특별한 사유가 없는 한 이행하여야 한다.

③ "갑"은 처리위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 1년에 (__)회 "을"을 교육할 수 있으며, "을"은 이에 응하여야 한다.2)
④ 제1항에 따른 교육의 시기와 방법 등에 대해서는 "갑"은 "을"과 협의하여 시행한다.

제8조 (손해배상) ① "을" 또는 "을"의 임직원 기타 "을"의 수탁자가 이 계약에 의하여 위탁 또는 재위탁받은 업무를 수행함에 있어 이 계약에 따른 의무를 위반하거나 "을" 또는 "을"의 임직원 기타 "을"의 수탁자의 귀책사유로 인하여 이 계약이 해지되어 "갑" 또는 개인정보주체 기타 제3자에게 손해가 발생한 경우 "을"은 그 손해를 배상하여야 한다.
② 제1항과 관련하여 개인정보주체 기타 제3자에게 발생한 손해에 대하여 "갑"이 전부 또는 일부를 배상한 때에는 "갑"은 이를 "을"에게 구상할 수 있다.

본 계약의 내용을 증명하기 위하여 계약서 2부를 작성하고, "갑"과 "을"이 서명 또는 날인한 후 각 1부씩 보관한다.

갑	을
○○시 ○○구 ○○동 ○○번지 성 명 : (인)	○○시 ○○구 ○○동 ○○번지 성 명 : (인)

※ 출처: 개인정보보호법 시행령 표준계약서

<그림 89> 영상정보처리기기 표준 위탁계약서

관련 근거	※ 개인정보보호법 <제25조 제4항> 영상정보처리기기의 설치·운영 제한
과징금 및 벌칙	※ 개인정보보호법 <제25조> 영상정보처리기기의 설치·운영 제한 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자 3년 이하의 징역 또는 3천만원 이하의 벌금

5.2. 영상정보처리기기 기술적 보호조치

5.2.1 영상정보처리기기의 사생활 침해 및 설치목적 외 임의 조작등을 제한하고 있습니까?			
항목구분			
대구분	영상정보보호 조치	**항목코드**	5.2.1
중구분	영상정보처리기기 기술적 보호조치	**중요도**	**H**
항목 개요	영상정보처리기기 사용 시 임의조작 및 음성녹음을 사용할 수 없도록 설계되어야 함.		
평가기준			
판단 기준	Y - 영상정보처리기기 설치 목적 외 임의조작 및 음성녹음 등을 금지되어 있음. N - 영상정보처리기기 설치 목적 외 임의조작 및 음성녹음 등을 금지하지 않음.		
점검 방법	▶ 영상정보처리기기 설치 제한 ① 영상정보처리기기의 설치 목적 외 임의조작, 회전 및 녹음기능 등을 제어금지  ※ 출처: 개인정보보호 위원회 공식블로그 공개된 장소의 CCTV편 **<그림 90> 영상정보처리기기 조작 금지**		
관련 근거	※ 개인정보보호법 <제25조 제4항> 영상정보처리기기의 설치·운영 제한		
과징금 및 벌칙	※ 개인정보보호법 <제25조> 영상정보처리기기의 설치·운영 제한 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자 3년 이하의 징역 또는 3천만원 이하의 벌금		
5.2.2 영상정보의 보관기간을 정하고, 기간 만료 시 지체 없이 파기하고 있습니까?			

<table>
<tr><th colspan="4">항목구분</th></tr>
<tr><td>대구분</td><td>영상정보보호 조치</td><td>항목코드</td><td>5.2.2</td></tr>
<tr><td>중구분</td><td>영상정보처리기기 기술적 보호조치</td><td>중요도</td><td>H</td></tr>
<tr><td>항목
개요</td><td colspan="3">영상정보 처리기기 설치 후 정보주체가 이를 쉽게 인식할 수 있도록 안내판을 설치하거나, 홈페이지 이메일 등을 통해 안내해야 함.</td></tr>
<tr><th colspan="4">평가기준</th></tr>
<tr><td>판단
기준</td><td colspan="3">Y - 설치목적이 분명하고 안내판 필수 기재사항을 모두 기재함
P - 설치목적이 분명하지 않거나, 안내판 필수 기재사항을 일부/전부 누락함
N - 안내 표지판을 설치하지 않음.</td></tr>
<tr><td>점검
방법</td><td colspan="3">▶ 영상정보 보유기간 산정
① 영상정보 보유 목적 달성을 위한 최소한의 기간으로 보유기간을 산정하고 있는지 확인
- 시스템 운영의 보유 목적상 최소한의 기간을 산정하고 있는지 확인·보유기간 산정이 어려울 경우 수집 후 30일 이내로 함
② 산정한 보유기간의 영상정보를 즉시 파기하고 있는지 확인
< 개인영상정보 관리대장 >
<table>
<tr><th>번호</th><th>구분</th><th>일시</th><th>파일명/
형태</th><th>담당자</th><th>목적/
사유</th><th>이용·제공
받는 제3자
/열람등
요구자</th><th>이용·
제공
근거</th><th>이용·
제공
형태</th><th>기간</th></tr>
<tr><td>1</td><td>☐ 이용
☐ 제공
☐ 열람
☐ 파기</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>2</td><td>☐ 이용
☐ 제공
☐ 열람
☐ 파기</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>3</td><td>☐ 이용
☐ 제공
☐ 열람
☐ 파기</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
※ 출처: 개인정보보호 법령 및 지침 고시 해설서
<그림 91> 영상정보처리기기 관리대장(이용, 제공, 열람, 파기)</td></tr>
<tr><td>관련
근거</td><td colspan="3">※ 개인정보보호법 <제25조> 영상정보처리기기의 설치·운영 제한</td></tr>
</table>

과징금 및 벌칙	※ 개인정보보호법 <제25조> 영상정보처리기기의 설치·운영 제한 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자 3년 이하의 징역 또는 3천만원 이하의 벌금

6. 개인정보 물리적 보호조치

6.1. 물리적 통제

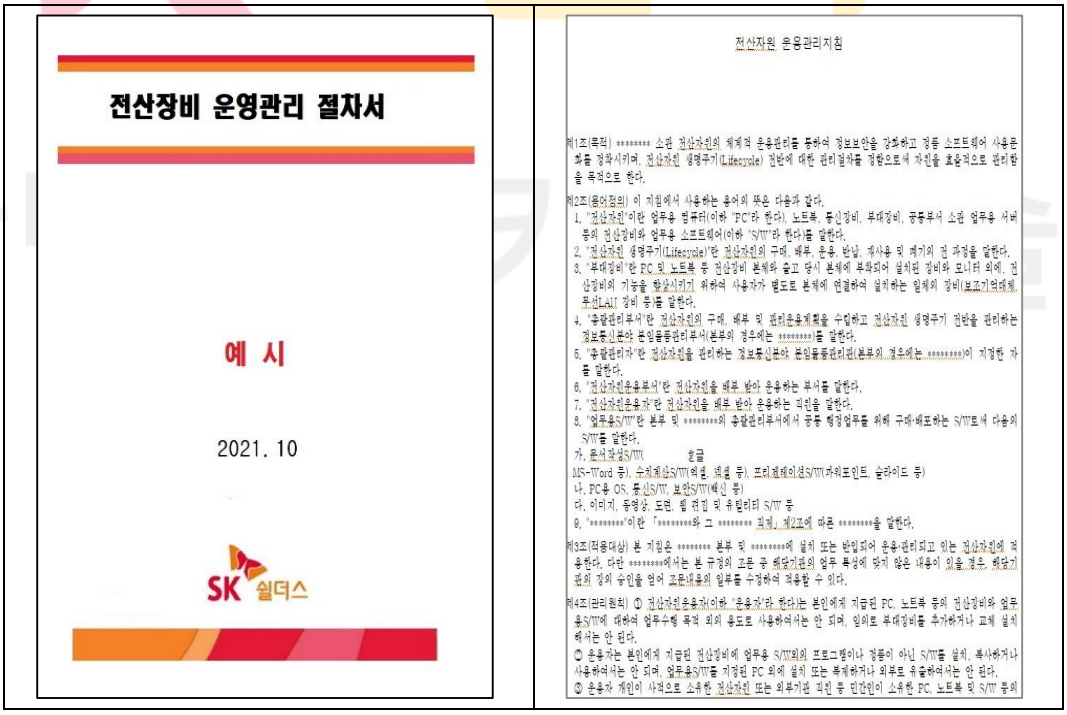
6.1.1 전산실의 출입 통제 적용이 되어 있습니까?			
항목구분			
대구분	개인정보 물리적 보호조치	**항목코드**	6.1.1
중구분	물리적 통제	**중요도**	**H**
항목 개요	보호구역별 보호조치(출입통제)의 절차와 물리적 보호조치를 갖춰야 함.		
평가기준			
판단 기준	Y - 전산실의 출입 통제 절차가 존재하고, 절차에 맞춰 출입 관리하고 있음. N - 전산실의 출입 통제 절차 없이 출입하고 있음.		
점검 방법	▶ 보호구역 별 보호조치(출입통제) 적용 ① 보호구역을 물리적으로 구분하고 출입통제장치 설치 확인 - 보호구역 지정 구역 중 출입통제장치 미설치 구역 존재여부 확인 ex) 출입통제장치: 열쇠, 도어락, 출입증, 지문인식 등 ② 보호구역 출입 인원 통제 방법 확인 - 보호구역 내 출입 인가자 명단을 보유하고 출입관리대장을 보유하고 있는지 확인 (지문 인식 시 Log) - 출입관리대장: 출입 시간, 출입자 명단, 출입 목적, 퇴실시간 ▶ 외부인 출입 시 통제 절차 확인 ① 외부인 출입 시 출입 절차 여부 확인 - 외부인 출입관리 대장 작성 및 출입 등록에 대한 절차 확인 ② 출입 인가자와 동행하고 있는지 확인 ▶ 서버/DB가 설치된 장소는 담당자 이외에는 접근 여부 확인 ① 전산실 등이 공개되지 않고 잠금장치로 잠겨져 있는지 확인 - 비인가자의 접근을 통제하고 있는지 확인 ▶ 출입 관리 대장 및 출입 인원 확인 / 감독 여부 ① 보호 구역 출입 관리에 대한 확인 / 감독을 하고 있는지 확인 - 출입 관리 대장 및 출입 Log를 정기적으로 확인하고 있는지 확인 - 비인가자 및 외부자의 출입이 통제되고 있는지 확인		

	 **<그림 92> 전산실 출입통제 시스템**
관련 근거	※ 정보통신망법 <제45조> 정보통신망의 안정성 확보 등 ※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보보호법 시행령 <제48조의2> 개인정보의 안전성 확보 조치에 관한 특례 ※ 개인정보의 안전성 확보조치 기준 <제11조> 물리적 안전조치 ※ 개인정보의 기술적·관리적 보호조치기준 <제8조> 물리적 접근 방지
과징금 및 벌칙	※ 개인정보보호법 <제29조> 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당한 경우 2년 이하 징역 또는 2천만원 이하 벌금 ※ 개인정보보호법 <제29조> 안전성 확보조치의무를 위반한 경우 3천만원 이하 과태료

6.1.2 전산실, 자료보관실 등의 개인정보가 보관된 장소에는 보호설비를 갖추고 있습니까?			
항목구분			
대구분	개인정보 물리적 보호조치	**항목코드**	6.1.2
중구분	물리적 통제	**중요도**	**H**
항목 개요	보호구역의 중요도 및 특성에 따라 화재, 수해, 전력이상 등 인재 및 자연재해 등에 대비한 설비 시설을 갖춰야 함.		
평가기준			
판단 기준	Y - 보안설비를 갖추고 관리하고 있음 N - 보안설비를 갖추고 관리하고 않음		
점검 방법	▶ 서버/DB가 설치된 전산실 등의 방화시설 설치 여부 확인 ① 전산실 등에 화재에 대비한 방화시설 설치 여부 확인 ▶ 각 보호구역의 중요도 및 특성에 따라 필요한 설비를 갖추고 운영하고 있는지 확인 ① 물리적 보호설비 - 온/습도 조절기, 화재감지 및 소화설비, 누수감지기, UPS, 비상발전기 등 ▶ IDC에 위탁하는 경우 해당 내용을 주기적으로 검토하고 있는지 확인 ① 계약서 내 물리적 보호에 필요한 요구사항 반영여부 확인(책임보험 가입 등) ② 운영상태 주기적 검토		
관련 근거	※ 정보통신망법 <제45조> 정보통신망의 안정성 확보 등 ※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보보호법 시행령 <제48조의2> 개인정보의 안전성 확보 조치에 관한 특례 ※ 개인정보의 안전성 확보조치 기준 <제11조> 물리적 안전조치 ※ 개인정보의 기술적·관리적 보호조치기준 <제8조> 물리적 접근 방지		
과징금 및 벌칙	※ 개인정보보호법 <제21조제1항> 개인정보가 불필요하게 되었을 때 파기하지 않은 경우 2년 이하의 징역 또는 2천만원 이하의 벌금 ※ 개인정보보호법 <제21조제1항> 개인정보의 파기 등 필요한 조치를 아니한 경우 3천만원 이하 과태료		

<table>
<tr><th colspan="4">6.1.3 개인정보가 저장된 물리적 장치 및 출력물에 대한 파기가 이루어져 있습니까?</th></tr>
<tr><th colspan="4">항목구분</th></tr>
<tr><td>대구분</td><td>개인정보 물리적 보호조치</td><td>항목코드</td><td>6.1.3</td></tr>
<tr><td>중구분</td><td>물리적 통제</td><td>중요도</td><td>H</td></tr>
<tr><td>항목
개요</td><td colspan="3">개인정보가 유출 및 오남용 방지를 위해 개인정보를 복원이 불가하도록 파기해야 함</td></tr>
<tr><th colspan="4">평가기준</th></tr>
<tr><td>판단
기준</td><td colspan="3">Y - 개인정보가 포함된 물리적 장치 및 문서에 대해서 물리적 파기 이행하고 있음
N - 개인정보가 포함된 물리적 장치 및 문서에 대해서 물리적 파기 이행하고 있지 않음</td></tr>
<tr><td>점검
방법</td><td colspan="3">▶ 개인정보가 포함된 종이문서, 하드디스크나 자기테이프 물리적 파기 확인
① 완전파괴(소각, 파쇄 등)
② 전용 소자장비를 이용하여 삭제
③ 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행 (완전삭제 프로그램 등)
<table>
<tr><th>파기 방법</th><th>예 시</th></tr>
<tr><td>완전파괴</td><td>개인정보가 저장된 회원가입신청서 등의 종이 문서,
하드디스크나 자기테이프를 파쇄기로 파기하거나 용해 또는
소각처리 등</td></tr>
<tr><td>전용 소자장비</td><td>디가우저(Degausser)를 이용해 하드디스크나 자기테이프에
저장된 개인정보 삭제 등</td></tr>
<tr><td>데이터 복원
불가 초기화</td><td>하드디스크 완전포맷(3회 이상 권고), 안전한 알고리즘 암호화
후 암호화키 완전삭제</td></tr>
</table>
<표 14> 물리적 파기방법 예시</td></tr>
<tr><td>관련
근거</td><td colspan="3">※ 개인정보보호법 <제21조> 개인정보의 파기
※ 개인정보의 안전성 확보조치 기준 <제13조> 개인정보의 파기</td></tr>
<tr><td>과징금
및
벌칙</td><td colspan="3">※ 개인정보보호법 <제21조제1항> 개인정보가 불필요하게 되었을 때 파기하지 않은 경우
2년 이하의 징역 또는 2천만원 이하의 벌금
※ 개인정보보호법 <제21조제1항> 개인정보의 파기 등 필요한 조치를 아니한 경우
3천만원 이하 과태료</td></tr>
</table>

6.1.4 자산에 대한 반·출입 절차 수립이 되어 있습니까?			
항목구분			
대구분	개인정보 물리적 보호조치	**항목코드**	6.1.4
중구분	물리적 통제	**중요도**	**H**
항목 개요	자산 및 저장매체 반·출입 시 절차 수립과 이행이 필요함.		
평가기준			
판단 기준	Y - 자산 및 저장매체의 반·출입 관리 절차가 수립 및 이행하고 있음 N - 자산 및 저장매체의 반·출입 관리 절차가 수립 및 이행이 되지 않음		
점검 방법	▶ 보유 자산에 대한 외부 반·출입 절차 수립 여부 ① 내부관리 규정/지침서 내 보유자산의 반·출입 시 관리절차 수립 여부 확인 - 서버 및 단말 등 보유 자산의 변동 및 반·출입에 대한 관리 절차 수립 여부 확인 - USB, HDD, CD등의 반·출입에 대한 관리 절차 수립 여부 확인 ② 반출 시 허가 요청 및 승인 절차 여부 확인 - 내부관리 규정 및 반출·입에 대한 승인 절차 수립 여부 확인 - 보유 자산의 반·출입 관리 대장 등의 관리적 증적 확인 - 유지보수, 폐기 등을 위해 저장매체의 외부 반출이 필요한 경우 작성 - 보유 자산 및 저장매체 반·출입 관리대장은 정기적으로 점검 및 확인/감독		



<그림 93> 전산장비 운영관리 절차서

장비 반출입대장

No.	대상장비			반출 사유	반출내역			반입내역			관 리 책임자
	장비명	관리번호	수량		일자	반출자	확인	일자	반입자	확인	

※ 출처: 개인정보보호 법령 및 지침 고시 해설서

<그림 94> 장비 반출입 대장

관련 근거	※ 개인정보보호법 <제29조> 안전조치의무 ※ 개인정보보호법 시행령 <제30조> 개인정보의 안전성 확보 조치 ※ 개인정보의 안전성 확보조치 기준 <제11조> 물리적 안전조치
과징금 및 벌칙	※ 개인정보보호법 <제21조제1항> 개인정보가 불필요하게 되었을 때 파기하지 않은 경우 2년 이하의 징역 또는 2천만원 이하의 벌금 ※ 개인정보보호법 <제21조제1항> 개인정보의 파기 등 필요한 조치를 아니한 경우 3천만원 이하 과태료

SK쉴더스㈜ 13486 경기도 성남시 분당구 판교로227번길 23, 4&5층
https://www.skshieldus.com

발행인 : SK쉴더스 취약점진단팀
제 작 : SK쉴더스 마케팅Comm.팀