

개인정보보호관리체계 인증준비 안내서(사업자용)

Guide to the Certification of Personal Information Management System

- 부록편 -

2010. 12

언제 어디서나 인터넷 관련 상담은

e콜센터 @118



해킹바이러스



불법스팸



개인정보침해



기타인터넷상담

한국인터넷진흥원이 운영하는 e콜센터 @

척척박사 118

무엇이든 물어보세요!

스팸문자를 받으셨나요? 개인정보가 유출되셨나요? PC가 해킹당하셨나요?

해킹·바이러스·불법스팸·개인정보침해 등 인터넷으로 인하여 어려움을 겪으신 분들을 위해 인터넷 이용 중 궁금한 것을 해결해드립니다.

언제 어디서나 인터넷 관련 상담은 **전국 무료 전화번호 118**



한국인터넷진흥원

e콜센터 @118 이란?

해킹, 바이러스, 불법스팸, 개인정보침해 등 인터넷으로 인해 어려움을 겪거나 인터넷 이용 중 궁금한 것을 해결해 주는 전국 무료 전화번호입니다.

개인정보보호관리체계 인증준비 안내서(사업자용)

Guide to the Certification of Personal Information Management System

- 부록편 -



2010. 12

목 차

부록 1. 개인정보 관리체계 인증양식 모음	1
부록 2. 개인정보보호 규정 예시	7
부록 3. 개인정보보호를 위한 기술적 보호조치 안내서	77
부록 4. 법률준수 통제항목	107
부록 5. 개인정보취급방침 작성 예시	131
부록 6. 개인정보보호 현황분석을 위한 체크리스트	173

■ 개인정보보호관리체계 인증준비 안내서(부 록)

부 록 1

개인정보 관리체계 인증양식 모음

[별지 제1호서식] 정보보호 및 개인정보보호관리체계 인증신청서

정보보호 및 개인정보보호관리체계 인증신청서				
		<input type="checkbox"/> 정보보호관리체계	<input type="checkbox"/> 개인정보보호관리체계	
신청인	성명(대표자)		생년월일	
	상호 또는 명칭		사업자등록번호	
	소재지		전화번호	
인증신청의 구분		<input type="checkbox"/> 인증심사(처음으로 인증신청을 하는 때) <input type="checkbox"/> 갱신심사(유효기간의 만료로 다시 인증신청을 하는 때) <input type="checkbox"/> 재심사(인증의 범위에 중요한 변경이 있어서 다시 인증신청을 하는 때)		
정보보호 또는 개인정보 보호 관리체계의 범위				
종업원 수 또는 개인정보취급자 수			정보통신시설 또는 개인정보취급 정보통신시설 수	
위와 같이 정보보호 (또는 개인정보보호관리체계) 인증을 신청합니다. <div style="display: flex; justify-content: space-around; align-items: center;"> 년 월 일 </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 10px;"> 신청인 (서명 또는 인) </div> <div style="text-align: center; margin-top: 20px; font-size: 1.2em;"> 한국인터넷진흥원장 귀하 </div>				
구비서류 1. 법인등기부등본(법인인 경우에 한합니다) 2. 정보보호(또는 개인정보보호)관리체계 내역서				

[별지 제2호서식] 정보보호관리체계 내역서

정보보호관리체계의 내역서			
<input type="checkbox"/> 정보보호관리체계		<input type="checkbox"/> 개인정보보호관리체계	
조직 소개	설립일		
	주요사업 및 업무 내용		
수립 목적	정보보호관리체계 수립 목적		
수립 범위	수립 범위내의 내용		
	수립범위 내·외의 연동업무		
	서버 수		종업원 수
운영 기간	년 월 일 ~ 년 월 일		
제출 문서	- 정보보호관리체계 인증범위서(자유 양식) ※ 조직소개, 조직도, 시스템 및 네트워크 구성도, 문서목록, 주요자산목록 포함		
기타	정보보호관리체계 수립 및 운영상의 조직적 환경적, 기술적 특성		

※ 서버수, 종업원 수, 제출자료는 신청기관이 수립한 정보보호관리체계 및 개인정보보호관리체계 범위내의 사항만 포함

※ 부족 시 별지사용

[별지 제4호서식] 정보보호관리체계 및 개인정보보호관리체계 보완조치 내역서

정보보호관리체계 및 개인정보보호관리체계 보완조치 내역서						
<input type="checkbox"/> 정보보호관리체계 <input type="checkbox"/> 개인정보보호관리체계						
관련조항 : 통제항목번호 및 제목						
<input type="checkbox"/> 중결함 <input type="checkbox"/> 결함						
보완조치 결과	※ 결함보고서의 결함사항에 대한 보완 조치 내용 작성					
	<input type="checkbox"/> 결함내용					
	<input type="checkbox"/> 보완내역					
	<input type="checkbox"/> 관련근거					
	작성자	(인)	확인자	(인)	작성일	년 월 일
보완조치 결과확인	확인자 (심사팀장)	(인)	확인일	년 월 일		
			결과	<input type="checkbox"/> 완료 <input type="checkbox"/> 미완료 <input type="checkbox"/> 현장확인		
현장확인	확인자 (심사팀장)	(인)	확인일	년 월 일		
			결과	<input type="checkbox"/> 완료 <input type="checkbox"/> 미완료		

부 록 2

개인정보보호 규정 예시

□ 개인정보보호정책

대외비

문서번호

개인정보보호정책

< 개정 이력 >

개정번호	조항번호	개정내용요약	개정일자	담당자
1.0		신규제정	2009.06.01	홍길동

목 차

제 1 장 총 칙	13
1. 목 적	13
2. 적용범위	13
3. 용어정의	13
4. 책임사항	14
제 2 장 개인정보보호정책	14
1. 개인정보보호정책과 지침	14
2. 개인정보보호정책의 유지 및 관리	15
3. 관련 지침서	16

제 1 장 총 칙

1. 목 적

본 정책은 OO주식회사(이하 “회사”라고 함)의 고객의 개인정보보호를 위한 최상위 정책으로서 비인가자에 의한 개인정보의 오남용, 훼손, 변조, 유출 등의 위협으로부터 개인정보자산을 보호하기 위한 기본 방침을 정립하는 것을 목적으로 한다.

2. 적용범위

본 규정서 및 지침서는 회사에 근무하는 전 임직원을 대상으로 적용되며 계약관계에 의하여 회사의 자산에 접근하는 모든 제3자에게도 적용된다.

3. 용어정의

- (1) “개인정보”라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 및 화상 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다.
- (2) “개인정보파일”이라 함은 컴퓨터 등에 의하여 처리할 수 있도록 체계적으로 구성된 개인정보의 집합물로서 자기테이프자기디스크 등 전자적인 매체에 기록된 것을 말한다.
- (3) “정보주체”라 함은 개인정보에 의하여 식별되는 자로서 당해 정보의 주체가 되는 자를 말한다.
- (4) “개인정보보호책임자”라 함은 회사의 고객의 개인정보보호를 총괄하는 자를 말한다.
- (5) “분야별 개인정보책임자”(이하 분야별 책임자)이라 함은 개인정보파일을 보유하는 부서장을 말한다.
- (6) “개인정보보호위원회”라 함은 개인정보보호를 청 전체에 걸쳐 동등한 수준으로 일관성있게 추진하기 위하여 개인정보보호에 관한 사안의 조정·심의 및 의사결정을 위한 협의체를 말한다
- (7) “취급부서장”이란 개인정보를 취급하는 부서의 장을 말하며 분야별 책임자를 포함한다.
- (8) “개인정보취급자”라 함은 개인정보에 대한 접근권한을 가진 자로서 업무를 수행하기 위하여 개인정보를 취급하는 자와 개인정보를 처리하는 시

스텝 및 단말기를 관리하는 자를 말한다.

(9) “중요 개인정보”라 함은 주민번호 및 은행 계좌정보를 말한다.

4. 책임사항

회사의 정보보호에 대한 책임은 전 임직원에게 있으며 이를 위하여 개인정보보호 정책 및 지침을 모든 임직원이 숙지하여 준수하여야 한다.

- 모든 임직원이 본 규정 및 지침서의 내용을 숙지하여 생활화하기 위해서 적절한 교육이 시행되어야 하며, 정보보호 담당팀은 이에 대한 책임이 있다.
- 법적, 규범적, 해당 감독기관의 요구사항이 만족되어야 한다.
- 모든 임직원에게 관련 정보보호 정책 및 지침이 배포되거나 또는 내부 정보통신망에 게시하고 관련 교육을 실시한다.
- 개인 정보보호 훈련이 모든 직원에게 적용되어야 한다.
- 개인 정보보호에 대한 위반은, 실제적이거나 의심스러운 경우 모두 개인정보보호책임자에게 보고되어야 하며, 개인정보보호책임자는 이를 면밀히 조사해야 한다.
- 개인정보보호책임자는 정책 및 지침의 유지관리 및 이행을 위한 충고 및 지침 제공의 직접적인 책임을 가진다.
- 개인정보보호관리자 및 개인정보보호담당자들은 그들의 업무 범주 내에서 방침의 이행에 대한 직접적인 책임을 가진다
- 개인정보보호책임자 주재 회의 시 정보보안 관련 사항이 논의되어야 한다.
- 개인정보보호책임자는 정보보안교육 실시, 불시 점검 등 정보보안 강화관련 내용을 지시한다.
- 이 방침을 지키는 것은 모든 임직원 각자의 책임이다

제 2 장 개인정보보호정책

1. 개인정보보호정책과 지침

개인정보보호정책·지침의 체계는 1개의 정책 1개의 지침으로 이루어진다. 정책은 회사의 최상위 개인정보보호정책으로 정책 및 지침의 체계를 선언하며 지침은 임직원 및 실무 개인정보보호 관련 업무 직원들이 수행해야 하는 업무 역할 및 수행 내역을 정의하였다.

개인정보보호정책과 지침은 회사의 고객의 개인정보보호를 위해 매우 중요하다. 본 정책서에 제시된 문서와 지침들은 회사의 고객의 개인정보보호를 위해 필수적이므로 모두 준수할 것을 원칙으로 한다.

개인정보보호담당자는 개인정보보호정책을 대외비 문서로 분류하여 관리한다.

1.1 개인정보보호정책의 수립

- 회사의 업무와 개인정보보호의 관계를 분석하여 사업 수행 시에 영향을 중심으로 정책 수립을 추진하여야 한다.
- 개인정보보호와 관련하여 현행 IT 아키텍처 뿐만 아니라 향후의 IT 도입 방향 및 아키텍처를 고려한다. 이를 통해 개인정보보호 체계 설계 단계에서 장기적 관점을 견지하고 향후 개인정보보호 요구에 부합하는 방향을 설정할 수 있도록 한다.

1.2 개인정보보호지침의 수립

개인정보보호정책의 효과적인 적용을 위해 적용대상의 상이한 보안 요구 수준을 고려하여 작성한다. 개인정보보호담당자는 개인정보보호 지침을 대외비 문서로 분류하여 관리한다.

- 개인정보보호지침 항목을 도출한다
- 대상이 되는 자산 및 업무 현황 파악을 바탕으로 지침을 수립하고 그 결과를 반영한다.
- 지침을 작성, 적용 검토 및 수정한다.

2. 개인정보보호정책의 유지 및 관리

2.1 지침의 검토

개인정보보호관리자는 업무환경 변화에 따라 정보보호 지침의 타당성을 연 1회 정기적으로 검토해야 하며, 필요 시 추가 검토를 수행하여 변경할 수 있다.

2.2 지침의 개정

개인정보보호와 관련하여 새로운 요구사항이 도출되거나 개인정보보호 정책 및 지침의 검토결과 개정이 필요한 경우 또는 임직원에 의해 개선안 이의,

■ 개인정보보호관리체계 인증준비 안내서(부 록)

불편사항, 문제점 등이 제기된 경우에는 개인정보보호 정책 및 지침을 개정해야 한다.

- 1) 개인정보보호관리자는 관련 전문가와 해당 실무자들과 함께 개정요인을 검토 후 개정한다.
- 2) 개정안은 개인정보보호책임자의 검토를 거친 후 담당 임원의 승인을 얻어야 한다.
- 3) 개인정보보호책임자는 개정된 정책 및 지침 사항을 모든 사용자에게 공지하고 유효기간을 고려하여 적용해야 한다.

3. 관련 지침서

본 개인정보보호정책의 적용을 위해 상세한 내용은 다음의 정보보호지침서에 별도로 규정한다.

- 1) 개인정보보호지침
- 2) 개인정보침해사고대응및복구지침

□ 지침 - ① 개인정보보호지침

대외비

문서번호

개인정보보호지침

< 개정 이력 >

개정번호	조항번호	개정내용요약	개정일자	담당자
1.0		신규제정	2009.06.01	홍길동

목 차

제 1 장 총 칙	21
제1조 (목적)	21
제2조 (적용 범위)	21
제3조 (용어 정의)	21
제4조 (개인정보 보호 원칙)	22
 제 2 장 책 임	 23
제5조 (개인정보보호책임자)	23
제6조 (분야별 개인정보보호책임자 및 개인정보보호담당자)	23
제7조 (취급부서장)	24
제8조 (개인정보취급자)	24
제9조 (개인정보보호위원회)	24
 제 3 장 개인정보파일	 25
제10조 (개인정보파일의 보유)	25
제11조 (개인정보파일의 파기)	25
제12조 (개인정보파일대장의 관리)	25
 제 4 장 개인정보보호 방침	 26
제13조 (개인정보보호방침의 수립)	26
제14조 (개인정보보호방침의 게재 및 관리)	26
 제 5 장 개인정보보호 관리	 27
제15조 (개인정보보호 계획의 수립 및 시행)	27
제16조 (개인정보보호 계획의 내용)	27
제17조 (개인정보보호 교육)	27
제18조 (개인정보취급자 및 단말기 관리)	28
제19조 (개인정보시스템 접근권한 관리)	28
제20조 (개인정보시스템 로그 기록 관리)	28
제21조 (개인정보 저장 매체 관리)	29
제22조 (악성 소프트웨어 예방 및 치료)	29
제23조 (개인정보침해사고 대응)	29

제24조 (개인정보보호의 날)	29
제 6 장 개인정보보호 라이프사이클 관리.....	29
제25조 (개인정보의 수집)	29
제26조 (인터넷 상의 본인확인)	31
제27조 (개인정보의 저장 및 전송)	31
제28조 (개인정보의 이용 및 제공의 제한)	31
제29조 (개인정보의 이용 및 제공 시 승인 및 보호조치)	31
제30조 (개인정보의 처리업무 위탁)	32
제31조 (개인정보의 출력)	33
제32조 (개인정보의 파기)	34
제33조 (이용자 권리 보호)	34
제 7 장 기타 개인정보보호 조치	35
제34조 (웹사이트 개인정보 노출 방지)	35
제35조 (개인정보영향평가)	35
[첨부 1] 개인정보파일대장	36
[첨부 2] 개인정보 접근권한 관리대장.....	37
[첨부 3] 개인정보 처리시스템의 접근기록 대장.....	38
[첨부 4] 개인정보 처리시스템의 로그관리 대장.....	39
[첨부 5] 개인정보의 이용-제공 관리대장	40
[첨부 6] 개인정보 입출력 자료 관리대장.....	41
[첨부 7] 개인정보 암호화 필드 정의서.....	42

제1장 총 칙

제1조 (목적)

본 지침은 OO주식회사(이하 “회사”라고함)에서 처리되는 고객의 개인정보를 보호하기 위하여 구체적 사항을 정하는 것을 목적으로 한다.

제2조 (적용 범위)

본 지침은 회사 내에 보유한 고객의 개인정보에 대하여 적용한다 회사의 전 임직원은 이 지침에 따라 고객의 개인정보를 안전하게 보호할 책임이 있다

제3조 (용어 정의)

- (1) “개인정보”라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 및 화상 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다.
- (2) “개인정보파일”이라 함은 컴퓨터 등에 의하여 처리할 수 있도록 체계적으로 구성된 개인정보의 집합물로서 자기테이프자기디스크 등 전자적인 매체에 기록된 것을 말한다.
- (3) “정보주체”라 함은 개인정보에 의하여 식별되는 자로서 당해 정보의 주체가 되는 자를 말한다.
- (4) “개인정보보호책임자”라 함은 회사 정보보안업무를 총괄하는 자를 말한다.
- (5) “분야별 개인정보책임자”(이하 분야별 책임자)라 함은 개인정보파일을 보유하는 부서장을 말한다.
- (6) “개인정보보호위원회”라 함은 개인정보보호를 청 전체에 걸쳐 동등한 수준으로 일관성있게 추진하기 위하여 개인정보보호에 관한 사안의 조정·심의 및 의사결정을 위한 협의체를 말한다
- (7) “취급부서장”이란 개인정보를 취급하는 부서의 장을 말하며 분야별 책임관을 포함한다.
- (8) “개인정보취급자”라 함은 개인정보에 대한 접근권한을 가진 자로서 업무를 수행하기 위하여 개인정보를 취급하는 자와 개인정보를 처리하는 시스템 및 단말기를 관리하는 자를 말한다.
- (9) “중요 개인정보”라 함은 주민번호 및 은행 계좌정보를 말한다.

제4조 개인정보 보호 원칙

개인정보는 다음의 원칙을 충족할 수 있도록 수집, 관리, 파기되어야 한다.

- (1) 개인정보 수집 시에는 그 목적을 명확히 제시하여야 한다.
- (2) 개인정보 수집은 목적에 필요한 최소한의 범위 안에서 법률에 의하거나 정보주체의 동의 등에 의해 적법하고 정당하게 수집하여야 한다
- (3) 수집한 개인정보는 목적 외의 용도로 활용하여서는 아니 된다.
- (4) 개인정보는 목적에 필요한 범위 안에서 정확하고 완전하여야 한다.
- (5) 개인정보는 목적에 필요한 범위 안에서 최신의 것이어야 한다.
- (6) 개인정보는 분실, 도난, 누출, 변조 또는 훼손되지 않도록 안전하게 보호하여야 한다.
- (7) 개인정보보호관리의 책임소재를 명확히 하여야 한다.
- (8) 개인정보의 수집·활용 등 개인정보의 취급에 관한 사항을 공개하여야 한다.
- (9) 개인정보처리에 있어서 열람 청구권 등 정보주체의 권리를 보장하여야 한다.

제2장 책임

제5조 (개인정보보호책임자)

- (1) 대표이사는 회사내의 개인정보보호를 총괄하는 부서의 장을 개인정보보호책임자를 지정한다.
- (2) 개인정보보호책임자는 회사 전체의 개인정보보호 업무를 총괄 관리할 책임이 있다.
- (3) 개인정보보호책임자의 업무는 다음과 같다.
 - (가) 개인정보보호 계획, 방침 및 관련 지침의 수립·시행
 - (나) 정보주체의 열람 청구 등 민원 및 개인정보침해신고 접수처리
 - (다) 개인정보처리실태의 점검 및 감독
 - (라) 각종 개인정보보호 관련 통계 및 자료의 취합
 - (마) 개인정보보호 관련 요건 준수 여부의 점검
 - (바) 개인정보보호 교육 등 기타 개인정보보호를 위하여 필요한 업무
- (4) 개인정보보호책임자는 개인정보보호관리자 및 담당자를 지정하여 업무를 위임하고 관련 실무를 수행하게 할 수 있다.

제6조 (분야별 개인정보보호책임자 및 개인정보보호담당자)

- (1) 분야별 개인정보책임자는 개인정보파일을 보유한 부서장을 말한다

- (2) 접수부서장은 다음과 같은 책임이 있다.
 - (가) 개인정보 수집의 목적을 명확히 제시하고 목적에 필요한 최소한의 범위 안에서 적법하고 정당하게 수집하여야 한다.
 - (나) 수집된 개인정보가 필요한 범위 안에서 정확하고 완전하며 최신의 것이 되도록 보장하여야 하며, 이를 위한 확인 절차를 수립하여야 한다.
 - (다) 수집, 확인 및 저장을 위한 보안 요구사항을 정의하고 이를 분야별 책임자 등 관련자에게 준수를 요구하여야 한다.
 - (라) 수집된 개인정보를 청 내외에서 이용 및 제공하고자 할 경우 그 용도가 수집 목적에 따른 것인지를 확인하여야 한다.
 - (마) 수집된 개인정보를 청 내외에서 이용 및 제공하고자 할 경우 보안 요구사항을 정의하고 이를 관련 취급부서장에게 준수하도록 요구하여야 한다.
 - (바) 접수된 개인정보 문서를 안전하게 보관하고 적법하게 파기하여야 한다.
- (3) 해당 개인정보보호담당자는 개인정보를 타 기관 및 업체에 제공하는 경우 적법성 및 타당성을 확인하고 안전성을 확보할 책임이 있다. 이를 위하여 다음과 같은 업무를 수행하여야 한다.
 - (가) 개인정보를 타 기관 및 업체에게 이용 또는 제공의 적법성 및 타당성을 검토하여야 한다.
 - (나) 개인정보를 타 기관 및 업체에게 이용 또는 제공 시 보안 요구사항 및 책임관계를 정의하고 타 기관 및 관련 분야별 책임관에게 이의 준수를 요구하여야 한다.
 - (다) 개인정보를 타 기관 및 업체에게 이용 또는 제공 시 보안 요구사항 만족 여부를 점검하여야 한다.
 - (라) 기타 타 기관 및 업체에게 이용 또는 제공 시 관련 개인정보보호에 관한 업무를 수행하여야 한다.
- (4) 해당 개인정보보호담당자는 회사의 개인정보를 처리하는 응용시스템의 안전성을 확보할 책임이 있다. 이를 위하여 관련 법 규정 및 보안 요구사항에 따라 개인정보처리시스템을 안전하게 설계, 개발, 구현하여야 한다.
- (5) 해당 개인정보보호담당자는 데이터베이스에 저장된 개인정보의 안전성을 확보할 책임이 있다. 이를 위하여 데이터베이스 내의 개인정보를 관리하고 중요 개인정보를 암호화하는 등 안전하게 보호하기 위한 업무를 수행하여야 한다.
- (6) 해당 개인정보보호담당자는 개인정보를 처리하는 하드웨어 및 네트워크 인프라의 안전성을 확보할 책임이 있다. 이를 위하여 개인정보처리시스템의 인프라 및 네트워크를 안전하게 운영하고 접수부서장의 승인에 따라 개인정보처리시스템의 접근권한을 설정, 관리하기 위한 업무를 수행하여야 한다.

제7조 (취급부서장)

- (1) 분야별 책임자를 포함하여, 개인정보를 취급하는 부서의 장(이하 취급부서장)은 자신의 소관 업무 분야에서 개인정보를 안전하게 취급하도록 관리·감독할 책임이 있다.
- (2) 취급부서장의 업무는 다음과 같다.
 - (가) 부서의 개인정보취급자를 지정하고 개인정보를 안전하게 취급하도록 교육 및 관리·감독
 - (나) 개인정보취급자의 접근권한 승인 및 단말기 설정 등 제반 보호장치에 관한 사항을 확인·감독
 - (다) 부서의 개인정보 이용, 제공, 열람, 정정, 삭제 등 취급 내역 및 취급자에 대한 기록 확보 및 정당성 여부의 주기적 점검을 통해 오·남용 사고를 예방
 - (라) 부서의 개인정보취급자 현황, 개인정보 취급 현황 등의 통계, 개인정보 침해 및 위법 사항 등을 개인정보보호책임자에게 통보
 - (마) 부서 내 개인정보침해사고 발생 시 침해사고대응팀과 협력하여 조사 처리 및 재발 방지 방안 수립
 - (바) 업무처리를 위해 개인정보를 유관기관에 제공하거나 접근권한을 제공할 경우 그 관리·감독
 - (사) 공개서버에 정보등록 시 개인정보나 중요자료 존재 여부의 점검
 - (아) 필요시 부서의 개인정보처리에 대한 절차 기준 및 계획 마련 등 소관 업무 분야 내 개인정보처리 및 보호에 관한 업무
 - (자) 취급 업무를 외부기관에 위탁한 경우 그 수탁기관의 개인정보보호 관리에 관한 업무
- (3) 취급부서장은 부서 내 개인정보보호담당자를 지정하여 업무를 위임할 수 있다.

제8조 (개인정보취급자)

- (1) 업무상 개인정보를 취급하는 자는 처리하는 개인정보가 훼손 및 누설되지 않도록 개인정보보호지침에 따라 안전하게 취급하여야 한다.
- (2) 직무상 알게 된 개인정보를 누설 또는 권한 없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적을 위하여 사용하여서는 안된다.
- (3) 개인정보취급자가 개인정보를 무단 조회하거나 오남용 하는 경우 내부 규정 및 관련 법규에 따라 징계 및 처벌될 수 있다.
- (4) 개인정보 접근 권한을 임의로 양도 및 대여하여서는 안 된다.

제9조 (개인정보보호위원회)

- (1) 개인정보보호위원회는 개인정보보호를 청 전체에 걸쳐 동등한 수준으로 일관성있게 추진하기 위하여 개인정보보호에 관한 사안의 조정·심의 및 의사결정을 수행한다.
- (2) 개인정보보호위원회는 개인정보보호책임자를 위원장으로 하고 분야별 개인정보보호책임자로 구성되며 필요시 관련 개인정보 취급 부서장을 포함하여 확대 운영할 수 있다.
- (3) 개인정보보호위원회의 업무는 다음과 같다
 - (가) 개인정보보호 지침의 심의 및 승인
 - (나) 개인정보보호 계획의 심의 및 승인
 - (다) 개인정보침해사고 대응
 - (라) 수집된 개인정보의 청 내외 이용 및 제공의 심의 및 승인
 - (마) 개인정보처리시스템 개발 및 운영 시 보안요구사항 심의 및 승인
 - (바) 개인정보처리 실태, 지침 및 요구사항 준수 등 점검 결과의 심의 및 승인
 - (사) 기타 개인정보보호 관련 사안의 검토, 조정, 심의 및 승인

제3장 개인정보파일

제10조 (개인정보파일의 보유)

회사는 그 소관업무를 수행하기 위하여 필요한 범위 내에서 개인정보 파일을 보유할 수 있다.

제11조 (개인정보파일의 파기)

(1) 개인정보보호책임자는 개인정보파일의 보유가 불필요하게 된 경우에는 당해 개인정보파일을 지체 없이 파기하여야 한다. 다만 다른 법률에 따라 보존하여야 하는 경우를 제외한다.

제12조 (개인정보파일대장의 관리)

- (1) 개인정보보호책임자는 보유하고 있는 개인정보파일 별로 개인정보파일 대장을 작성, 관리한다.
- (2) 개인정보파일 대장에 기재하여야 하는 사항은 다음과 같다
 - (가) 개인정보파일의 명칭
 - (나) 개인정보파일의 보유목적
 - (다) 보유기관의 명칭
 - (라) 개인정보파일에 기록되는 개인 및 항목의 범위

- (마) 개인정보의 수집방법과 처리정보를 통상적으로 제공하는 기관이 있는 경우에는 그 기관의 명칭
- (바) 개인정보파일의 열람예정시기
- (사) 열람이 제한되는 처리정보의 범위 및 그 사유
- (3) 개인정보파일 대장은 [첨부 1] 개인정보파일대장 양식에 따라 기록 관리한다.
- (4) 개인정보파일대장은 고객이 열람할 수 있도록 열람 장소를 지정하고 공개한다.

제4장 개인정보보호 방침

제13조 (개인정보보호방침의 수립)

개인정보보호책임자는 다음 각 호의 내용이 포함된 개인정보보호 방침을 수립하여야 한다.

- (1) 이 지침 제12조 2항의 개인정보파일대장의 기재사항
- (2) 보유하고 있는 개인정보파일의 보유근거 및 목적 관리자, 보호책임관, 파기시기
- (3) 개인정보파일의 열람 및 정정청구 안내
- (4) 권익침해 구제절차에 대한 안내
- (5) 개인정보보호책임자 성명, 소속 부서, 직위 및 전화번호 및 이메일 등 연락방법
- (6) 인터넷 홈페이지 접속정보파일 등 인터넷 홈페이지를 통하여 수집되는 개인정보의 보호에 관한 사항
- (7) 그 밖에 개인정보의 보호를 위하여 필요한 사항

제14조 (개인정보보호방침의 게재 및 관리)

- (1) 개인정보보호책임자는 개인정보보호 방침의 내용을 개인정보보호심의위원회의 심의를 거쳐 인터넷 홈페이지 등에 게재하여야 한다.
- (2) 개인정보보호방침을 홈페이지에 게재 시에는 홈페이지 초기화면 하단 등에 「개인정보보호방침」 웹 페이지를 하이퍼링크(Hyperlink)할 수 있도록 하는 아이콘, 배너 등을 설치하여 고객이 쉽게 찾아 볼 수 있도록 하며 전자적 표시를 함께 부착할 수 있다.
- (3) 개인정보취급방침을 변경하는 경우 그 이유 및 변경 내용을 홈페이지의 메인 화면에 별도의 알림창을 띄우거나 공지사항에 공지한다.

제5장 개인정보보호 관리

제15조 (개인정보보호 계획의 수립 및 시행)

- (1) 개인정보보호책임자는 이 지침의 내용을 반영하고 개인정보보호에 필요한 업무를 수행하기 위한 연간 개인정보보호 계획을 수립하고 시행할 책임이 있다.
- (2) 취급부서장은 소관 업무 분야 내에서의 개인정보보호에 필요한 조치를 취하기 위한 개인정보보호 계획을 수립하고 이를 개인정보보호책임자에게 제출한다.
- (3) 개인정보보호책임자는 취급부서장의 개인정보보호 계획을 취합·조정하여 개인정보보호 계획을 수립하고 개인정보심의위원회를 개최하여 확정한다
- (4) 개인정보보호책임자는 차년도 정보보호 계획 수립 전에 정보보호 계획의 시행 여부를 점검하고 차년도 정보보호 계획 수립 시 반영한다.

제16조 (개인정보보호 계획의 내용)

개인정보보호 계획은 다음 사항을 포함하여야 한다.

- (1) 개인정보보호 교육
- (2) 부서별 개인정보보호 준수 점검 및 실태 조사
- (3) 웹사이트 개인정보 노출 점검 및 보완
- (4) 개인정보보호관련 지침의 검토 및 개정
- (5) 기타 개인정보보호를 위하여 필요한 업무 계획

제17조 (개인정보보호 교육)

개인정보보호를 위하여 다음과 같이 교육을 수행하여야 한다.

- (1) 개인정보보호책임자 및 취급부서장은 연 1회 이상 개인정보보호 교육에 참석하여야 한다.
- (2) 개인정보보호 관리자 및 담당자는 연 20시간 이상의 개인정보보호 전문 교육을 참석하여야 한다.
- (3) 취급부서장은 소관 업무 분야 내에서 개인정보 취급 업무를 처음 시작하는 자에게 관련 법령에 따른 의무사항 및 처벌규정을 주지시켜야 한다
- (4) 취급부서장은 소관 업무 분야 내의 개인정보취급자에게 연회 이상 개인정보보호 교육을 실시하여야 한다.
- (5) 개인정보보호교육 내용에는 이 지침 및 관련 지침에서 교육대상자에 관하여 규정한 사항을 최소 연 1회 이상 포함하여야 한다.
- (6) 개인정보보호책임자는 전 직원의 개인정보보호 인식 제고를 위한 교육 기회를 제공하여야 한다.

(7) 교육 시행 후 교육 결과를 평가하여 차기 교육 계획에 반영하여야 한다.

제18조 (개인정보취급자 및 단말기 관리)

(1) 취급부서장은 소관 업무 분야 내에서 개인정보를 취급하는 자를 업무 수행에 필요한 최소한으로 제한하여 개인정보취급자로 지정하여야 한다

(2) 취급부서장은 소관 업무 분야 내의 개인정보취급자 명단을 관리하여야 한다.

(3) 취급부서장은 소관 업무 분야 내의 개인정보취급자가 개인정보를 안전하게 처리할 수 있도록 취급 업무를 지도·감독하고 교육 등 필요한 적절한 조치를 취해야 한다.

(4) 취급부서장은 소관 업무 분야 내에서 개인정보를 취급하는 단말기를 안전하게 설치하고 개인정보 단말기별로 개인정보취급자를 지정하여 관리하여야 한다.

(5) 취급부서장은 개인정보 취급 단말기의 공유 설정을 원칙적으로 금지하고 이메일이나 인터넷사이트 접속 메신저, P2P등을 통해 개인정보가 포함된 파일이 전송되지 않도록 설정·관리하여야 한다.

(6) 개인정보취급자가 다수인 경우 취급부서장은 부서 내 개인정보관리자를 지정하여 업무를 위임할 수 있다.

(7) 취급부서장은 [첨부 2] 개인정보 접근권한 관리대장 양식에 따라 개인정보취급자에 대한 권한을 기록 관리한다.

제19조 (개인정보시스템 접근권한 관리)

(1) 취급부서장은 개인정보처리시스템의 접근 권한을 개인정보취급자의 업무에 따라 세분화하여 할당하여야 한다.

(2) 취급부서장은 일반 개인정보 외 주민등록번호 및 계좌번호 등의 중요 개인정보는 업무 수행을 위해 반드시 필요한 경우에만 접근 권한을 허용하여야 한다.

(3) 비정규직의 경우 원칙적으로 개인정보취급자로 지정할 수 없으니 부득이한 경우 유효기간을 한정하는 등의 보안 조치를 강구한 후 취급부서장의 문서승인을 받아 허용할 수 있다.

(4) 취급부서장은 [첨부 3] 개인정보 처리시스템의 접근기록 대장 양식에 따라 개인정보 처리시스템의 접근기록을 관리한다.

제20조 (개인정보시스템 로그 기록 관리)

(1) 개발부서장은 개인정보에 대한 입력 출력, 변경 사건에 대하여 데이터별 파일 별 접근 내역의 로그 기록을 남기고 최소한 최근 3개월 분을 관리

하여야 한다.

(2) 취급부서장은 개인정보의 오남용 사고를 예방하기 위하여 개인정보처리 로그 기록을 주기적으로 분석하여 오남용 여부를 확인하여야 한다.

(3) 개발부서장은 [첨부 4] 개인정보 처리시스템의 로그관리 대장 양식에 따라 개인정보 처리시스템의 로그를 관리한다

제21조 (개인정보 저장 매체 관리)

(1) 개인정보를 매체에 저장할 경우에는 보안 USB등 보안성이 높은 저장매체를 사용하고 반드시 암호화하여 저장하여야 한다.

(2) 개인정보를 저장매체에 저장하여 이동할 경우 안전하게 이동 한 후 그 저장매체의 처리 정보를 완전히 파기하여야 한다.

(3) 개인정보를 저장한 매체는 회사 정보보안업무 세부지침 별지8호 서식을 따라 라벨을 부착하여야 한다.

(4) 매체 및 저장 개인정보의 파기에 관해서는 이 지침 '제32조 개인정보의 파기'를 따른다.

제22조 (악성 소프트웨어 예방 및 치료)

개인정보처리시스템 및 단말기의 악성 소프트웨어 예방 및 치료에 대해서는 PC 보안지침을 따른다.

제23조 (개인정보침해사고 대응)

개인정보 침해사고 대응에 관해서는 「개인정보침해사고 대응 및 복구지침」을 따른다.

제24조 (개인정보보호의 날)

(1) 개인정보보호책임자는 매월 1일을 개인정보보호의 날로 지정하여 관련 정책을 홍보하고 개인정보보호의 중요성을 인지시킨다.

(2) 정책 홍보 시에는 웹사이트 및 내부 업무관리시스템 초기화면에 플래시나 지침을 게재하는 등 다양한 보안 홍보 및 이벤트를 수행한다.

(3) 1일이 휴일인 경우 다음 평일에 시행한다.

제6장 개인정보 라이프사이클 관리

제25조 (개인정보의 수집)

(1) 수집부서장은 수집 목적을 명확히 하여야 하고, 목적에 필요한 최소한의

범위 안에서 적법하고 정당하게 수집하여야 하며, 목적 외의 용도로 활용하여서는 안된다.

(2) 수집부서장은 사상·신조등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 안 된다. 다만, 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 가능하다.

(3) 수집부서장은 개인정보 수집 시 정보를 제공하는 사람이 본인 또는 합법적인 대리인임을 확인하기 위한 본인확인 절차를 수립하여야 한다

(4) 신규로 개인정보를 수집하거나 변경, 삭제하고자 하는 경우에는 개인정보 보호책임자의 승인을 받는다.

(5) 개인정보보호책임자는 개인정보 수집 시 이에 관한 사항을 이 지침 제4장의 규정에 따라 정보보호 방침을 통하여 공개한다.

(6) 개인정보보호책임자는 신규 개인정보 수집이나 변경 삭제 시 제12조에 따라 처리한다. 개인정보보호책임자는 필요한 경우 관련 사항을 결정 및 처리하기 위하여 개인정보보호위원회를 소집할 수 있다.

(7) 개인정보의 수집과 그 보호대책의 방법에 관하여서는 개인정보 수집·장·이용·과기에 관한 절차서를 따른다.

제26조 (인터넷 상의 본인확인)

개발 분야의 분야별 책임자는 인터넷 상의 본인확인이 필요한 경우 이 과정에서 주민등록번호, 성명 등의 개인정보가 변조·유출 또는 도용되지 않도록 I-PIN 등의 안전성 확보에 필요한 조치를 취해야 한다.

제27조 (개인정보의 저장 및 전송)

- (1) 개인정보처리시스템에 중요 개인정보를 저장할 경우에는 전부 또는 일부를 암호화하여 저장하여야 한다. DB 담당자는 [첨부 7] 암호화 필드 정의서에 따라 개인정보를 암호화하여 저장하여야 한다.
- (2) 개인정보를 PC나 노트북에 저장할 경우에는 반드시 암호화하여 저장하여야 한다.
- (3) 개인정보를 정보통신망을 통하여 송·수신하는 경우 개인정보가 분실·도난·누출·변조 또는 훼손되지 않도록 PKI 및 이에 상응하는 보안기술을 적용하여 암호화 등의 안전 조치를 취하여야 한다.
- (4) 회사에서 제공하는 메일 시스템 외의 일반 상용 메일, 웹하드 등을 통하여 개인정보를 송수신하여서는 안된다.
- (5) 개인정보의 저장 및 전송 방법에 관하여서는 개인정보 수집·저장·이용·파기에 관한 절차서를 따른다.

제28조 (개인정보의 이용 및 제공의 제한)

- (1) 취급부서장은 개인정보 수집 시의 보유 목적 외의 목적으로 처리정보를 회사 내부 또는 회사 외의 자에 대하여 이용하게 하거나 제공하여서는 안된다.
- (2) 취급부서장은 보유 목적에 따라 처리정보를 이용하게 하거나 제공하는 경우에도 업무 수행에 필요한 최소한의 범위로 그 이용 또는 제공을 제한하여 승인하여야 한다.
- (3) 취급부서장의 승인을 받아 처리정보를 이용하는 자는 취급부서장의 동의 없이 당해 처리 정보를 제3자에게 이용하게 하거나 제공해서는 안 된다.
- (4) 개인정보보호책임자는 정보통신망을 통해 외부 기관 및 업체에 처리정보를 이용·제공하는 경우 최소한의 항목으로 제한하여 이용하도록 제한하여야 한다.
- (5) 개인정보의 이용 및 제공 제한에 관한 방법에 관하여서는 개인정보 수집·저장·이용·파기에 관한 절차서를 따른다.

제29조 (개인정보의 이용 및 제공 시 승인 및 보호조치)

- (1) 취급부서장은 소관 업무 분야의 개인정보를 정보주체 외의 자에게 이용

하게 하거나 제공하는 때에는 처리 정보를 수령한 자에 대하여 사용목적사용방법 기타 필요한 사항에 대하여 제한을 하거나 처리정보의 안전성확보를 위하여 필요한 조치를 명시하여 요구하여야 하며, 이러한 요청을 받은 정보수령자는 필요한 조치를 취하여야 한다.

(2) 외부 기관으로부터 이용·제공 요청을 받은 경우 취급부서장은 다음의 사항을 검토하여 적정한 경우 개인정보보호책임자의 승인을 받아 해당 정보를 요청기관에게 제공하고 그 내용을 [첨부 5] 개인정보의 이용·제공 관리대장'에 기록한다.

(가) 법률 등 요청 근거 및 이용 목적의 정당성

(나) 목적달성에 필요한 최소한의 범위 제공

(다) 당해 개인정보를 제공함으로써 개인이 입는 사생활 침해와 그로 인해 얻는 공익상의 목적과의 비례관계 유지

(라) 이용·제공받는 기관의 처리정보 안전성 확보 대책의 적정성 등

(3) 취급부서장은 정보수령자에 대하여 사용 목적 외 사용 금지 및 안전성 확보 조치 준수 여부를 지속적으로 관리하고 만일 준수하지 않을 경우에는 수령자에게 시정을 요구하고 처리 정보의 파기를 요청하여야 한다 또한 이용·제공 목적 외 이용 시에는 고발 등의 조치를 취해야 한다.

(4) 개인정보보호책임자는 처리정보를 이용하거나 제공받은 기관 및 업체가 본래 목적 이외에 개인정보를 이용하는 경우 즉시 처리정보의 이용을 중지시키거나 제공을 중지하여야 한다.

(5) 개인정보의 이용 제공시 보호조치에 관하여서는 개인정보 수집·저장·이용·파기에 관한 절차서를 따른다.

제30조 (개인정보의 처리업무 위탁)

(1) 개인정보 처리 및 개인정보처리시스템 관리 업무를 외부기관 및 업체에 위탁하는 경우에도 개인정보보호에 대한 책임은 해당 업무의 취급부서장에게 있다.

(2) 해당 취급부서장은 소관 업무 부서 내의 업무와 마찬가지로 수탁기관이 개인정보를 안전하게 보호하도록 지도·감독하여야 한다.

(3) 해당 취급부서장은 위탁 관리할 개인정보 처리 범위 등 위탁범위를 설정하고 위탁관리 계획서 및 계약 요구사항을 작성하여야 한다.

(4) 위탁관리 계약 요구사항에는 다음 사항을 포함하여야 한다

(가) 재위탁 금지

(나) 개인정보사고 발생 시 공무원에 준한 처벌 및 손해배상 의무

(다) 회사 개인정보지침 준수

(라) 회사에 의한 개인정보보호 실태조사 권한

- (마) 개인정보취급 직원의 교육 책임
- (바) 수탁기관의 준수 의무 위반 시 처리 방법
- (사) 기타 위탁 업무에 따른 개인정보보호에 필요한 사항
- (4) 위탁관리 계약 요구사항은 개인정보보호책임자의 승인을 받아야 하며 계약 부서에서는 위탁 계약서에 이를 반영하여야 한다.
- (5) 개인정보 처리에 관한 업무를 위탁하는 경우 이를 정보보호방침에 포함하여 공개하여야 한다.
- (6) 개인정보보호책임자는 필요시 위탁관리 계약 요구사항의 검토 및 위탁의 공개에 관하여 개인정보보호위원회를 소집하여 심의할 수 있다.
- (7) 해당 취급부서장은 최소 연 2회 이상 수탁기관에 대한 실태 점검을 수행하고 그 결과를 개인정보보호책임자에게 보고하여야 한다.

제31조 (개인정보의 출력)

- (1) 취급부서장은 소관 업무분야 내에서 개인정보가 기록된 출력자료와 기록 매체가 유출되지 않도록 시건장치가 된 캐비닛 등에 안전하게 보관하여야 하며, 활용이 종료된 출력자료 등은 즉시 파기하여야 한다. 파기 방법은 이 지침 '제32조 개인정보의 파기를 따른다.
- (2) 개인정보취급자는 개인정보를 종이로 인쇄하거나 보안 USB 메모리 등 이동 가능한 저장매체에 복사할 경우 취급부서장의 사전 승인을 받고 개인정보가 기록된 입출력 자료를 [첨부 6] 개인정보 입출력 자료 관리대장에 기록하여야 한다. 출력, 복사물로부터 다시 복사하는 경우에도 적용된다. 단, 자동 기록이 남는 경우에는 제외한다.
- (3) 취급부서장은 개인정보를 인쇄 및 저장매체에 복사할 경우 그 적절성을 검토하여 적절한 경우 승인하여야 하며 개인정보취급자에게 불법 유출 시 법적 책임을 지게 됨을 주지시켜야 한다.
- (4) 개인정보가 기록되는 출력 자료에는 출력 일시, 면수 표시 및 출력 장비 고유번호 등이 당해 출력자료에 자동으로 기록되도록 하여야 한다.
- (5) 취급부서장은 개인정보처리시스템에서 파일 또는 문서로의 개인정보 출력 기능에 대하여 용도를 특정하고 용도에 따라 출력할 항목을 최소화하여 정의하고 이의 준수를 개발부서장에게 요구하여야 한다
- (6) 취급부서장은 개인정보처리시스템에서 개인정보 출력 화면에 대하여 업무 내용 및 취급자의 권한에 따라 최소한의 정보만을 표시하거나 중요 개인정보의 일부 또는 전부를 마스킹하도록 화면을 정의하고 이의 준수를 개발부서장에게 요구하여야 한다.
- (7) 취급 부서장은 입출력 자료의 파기를 확인하고 파기일을 기록관리하여야 한다.

제32조 (개인정보의 파기)

- (1) 취급부서장은 소관 업무 내에서 보유하고 있는 개인정보의 해당 목적을 달성한 경우 해당 개인정보를 지체 없이 파기하여야 한다. 이때 위탁 또는 제3자에게 제공한 개인정보도 함께 지체 없이 파기하도록 하여야 한다.
- (2) 개인정보의 파기 시에는 해당 개인정보를 복구할 수 없도록 완전히 삭제하여야 한다. 종이문서의 경우 파쇄, 소각, 용해 등의 방법을 사용하며 저장 매체를 재사용하지 않을 경우 해당 매체를 물리적으로 파쇄하는 등의 방법을 사용한다.
- (3) 외부 위탁업체를 사용하여 파기할 경우에는 청 직원이 이동 및 파기를 참관하고 사진 등 증적자료를 첨부하여 파기사실을 대장으로 관리하여야 한다.
- (4) 개인정보의 파기 방법에 관하여서는 개인정보 수집·저장·이용·파기에 관한 절차서를 따른다.

제33조 (이용자 권리 보호)

- (1) 개인정보보호책임자는 개인정보 관련 이용자 의견 및 불만을 접수 처리하기 위하여 상담창구를 운영하여야 한다.
- (2) 개인정보보호책임자는 이용자 및 이용자의 법적 대리인이 이용자의 개인정보에 대한 열람, 정정, 파기 또는 이용 및 제공 내역을 청구할 수 있도록 창구를 운영하여야 한다.
- (3) 개인정보에 대한 열람, 정정, 파기 또는 이용 및 제공 내역의 청구방법은 개인정보 수집 시 보다 어려워서는 안된다.
- (4) 개인정보보호책임자는 청구자가 이용자 및 이용자의 정당한 법적대리인인지 여부를 확인하여야 한다.
- (5) 개인정보보호책임자는 이용자의 개인정보 열람 정정, 파기 또는 이용 및 제공 내역을 청구할 경우 지체 없이 필요한 조치를 취하여 10일 이내에 처리되도록 하여야 한다. 단, 관련 법률에 따라 타당한 사유가 있는 경우 그 사유를 통보하고 거절할 수 있다.
- (6) 오류의 정정요구를 받은 경우 그 오류를 정정할 때까지 해당 개인정보를 이용 또는 제공해서는 안되며, 외부 위탁 또는 제3자에게 제공한 개인정보가 있을 경우 이에 대해서도 정정조치를 취하고 결과를 확인하여야 한다.
- (7) 개인정보보호책임자는 이용자에게 불복청구 방법을 안내하여야 한다.
- (8) 개인정보보호책임자는 이용자의 요청 및 처리에 대한 모든 기록을 유지 관리하여야 한다.

제7장 기타 개인정보보호 조치

제34조 (웹사이트 개인정보 노출 방지)

- (1) 홈페이지 자료 게재 시 취급부서장은 개인정보 노출 여부를 검토하여 게재한다.
- (2) 웹사이트 개인정보 노출 예방·점검 및 웹사이트 개인정보 노출 취약점 점검에 대해서는 「개인정보침해사고 대응 및 복구지침」 제11조 (개인정보 침해 예방 및 탐지)를 따른다.

제35조 (개인정보영향평가)

개인정보보호책임자는 필요시 개인정보파일 및 개인정보처리시스템에 관하여 개인정보영향평가를 실시할 수 있다. 개인정보영향평가에 대해서는 「개인정보영향평가지침」을 따른다.

[첨부 1] 개인정보파일대장

개인정보파일대장

파 일 명	
보 유 목 적	
보 유 근 거	
수 집 방 법	
대상개인범위	
대상인원수	
보 유 기 간	
기 록 항 목 (항 목 수)	

첨부 3] 개인정보 처리시스템의 접근기록대장

개인정보 처리시스템의 접근기록대장

번호	자료의 종류	주요항목	시스템 : [] 의 접근 기록				처리부서장
			사용목적	접근발생일시	접근중지일시	처리담당자	

[첨부 4] 개인정보 처리시스템의 백업관리 대장

개인정보 처리시스템의 백업관리 대장

()월

시스템 담당자	시스템 관리자

작성일: 년 월 일

()월 로그관리 일정에 따라 아래의 시스템에 대한 백업을 실시하였음

시스템명	백업종류	보관장소	담당자	비고
참고 사항				

[첨부 5] 개인정보의 이용·제공 관리대장

개인정보의 이용·제공 관리대장

정보명			
이용·제공받는 기관(업체)			
이용·제공일자		이용·제공주기	
이용·제공형태		이용·제공기간	
이용·제공목적			
이용·제공근거			
이용·제공항목			
비고			

[첨부 7] 개인정보 암호화 필드 정의서

개인정보 암호화 필드 정의서

암호화 대상 개인정보	암호화 방법	출력 구분	출력시
주민번호	(전체 암호화 저장을 원칙으로 함)	화면	뒷자리 7자리 마스킹
계좌정보	(전체 암호화 저장을 원칙으로 함)	출력물	뒷자리 4자리 마스킹

□ 지침 - ② 개인정보보호 침해사고 대응 및 복구지침

대외비

문서번호	
호	

개인정보 침해사고 대응 및 복구지침

목 차

제 1 장 총 칙	47
제1조 (목적)	47
제2조 (적용 범위)	47
제3조 (용어 정의)	47
제 2 장 개인정보침해사고에 관한 책임	47
제4조 (개인정보보호책임자)	47
제5조 (개인정보침해사고대응팀)	47
제6조 (침해사고처리책임자)	47
제7조 (개인정보보호담당자)	48
제8조 (정보보호책임자)	48
제9조 (전직원)	48
제 3 장 침해사고의 분류	48
제10조 (개인정보침해의 분류)	48
제 4 장 개인정보침해 대응 절차	48
제11조 (개인정보침해 예방 및 탐지)	48
제12조 (개인정보침해의 신고)	49
제13조 (개인정보보호 계획의 수립 및 시행)	49
제14조 (개인정보침해 대응체계)	49
제15조 (침해사고의 분석)	50
제16조 (침해사고의 대응 및 복구)	50
제17조 (침해사고의 종료)	50
제18조 (침해사고 사후분석)	50
제 5 장 개인정보침해사고의 관리	51
제19조 (개인정보침해사고의 보고)	51
제20조 (개인정보침해사고의 현황 관리)	51
제21조 (개인정보침해사고 교육훈련)	51
제 6 장 기 타	51
제22조 (개인정보침해 신고자의 보호)	51
제23조 (개인정보침해 신고자의 보상)	51
[첨부 1] 개인정보침해사고 관리대장	52
[첨부 2] 개인정보침해사고 처리보고서	53
[첨부 3] 개인정보 침해사실 신고서	54

제1장 총 칙

제1조 (목적)

본 지침은 「개인정보보호 지침」 제23조에 의거하여 개인정보침해사고 발생 시 사고대응 및 처리방법과 이를 위한 사전 준비사항을 정의함을 목적으로 한다

제2조 (적용 범위)

본 지침의 적용 범위는 「개인정보보호 지침」의 적용 범위를 따른다.

제3조 (용어 정의)

- (1) “개인정보”의 정의는 개인정보보호 지침의 정의를 따른다
- (2) “개인정보침해”라 함은 법적 근거, 규정 또는 본인 동의에 의하지 않고 이루어지는 개인정보의 수집, 저장, 이용 및 제공, 파기행위 일체를 말한다.
- (3) “개인정보보호책임자”, “개인정보보호담당자”, “개인정보보호위원회”라 함은 「개인정보보호 지침」의 정의에 따른다
- (4) “침해사고 처리책임자”라 함은 해당 개인정보침해사고가 발생한 부서의 장이 된다. 발생 부서가 분명치 않은 경우에는 개인정보보호담당자가 발생 부서가 명확해 질 때까지 그 역할을 담당한다.

제2장 개인정보침해사고에 관한 책임

제4조 (개인정보보호책임자)

- (1) 개인정보침해사고 예방, 처리 및 재발방지의 총괄 관리 책임을 진다
- (2) 개인정보침해사건 발생 시 침해사고 처리책임자를 지정하고 개인정보침해사고 대응팀을 소집하여 운영한다.

제5조 (개인정보침해사고 대응팀)

개인정보보호위원회의 구성원으로 구성되며 개인정보보호책임자가 해당 침해사고 분석, 대응 및 복구에 필요한 관련자를 지정하여 소집한다. 필요시 업무 담당자, 홍보부서, 법무부서, 외부 전문가 등이 포함될 수 있다.

제6조 (침해사고 처리책임자)

해당 침해사고의 발생 부서의 장으로 지정되며 처리 및 재발방지에 대한 책

임을 지고 개인정보침해사고 대응팀과 협력하여 사고를 해결한다

제7조 (개인정보보호담당자)

- (1) 개인정보침해사고를 접수하고 제10조의 기준에 따라 등급을 분류하여 침해사고 대응 절차를 개시한다.
- (2) 개인정보침해사고 대응팀의 간사로서 대내외 비상연락망을 관리하고 팀 내 연락 및 조정을 담당한다.
- (3) 개인정보침해기록을 관리하고 필요시 관련자 및 기관에 보고한다

제8조 (정보보호관리자)

정보보호관리자는 침해사고가 기술적인 분석을 요할 경우 이에 대한 지원을 제공한다.

제9조 (전직원)

회사 내의 모든 임직원 및 계약직원은 회사의 개인정보에 대한 침해가 발생한 것을 인지한 경우 개인정보보호담당자에게 신고하여야 한다.

제3장 침해사고의 분류

제10조 (개인정보침해의 분류)

개인정보침해사고는 다음과 같이 3등급으로 분류한다.

- (1) 1등급 침해는 법적 근거, 규정 또는 본인의 동의 없이 개인정보가 회사 외부의 제3자에게 노출 또는 제공된 것을 말한다.
- (2) 2등급 침해는 법적 근거, 규정 또는 본인의 동의 없이 개인정보를 수집 접근, 분석, 이용, 내부자에게 제공, 저장, 파기하는 것을 말한다.
- (3) 3등급 침해는 안전하지 않은 상태로 개인정보를 저장하거나, 파기해야 할 정보를 파기하지 않는 등 개인정보보호 지침의 규정을 위반한 것을 말한다

제4장 개인정보침해 대응 절차

제11조 (개인정보침해 예방 및 탐지)

- (1) 홈페이지 담당자는 웹사이트를 통한 개인정보 노출을 예방하기 위하여

개인정보 노출차단 솔루션을 운영하고 월별 현황을 관리한다

- (2) 홈페이지 담당자는 분기별로 웹페이지, 첨부파일, 소스코드 및 외부 검색 엔진 상의 노출을 점검하고 분기별 현황을 관리한다.
- (3) 고객이 게시판 등에 자료를 게재할 때 개인정보 노출에 대하여 주의를 환기시키기 위한 경고를 제공하여야 한다.
- (4) 개인정보보호담당자는 반기별로 웹사이트의 개인정보 노출 취약점 점검을 시행하고 개인정보보호책임자에게 결과를 보고한다.

제12조 (개인정보침해의 신고)

회사의 모든 임직원 및 계약직원은 회사의 개인정보에 대하여 제0조에서 정의한 침해가 발생한 것을 인지한 경우 또는 그러한 침해의 발생이 의심되는 경우 지체없이 개인정보보호담당자에게 신고하여야 한다.

제13조 (개인정보침해사고의 접수)

- (1) 개인정보보호담당자는 개인정보침해사고를 접수한 경우 [별첨1] “개인정보 침해사고 관리대장”에 사고 접수를 기록한다.
- (2) 개인정보보호담당자는 접수 후 지체 없이 개인정보보호책임자에게 보고한다.

제14조 (개인정보침해 대응체계)

- (1) 개인정보보호책임자는 노출 또는 제공된 정보의 종류에 따라 또는 발생 부서의 담당 부서장으로 침해사고 처리책임자를 지정하고 개인정보침해사고 대응팀을 구성한다.
- (2) 발생 부서를 적시할 수 없거나 담당 부서장이 침해사고에 연루된 경우 개인정보보호책임자가 임의로 침해사고 처리책임자를 지정할 수 있다
- (3) 개인정보침해사고 대응팀은 개인정보보호위원회의 구성원 중에서 사안에 따라 선정한다. 필요시 정보보호책임자, 업무 담당자, 홍보부서, 법무부서, 외부 전문가 등이 포함될 수 있다.
- (4) 2등급 또는 3등급 침해의 경우 개인정보보호책임자는 침해사고처리책임자와 협의하여 개인정보침해사고 대응팀을 구성하지 않을 수 있다
- (5) 개인정보보호책임자는 필요시 외부 전문가에게 분석을 의뢰할 수 있다
- (6) 개인정보보호책임자가 유관기관 또는 사법기관 등에 대한 협조 요청 또는 신고가 필요하다고 판단할 경우 대표이사의 승인을 받아 시행한다

제15조 (침해사고의 분석)

- (1) 침해사고 처리책임자는 침해 사실 여부를 확인하고 사실로 확인될 경우 침해의 규모, 경위, 방법, 원인 및 관련자를 조사한다.
- (2) 침해사고 처리책임자는 필요한 경우 개인정보침해사고 대응팀 또는 개인정보보호책임자가 승인한 외부 전문가의 지원을 받아 증거자료를 수집한다.

제16조 (침해사고의 대응 및 복구)

- (1) 1등급 침해의 경우 침해사고 처리책임자는 해당 개인정보를 파기 또는 회수하기 위한 조치를 취한다.
- (2) 2등급 침해의 경우 침해사고 책임자는 해당 개인정보를 파기, 회수 또는 복구하기 위한 조치를 취하거나 정보주체의 사후 동의를 받아 근거를 마련한다.
- (3) 3등급 침해의 경우 침해사고 처리책임자는 해당 개인정보를 적절히 보호하거나 파기하기 위한 조치를 취한다.
- (4) 침해사고 처리책임자는 즉각적 조치가 가능한 경우 재발방지 조치를 취한다.

제17조 (침해사고의 종료)

- (1) 침해사고 처리책임자는 [별첨 2] 개인정보침해사고 처리보고서를 작성하여 개인정보보호책임자에게 제출한다.
- (2) 개인정보보호책임자는 개인정보침해사고 처리보고서를 검토하고 승인한다.
- (3) 개인정보보호책임자는 개인정보침해 관련자에 대한 처분을 징계위원회에 회부한다.
- (4) 개인정보보호담당자는 개인정보침해사고 처리보고서를 관리하고 징계조치 결과를 기록한다.

제18조 (침해사고 사후분석)

- (1) 침해사고 처리책임자는 처리보고서 제출 후 30일 이내 근본원인 분석, 교훈 및 예방을 위한 개선대책을 마련하여 개인정보보호책임자에게 제출한다.
- (2) 개인정보보호책임자는 개선안을 검토하여 시행 및 변경 여부와 시기를 결정한다. 필요한 경우 개인정보보호위원회를 통해 결정할 수 있다.
- (3) 개인정보보호책임자는 필요하다고 판단할 경우 사고의 교훈을 적절한 대상을 지정하여 전파할 수 있다.
- (4) 개인정보보호책임자는 개선안 시행 및 교훈 전파 후 그 성과를 검토한다.

제5장 개인정보침해사고의 관리

제19조 (개인정보침해사고의 보고)

- (1) 개인정보보호책임자는 1등급 사고의 경우 발생 즉시 및 수시로 그 진행 현황을 대표이사에게 보고한다.
- (2) 개인정보보호담당자는 반기별로 등급별·유형별 침해사고 발생 및 처리 현황을 개인정보보호책임자에게 보고한다.

제20조 (개인정보침해사고의 현황 관리)

개인정보보호책임자는 개인정보침해사고 현황을 분석하여 추가적인 개선대책이 필요한 경우 개선 대책을 마련하여 시행한다. 개선 대책에는 교육자료 활용 등을 포함할 수 있다.

제21조 (개인정보침해사고 교육훈련)

- (1) 개인정보보호책임자는 전 직원에게 연 1회 이상 개인정보침해사고의 유형과 보고 방법을 교육하여야 한다.
- (2) 개인정보보호책임자는 연 1회 이상 개인정보침해사고 시나리오를 마련하여 모의훈련을 실시하여야 한다.

제6장 기타

제22조 (개인정보침해 신고자의 보호)

- (1) 개인정보침해 신고자의 신분은 침해사고 대응에 반드시 필요한 경우 반드시 필요한 담당자 및 권한자에게만 제공되어야 하며 외부로 노출되어서는 안된다.
- (2) 개인정보침해 신고자는 어떠한 경우에도 신고로 인해 불이익을 당하는 경우가 없어야 한다.

제23조 (개인정보침해 당사자에게 통보)

개인정보담당자는 개인정보 유출사실을 인지하였을 경우 지체 없이 해당 정보주체에게 관련 사실을 통지한다.

[첨부 1] 개인정보침해사고 관리대장

접 수		신 고 개 요	등급	처리 유형	종결 일자	처리내용	비고
일 시	신고자 유형						

- ※ 접수 일시는 신고 접수 일시를 기록
- ※ 신고자 유형은 직원/고객으로 구분
- ※ 신고 개요는 신고 내용을 기록
- ※ 등급은 1/ 2/ 3등급으로 구분
- ※ 처리유형은 사실 확인 중/ 상담 및 자료제공/ 타기관 이송/ 위법성 통보/ 수사 의뢰/ 범위만 확인 불가/ 기타(징계위원회 회부)로 구분
- ※ 종결일자는 개인정보침해사고 처리보고서 접수일을 기준으로 기록
- ※ 처리 내용은 처분 유형을 사법처리(징역, 벌금, 추징, 재판계류중, 수사중)/ 징계 처분(파면, 해임, 정직, 감봉, 견책, 기타)로 구분
- ※ 비고란에는 처리보고서 문서번호를 기록

[첨부 2] 개인정보침해사고 처리보고서

보 고 일 자	0000년 00월 00일	문 서 번 호	
침해 신고 / 접수 정보			
침해등급	<input type="checkbox"/> 1등급 <input type="checkbox"/> 2등급 <input type="checkbox"/> 3등급	침해대상정보	<input type="checkbox"/> 일반 개인정보 <input type="checkbox"/> 주민번호 <input type="checkbox"/> 계좌번호
접수일시		신고자	
침해사고 처리책임자		신고자 연락처	
신고내용			
대응 과정	일시	대응 활동	
침해 내용	확인된 침해 정보의 세부사항, 규모 및 침해 방법(노출, 외부자 제공, 수집, 접근, 분석, 이용, 내부자 제공, 불법 저장, 불안정한 저장, 파기, 비파기 등 세부사항)		
침해 발생 경위			
관련자			
침해 발생 원인			
증거자료			
복구 및 재발방지 조치			
처분			

[첨부 3] 개인정보 침해사실 신고서

개인정보 침해사실 신고서

신고인	성 명		
	생년월일		
	연락처	전화번호(핸드폰)	
		전자우편	
		주 소	
접수부서	부 서 명		
	연락처	전화번호	
		주 소	
신고내용			
<p>위와 같이 개인정보침해사실을 신고합니다.</p> <p>첨부 :</p> <p> 년 월 일</p> <p> 신고인 : (서명 또는 인)</p>			

□ 절차서·기술서·계획서 - ① 교육 계획서

대외비

문서번호	
호	

개인정보보호 교육 계획서

< 개정 이력 >

개정번호	조항번호	개정내용요약	개정일자	담당자
1.0		신규제정	2009.06.01	홍길동

목 차

1. 추진배경	59
2. 교육 목표 및 추진 방법	59
3. 세부 교육 계획	59
4. 교육 실적 관리	61
[첨부 1] 개인정보보호 교육 관리 대장	62
[첨부 2] 개인정보교육 참석자 확인서	63
[첨부 3] 개인정보교육 교육 결과 설문서	64
[첨부 4] 개인정보교육 교육 공고문 예시	65

1. 추진 배경

개인정보보호 관련 법률 및 회사의 개인정보보호지침을 준수하고 고객의 개인정보를 안전하게 보호하기 위하여 개인정보의 관리 책임을 갖는 임원 및 개인정보취급자들에게 대한 인식 제고 교육이 필요하다

2. 교육목표 및 추진방법

- 교육 목표

외부환경에 대응하여 고객의 개인정보를 보호할 수 있도록 개인정보보호 인식 및 역량 강화를 목표로 한다.

☞ 근거) 1. 개인정보보호지침 제17조

- 대상 인원 : 개인정보보호책임자 이하 전직원 및 외주직원

- 1) 개인정보보호책임자 및 분야별 책임자
- 2) 개인정보보호관리자 및 담당자
- 3) 개인정보취급부서장
- 4) 개인정보취급자 및 외주직원
- 5) 전직원

- 추진 방향

- 개인정보보호책임자 및 취급부서장의 책임 교육을 통해 법 규정 요구사항 준수
- 개인정보보호 담당자 및 취급자에 대한 교육을 통해 개인정보보호 강화 및 무지에 의한 오남용 억제
- 전직원에 대한 교육을 통해 개인정보보호 인식 제고

3. 세부 교육 계획

3.1 개인정보보호책임자 및 분야별 책임자 교육

- 교육 과정 : OO 개인정보보호를 위한 워크샵 및 세미나
- 교육 대상 : 개인정보보호(총괄)책임자 및 분야별 책임자
- 교육 일정 및 추진기간 : 2009년 OO월 OO일 ~ OO월 OO일

3.2 개인정보보호 관리자 및 담당자 교육

- 교육 과정 : 연 20시간 이상의 개인정보보호 전문교육
- 교육 대상 : 개인정보보호 관리자 및 담당자
- 교육 방법 : 집합 및 사이버 교육 등, 정보보호 강좌 활용
- 교육 일정 및 추진기간 : 2009년 00월 00일 ~ 00월 00일

3.3 개인정보보호 취급부서장 및 부서별 개인정보보호 담당자 교육

- 교육 과정
 - 개인정보보호 관련 법규정
 - 회사 개인정보보호지침
 - 내/외부 개인정보보호사고 예방, 대응책 및 현안
- 교육 대상 : 회사 모든 취급부서장 및 부서별 개인정보보호 담당자
- 교육 방법 : 강사초빙 집합 교육
- 교육 일정 및 추진기간 : 2009년 4/4분기

3.4 개인정보취급자 및 개인정보취급 외주직원 교육

- 교육 내용
 - 개인정보보호 관련 법규에 따른 의무사항 및 처벌규정
 - 회사 개인정보보호지침
 - 내/외부 개인정보보호사고 현황, 개인정보사고 예방 및 발견 시 보고 방법
- 교육 대상 : 회사 내외 모든 개인정보취급자
- 교육 방법
 - 부서별 확산 교육
 - 사이버 교육 과정 개설(2009년)
- 교육 일정 및 추진기간
 - 2009년 4/4분기
 - 2010년부터 신규직원 교육 또는 정기 전문 교육 과정에 포함하여 실시

3.5 전 직원 인식제고

- 교육 내용
 - 개인정보보호 관련 법규에 따른 의무사항 및 처벌규정
 - 내/외부 개인정보보호사고 현황, 개인정보사고 예방 및 발견 시 보고 방법
- 교육 대상 : 회사 내 전 직원
- 교육 방법 : 사이버 교육 또는 현안 발생 시 회람

- 교육 일정 및 추진기간 : 정보보호 교육 시 포함하여 시행

4. 교육 실적 관리

- 개인정보보호 교육 체계 문서화
 - 교육일자, 강사, 교육 과정 명, 교육 내용 등을 기록
 - 정보보호 교육 계획(신규직원 대상 교육, 정규 보안 교육 등) 작성에 활용
 - 조직의 정보보호 수준을 향상시키기 위한 교재로 사용
 - 교육 참여 결과 기록 보관
 - 정보보호 교육 성과 등을 시스템(그룹웨어) 등으로 기록 관리
 - 개인정보 보안사고 대응과 개인정보보호 관리 활동 수행 등을 위한 참고자료로 활용
- 개인정보보호 교육 효과 분석
 - 실행 목적
 - 개인정보보호 교육효과를 측정하므로 교육 인지도 및 학습도를 측정함
 - 향후 교육수행의 지표로 활용
 - 조사 대상 : 개인정보보호 교육 이수자
 - 조사 방법 : 교육실시 이후 설문조사 실시
 - 조사 일정 : 교육실시 이후 매번
 - 효과분석 시행 범위
 - 설문지 기획 및 설문문항 개발
 - 설문 데이터 분석 및 보고서 작성
 - 효과분석 활용 방안
 - 교육에 대한 호감도, 교육내용에 대한 인지도 등을 조사하여 효율적인 개인정보보호 수행을 위한 기본 데이터로 활용

[첨부 1] 개인정보보호 교육 관리 대장

No	교육명	교육일자	교육대상	참석률 (대상인원 /참석인원)	주관 부서	담당자	비고

[첨부 2] 개인정보교육 참석자 확인서

담당자	관리자

교육자 :

교육 실행 일자 : 20 년 월 일

No	소속	직위	참석자 명	서명

[첨부 3] 개인정보교육 교육 결과 설문서

개인정보보호 교육결과 설문서

교육명:

교육자:

교육 시행 일자 : 200 년 월 일

교육에 대한 의견을 듣고 이후의 과정에 반영하고자 합니다.

이 설문지는 교육 참석 확인용으로 활용되오니 바쁘시더라도 잠시 시간을 내어 설문에 답해 주시기 바랍니다.

1	교육 내용이 유익하다고 느끼셨습니까?	매우 유익	유익	보통	불필요	전혀 불필요
2	교육 내용은 업무에 활용하실 수 있는 것입니까?	직접 활용	활용	잘모름	무관	전혀 무관
3	교육 진행은 흥미롭게 이루어졌습니까?	매우 흥미	흥미	보통	지루함	매우 지루함
4	교육 내용 중 가장 유용한 부분은 어떤 부분이었습니까?					
5	좀 더 교육이 필요하다고 생각되는 내용이나 개선이 필요한 사항이 있으면 알려주십시오.					

여러분의 의견을 반영하여 더욱 충실한 교육 과정을 만들겠습니다.

감사합니다.

[첨부 4] 개인정보교육 교육 공고문 예시

2009년도 4/4분기 개인정보보호 교육실시

• 개요

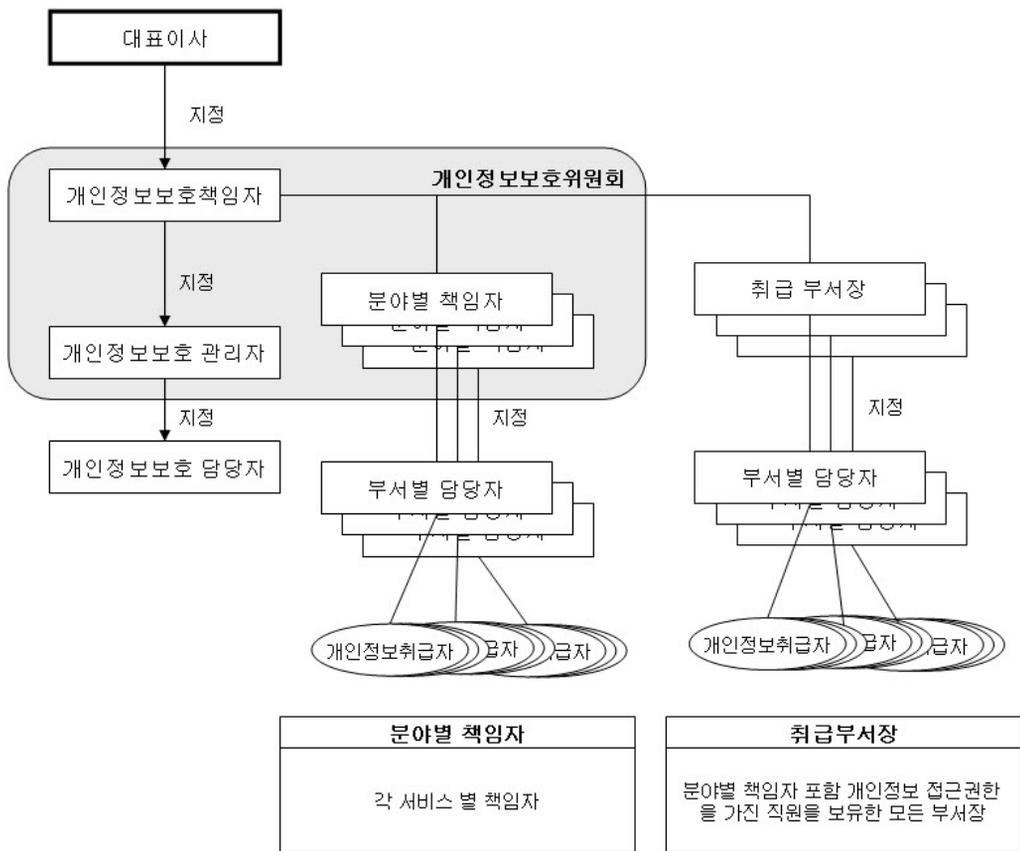
- 일시 : 2009. 00월.00일 PM 04:00~ 04:30
- 장소 : 대강당
- 대상 : 부서별 개인정보보호담당자
- 강사 : OO 시큐리티서비스 정OO 컨설팅 본부장

• 교육 내용

- 개인정보보호 법규정
- 개인정보 침해 유형 및 최근 동향

□ 절차서 · 기술서 · 계획서 - ② 개인정보보호 조직도

개인정보보호 조직도 예시



□ 절차서 · 기술서 · 계획서 - ③ 개인정보 수행담당자 직무
기술서

대외비

문서번호	
------	--

개인정보 수행담당자 직무기술서

1. 개인정보보호책임자 직무기술서

1. 직무 개요		
직무명	개인정보보호책임자	직무코드
직종		수행직급
2. 직무 수행 요건		
구 분	내 용	비 고
일 반	<ul style="list-style-type: none"> ▪ 개인정보보호 계획, 방침 및 관련 지침의 수립·시행 ▪ 정보주체의 열람 청구 등 민원 및 개인정보침해신고 접수·처리 ▪ 개인정보처리실태의 점검 및 감독 ▪ 각종 개인정보보호 관련 통계 및 자료의 취합 ▪ 개인정보보호 관련 요건 준수 여부의 점검 ▪ 개인정보보호 교육 등 기타 개인정보보호를 위하여 필요한 업무 	
경 력		
기 타		
3. 세부 직무 내용		
직무 내용	처리 절차 및 방법	수행 주기
보호대책 검토	개인정보보호대책 수립 및 검토	년 1회
관리체계 검토	개인정보보호 조직체계 검토	년 1회
보호대책 주관	관리기관 개인정보보호 대책 수립의 적정성 및 이행 여부 확인	반기 1회
위원회 운영	개인정보보호 위원회 소집 및 운영	필요 시
4. 특기 사항		

2. 분야별 개인정보보호책임자 직무기술서

1. 직무 개요			
직무명	분야별 개인정보보호책임자	직무코드	
직 종		수행직급	
2. 직무 수행 요건			
구 분	내 용		비 고
일 반	<ul style="list-style-type: none"> ▪ 개인정보 수집의 목적을 명확히 제시하고 목적에 필요한 최소한의 범위 안에서 적법하고 정당하게 수집하여야 한다. ▪ 수집된 개인정보가 필요한 범위 안에서 정확하고 완전하며 최신의 것이 되도록 보장하여야 하며, 이를 위한 확인 절차를 수립하여야 한다. ▪ 수집, 확인 및 저장을 위한 보안 요구사항을 정의하고 이를 분야별 책임자 등 관련자에게 준수를 요구하여야 한다. ▪ 수집된 개인정보를 청 내외에서 이용 및 제공하고자 할 경우 그 용도가 수집 목적에 다른 것인지를 확인하여야 한다. ▪ 수집된 개인정보를 청 내외에서 이용 및 제공하고자 할 경우 보안 요구사항을 정의하고 이를 관련 취급부서장에게 준수하도록 요구하여야 한다. ▪ 접수된 개인정보 문서를 안전하게 보관하고 적법하게 파기하여야 한다. 		
경 력			
기 타			
3. 세부 직무 내용			
직무 내용	처리 절차 및 방법		수행 주기
보호현황 검토	개인정보 생명주기별 관리현황 검토		월 1회
침해사고 예방	개인정보 침해사고 예방		월 1회
불만처리 감독	개인정보관련 불만, 의견 처리 및 감독		월 1회
각종보고업무	개인정보보호책임자에게 개인정보보호 교육, 이행점검, 모니터링, 침해행위, 불만·의견 처리 사항 보고		월 1회
각종보고업무	개인정보보호 실무자 지정 명단 변경 시 개인정보보호책임자에게 보고		필요 시
각종보고업무	기존 개인정보를 신규서비스에 이용 시 승인		필요 시
각종보고업무	개인정보 출력 및 저장 시 사전 승인		필요 시
보호대책 주관	개인정보보호 관련 시스템(솔루션) 모니터링 및 분석·처리 내용 검토		월 1회
보호대책 주관	취급자의 개인정보보호 의무 이행 여부 정기점검		반기 1회
4. 특기 사항			

3. 분야별 개인정보보호담당자 직무기술서

1. 직무 개요			
직무명	분야별 개인정보보호책임자	직무코드	
직 종		수행직급	
2. 직무 수행 요건			
구 분	내 용		비 고
일 반	<ul style="list-style-type: none"> ▪ 개인정보를 타 기관 및 업체에게 이용 또는 제공의 적법성 및 타당성을 검토하여야 한다. ▪ 개인정보를 타 기관 및 업체에게 이용 또는 제공 시 보안 요구사항 및 책임관계를 정의하고 타 기관 및 관련 분야별 책임관계에 이의 준수를 요구하여야 한다. ▪ 개인정보를 타 기관 및 업체에게 이용 또는 제공 시 보안 요구사항 만족 여부를 점검하여야 한다. ▪ 기타 타 기관 및 업체에게 이용 또는 제공 시 관련 개인정보보호에 관한 업무를 수행하여야 한다. ▪ 해당 개인정보보호담당자는 회사의 개인정보를 처리하는 응용시스템의 안전성을 확보할 책임이 있다. 이를 위하여 관련 법 규정 및 보안 요구사항에 따라 개인정보처리시스템을 안전하게 설계, 개발, 구현하여야 한다. ▪ 해당 개인정보보호담당자는 데이터베이스에 저장된 개인정보의 안전성을 확보할 책임이 있다. 이를 위하여 데이터베이스 내의 개인정보를 관리하고 중요 개인정보를 암호화하는 등 안전하게 보호하기 위한 업무를 수행하여야 한다. ▪ 해당 개인정보보호담당자는 개인정보를 처리하는 하드웨어 및 네트워크 인프라의 안전성을 확보할 책임이 있다. 이를 위하여 개인정보처리시스템의 인프라 및 네트워크를 안전하게 운영하고 접수부서장의 승인에 따라 개인정보처리시스템의 접근권한을 설정, 관리하기 위한 업무를 수행하여야 한다. 		
경 력			
기 타			
3. 세부 직무 내용			
직무 내용	처리 절차 및 방법		수행 주기
침해사고 예방	개인정보 침해사고 예방		월 1회
불만처리 감독	개인정보관련 불만, 의견 처리		월 1회
각종보고업무	기존 개인정보를 신규서비스에 이용 시 승인		필요 시
각종보고업무	개인정보 출력 및 저장 시 사전 승인		필요 시
4. 특기 사항			

4. 취급부서장 직무기술서

1. 직무 개요			
직무명	취급부서장		직무코드
직 종			수행직급
2. 직무 수행 요건			
구 분	내 용		비 고
일 반	<ul style="list-style-type: none"> ▪ 부서의 개인정보취급자를 지정하고 개인정보를 안전하게 취급하도록 교육 및 관리·감독 ▪ 개인정보취급자의 접근권한 승인 및 단말기 설정 등 제반 보호장치에 관한 사항을 확인·감독 ▪ 부서의 개인정보 이용, 제공, 열람, 정정, 삭제 등 취급 내역 및 취급자에 대한 기록 확보 및 정당성 여부의 주기적 점검을 통해 오·남용 사고를 예방 ▪ 부서의 개인정보취급자 현황, 개인정보 취급 현황 등의 통계, 개인정보 침해 및 위법 사항 등을 개인정보보호책임자에게 통보 ▪ 부서 내 개인정보침해사고 발생 시 침해사고대응팀과 협력하여 조사, 처리 및 재발 방지 방안 수립 ▪ 업무처리를 위해 개인정보를 유관기관에 제공하거나 접근권을 제공할 경우 그 관리·감독 ▪ 공개서버에 정보등록 시 개인정보나 중요자료 존재 여부의 점검 ▪ 필요시 부서의 개인정보처리에 대한 절차, 기준 및 계획 마련 등 소관 업무 분야 내 개인정보처리 및 보호에 관한 업무 ▪ 취급 업무를 외부기관에 위탁한 경우 그 수탁기관의 개인정보보호 관리에 관한 업무 		부서의 장으로서 의 역할 및 책임을 짐
경 력			
기 타			
3. 세부 직무 내용			
직무 내용	처리 절차 및 방법		수행 주기
보호계획 주관	부서내 개인정보취급자의 개인정보보호 활동을 위한 업무수행 독려, 지휘 및 감독		수시
보호계획 주관	취급 업무상 개인정보보호 대·내외 협의 담당		필요 시
보호계획 주관	개인정보 관련 외부 협력업체의 현황 유지 및 관리		수시
각종보고업무	기존 개인정보를 신규서비스에 이용시 보고		필요 시
보호계획 주관	개인정보사전영향평가 수행 검토		필요 시
보호계획 주관	개인정보 미 파기 현황 파악		
4. 특기 사항			

5. 개인정보취급자 직무기술서

1. 직무 개요			
직무명	개인정보관리실무자	직무코드	
직종		수행직급	
2. 직무 수행 요건			
구분	내용		비고
일반	<ul style="list-style-type: none"> ▪ 업무상 개인정보를 취급하는 자는 처리하는 개인정보가 훼손 및 누설되지 않도록 개인정보보호지침에 따라 안전하게 취급하여야 한다. ▪ 직무상 알게 된 개인정보를 누설 또는 권한 없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적을 위하여 사용하여서는 안된다. ▪ 개인정보취급자가 개인정보를 무단 조회하거나 오남용 하는 경우 내부 규정 및 관련 법규에 따라 징계 및 처벌될 수 있다. ▪ 개인정보 접근 권한을 임의로 양도 및 대여하여서는 안 된다. 		
경력			
기타			
3. 세부 직무 내용			
직무 내용	처리 절차 및 방법		수행 주기
보호계획 주관	개인정보보호 이행점검		월 1회
보호계획 주관	개인정보사전영향평가 수행점검		필요 시
보호계획 주관	인터넷에 게시된 개인정보보호방침 및 개인정보취급방침 수시 변경 검토		반기 1회, 필요 시
보호계획 주관	개인정보의 안전한 수집 및 이용자 동의 획득 관리(방법과 정책 비교 검토)		반기 1회, 수시
보호계획 주관	개인정보자산 현황 파악 및 등급분류		년 1회, 개인정보사전영향 평가지
보호계획 주관	개인정보보호 정책과 실제 현황 비교검토		반기 1회, 수시

■ 개인정보보호관리체계 인증준비 안내서(부 록)

보호계획 주관	개인정보 비밀유지를 위한 보안서약서 징구	필요 시
보호계획 주관	이용자가 본인의 개인정보 열람·정정·삭제 요구 시 본인 확인 및 요구에 대한 조치	필요 시
보호계획 주관	개인정보 외부업체 제공, 위탁시 해당 내역 검토	반기 1회, 필요 시
보호계획 주관	개인정보파일대장 작성 및 관리	필요 시
보호계획 주관	CCTV관리현황 및 화상정보 열람·재생 현황, 장소 출입통제현황 검토	월 1회
보호계획 주관	개인정보 접근 권한 부여 및 기록유지 검토	월 1회
보호계획 주관	데이터베이스 접근권한 기록유지 검토	월 1회
보호계획 주관	개인정보처리시스템 접속기록 확인·감독	월 1회
보호계획 주관	개인정보 항목별 출력 항목 최소화, 변환처리 및 암호화 확인검토	월 1회
각종보고업무	개인정보보호 관련 시스템(솔루션) 모니터링 및 분석·처리 및 주기적으로 책임자에 보고	월 1회
보호계획 주관	개인정보 파기 확인	필요 시
보호계획 주관	취급자의 개인정보보호 의무 이행 여부 정기점검	분기 1회
보호계획 주관	개인정보 미 파기 현황 파악	분기 1회
4. 특기 사항		

부 록 3

개인정보보호를 위한 기술적 보호조치 안내서

- 예약시스템 예시

목 차

I. 예약시스템에 대한 이해	81
1. 개요	81
2. 예약시스템의 주요 프로세스	81
3. 개인정보 생명주기별 업무 분류	85
4. 예약시스템 업무별 개인정보	86
II. 개인정보보호와 관련한 응용프로그램 보안	87
1. 개인정보수집시 응용프로그램 보안	87
2. 개인정보이용시 응용프로그램 보안.....	92
3. 개인정보보관시 응용프로그램 보안.....	94
4. 개인정보파기시 응용프로그램 보안.....	95
III. 개인정보보호와 관련한 인프라 보안.....	96
1. 웹서비스 보안	96
2. 서버 보안	100
3. 데이터베이스 보안	104
4. 네트워크 보안	106

I. 예약시스템의 서비스 개요 및 특성

1. 개 요

- 예약은 시설 및 서비스에 대한 사용에 대해 미리 약속하여 두는 계약 서비스이다.

2. 예약시스템의 주요 프로세스

가. 회원가입

□ 사용자 동의

- 개인정보 수집과 관련하여 개인정보를 수집하는 목적, 수집하는 개인정보 항목, 개인정보 보유 및 이용기간에 대해 동의를 받는다

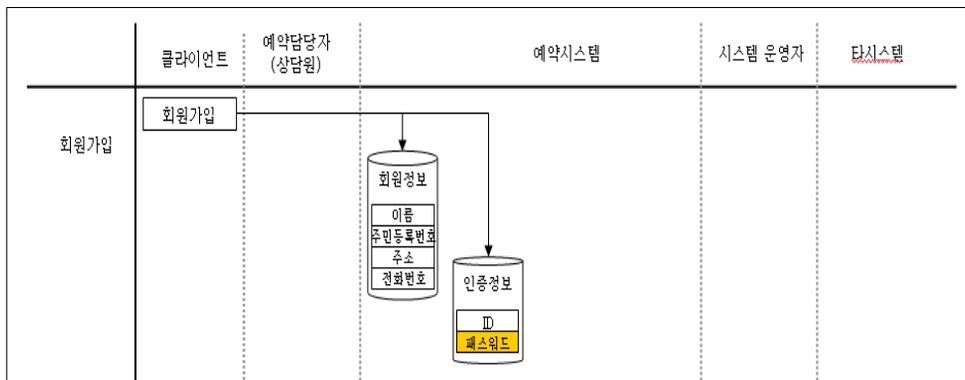
□ 회원정보 입력

- 성명, 주민등록번호, 주소, 전화번호 등의 사용자 개인정보를 입력한다
- 입력된 개인정보는 웹 서버의 회원 정보 테이블에 저장된다

□ 인증정보 입력

- 해당 웹 사이트를 이용하기 위해 사용할 사용자ID 와 패스워드를 입력한다.
- 입력된 사용자 인증정보는 웹 서버의 인증 정보 테이블에 저장된다

<그림 1> 회원 가입시 업무 흐름도



나. 인증

□ 인증수행

- 기 생성한 사용자의 ID 와 패스워드를 웹 인증창을 통해 입력하고, 해당 입력값을 인증 테이블에서 확인하여 인증 성공여부를 결정한다

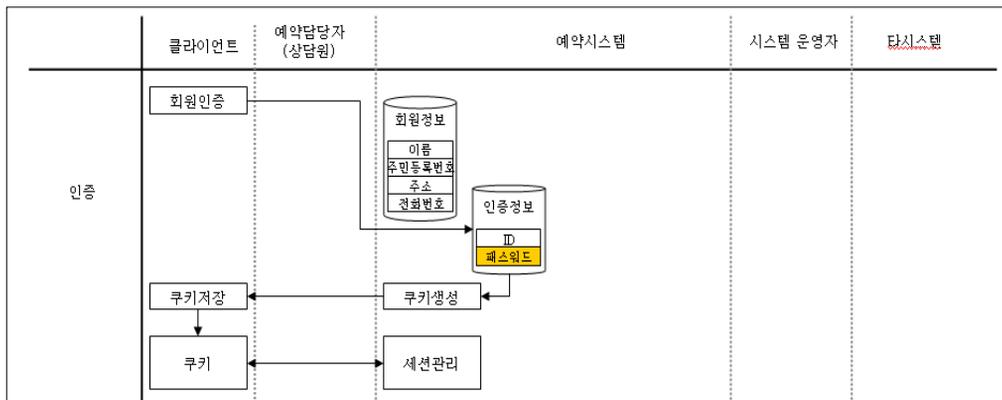
□ 쿠키정보생성

- 회원정보 또는 인증정보를 이용하여 웹 서비스의 세션 관리를 위한 쿠키를 생성하여 클라이언트의 PC 에 전송한다.

□ 쿠키를 이용한 세션 인증

- 서비스 이용자는 PC 에 저장된 쿠키 정보를 이용하여 예약시스템의 웹 사이트에 지속적인 인증을 수행하며 이용한다

<그림 2> 인증시 업무 흐름도



다. 예약 및 결제

□ 예약현황 조회

- 서비스 이용자는 인증을 수행한 뒤 생성된 쿠키를 이용하여 예약현황을 조회한다.

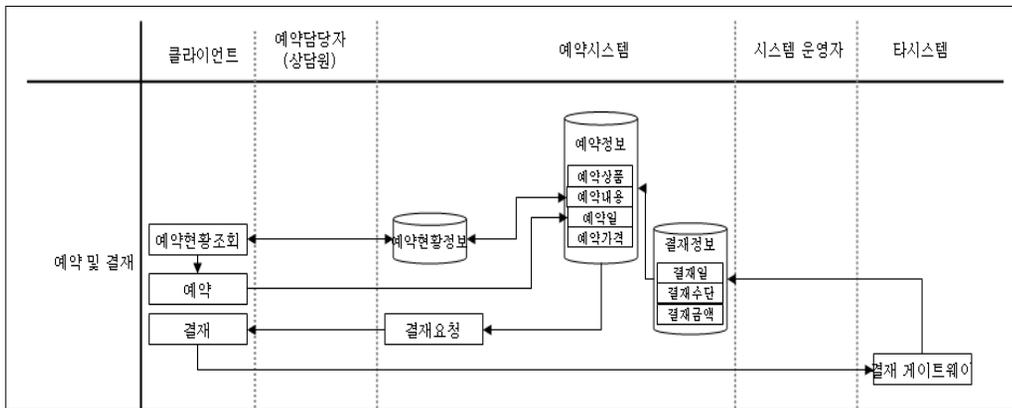
□ 예약정보 입력

- 서비스 또는 시설을 이용하기 위한 이용 내역 및 날짜 등을 입력한다

□ 결제

- 예약한 사항에 대해 결제를 수행한다
 - 카드 결제시에는 카드 번호, CVS, 카드 비밀번호, 카드 유효일 등의 정보를 입력한다.
 - 은행 이체시에는 이체 계좌번호, 이체 계좌주 명, 금액 등의 정보를 입력한다.
- 결제 결과를 예약 시스템에 저장한다.
 - 카드 결제시에는 결제 확인 및 결제 취소를 위한 결과만을 저장하며, 카드 결제를 위한 관련한 정보는 저장하지 않는다.
 - 은행 이체시에는 입금주 명과 금액 정보를 예약시스템에 저장한다.

<그림 3> 예약 및 결제시 업무 흐름도



라. 예약 변경 및 취소

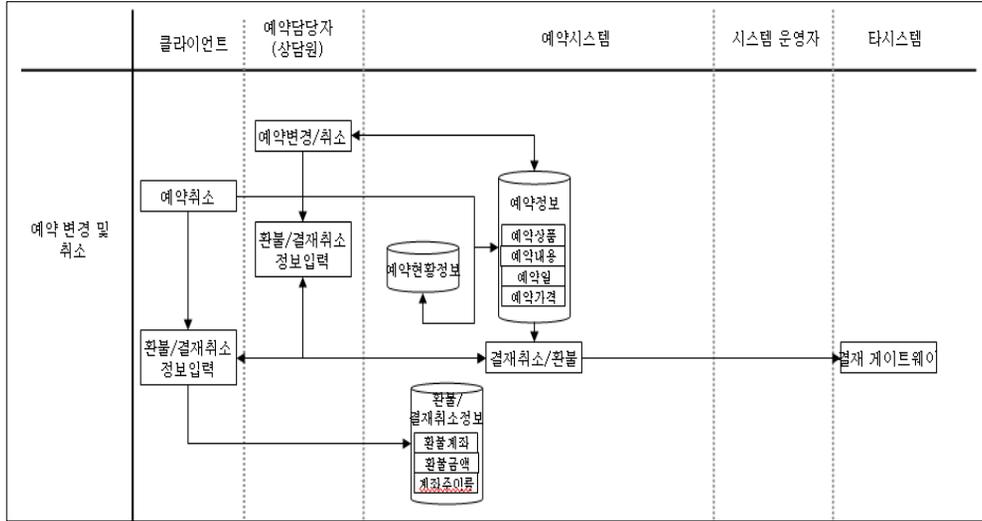
□ 예약정보 변경/취소

- 기 예약된 정보를 확인하고 예약 정보를 변경하거나 취소한다.

□ 환불 정보 입력/결제취소

- 예약의 변경 또는 취소 사항에 따라 환불/결제취소/추가결제 등의 절차를 수행한다.
 - 환불시에는 환불을 받기 위한 계좌번호, 계좌주 명 등의 정보를 입력한다.
 - 카드 결제시에는 결제 결과만을 저장하며, 카드 결제와 관련한 일련의 정보를 저장하지 않는다.

<그림 4> 예약변경 및 취소시 업무 흐름도

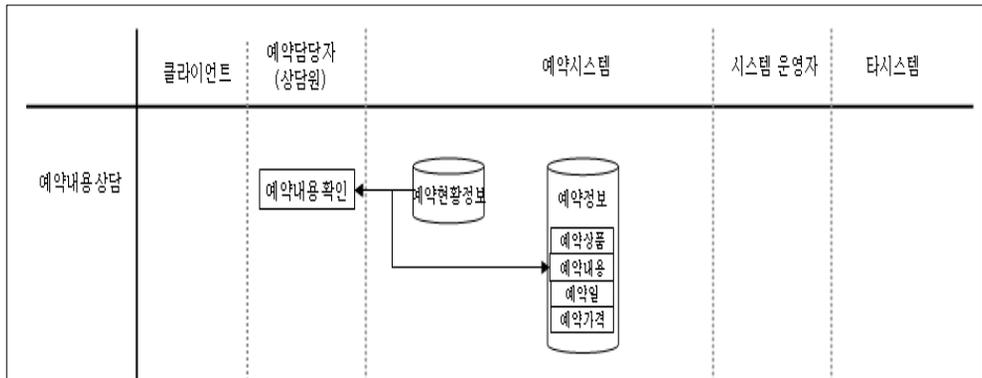


마. 예약 내용 상담

□ 예약현황 조회

- 상담원은 본인의 ID 와 패스워드로 예약 사이트에 접속한 뒤, 서비스 이용자의 예약현황을 조회하고, 일부 내용에 대해 변경할 수 있다.
- 상담원은 개별 예약사항에 대해 임의로 조회할 수 없으며, 사용자의 ID 또는 주민번호등을 이용하여 조회할 수 있다.

<그림 5> 예약내용상담시 업무 흐름도



바. 회원정보제공

회원정보 전송

- 서비스 제공 및 회원의 개인 정보를 타 사이트로 전송할 시에는 이를 암호화하여 전송한다.

사. 회원정보 보관

회원정보 보관

- 서비스 제공 및 회원의 개인정보는 임의의 접근을 통제하고 주민등록번호와 같이 개인식별도가 높은 개인정보의 경우에는 이를 암호화하여 저장한다

아. 회원탈퇴

회원정보 폐기

- 서비스 제공 및 회원이 입력한 일련의 개인정보는 그 사용목적이 소멸되거나 회원의 탈퇴 등의 요구가 있을 때 모두 삭제한다.

3. 개인정보 생명주기별 업무 분류

- 예약시스템의 각 개별업무는 개인정보 생명주기에 따라 다음과 같이 분류될 수 있다.

개인정보 생명주기별 관련 업무

개인정보 생명주기	예약 업무
수집	사용자 동의, 회원정보 입력, 인증정보 입력, 예약정보 입력, 결제, 환불 정보 입력/결제취소, 회원탈퇴 정보입력
이용	인증수행, 쿠키정보생성, 쿠키를 이용한 세션 인증, 예약현황 조회, 예약정보 변경/취소, 회원정보 전송
보관	회원정보 보관
폐기	회원정보 폐기

4. 예약시스템 업무별 개인정보

o 각 업무별 이용되는 개인정보는 다음과 같다.

개인정보 생명주기별 관련 업무

개인정보 생명주기	예약 업무	관련 개인정보
수집	사용자 동의	해당사항 없음
	회원정보 입력	(회원신상정보) 성명, 주민등록번호, 주소, 전화번호 등 연락처, 생년월일, 이메일 주소, 가족관계 및 가족구성원 정보 등 (근로정보) 직장, 고용주, 근무처 등
	인증정보 입력	(사용자 인증정보) 사용자 ID, 패스워드, 주민등록번호
	예약정보 입력	(의료·건강정보) 건강상태, 진료기록, 신체장애, 장애등급, 병력(병력) 등 (서비스 이용정보) 예약서비스 상품명, 서비스 이용일시 및 장소
	결제	(개인금융정보) 신용카드번호, CVS, 신용카드 비밀번호, 카드유효일자, 통장계좌번호, 계좌주 이름
	환불정보 입력/결제취소	(개인금융정보) 신용카드번호, CVS, 신용카드 비밀번호, 카드유효일자, 통장계좌번호, 계좌주 이름
	회원탈퇴 정보입력	회원탈퇴사유
이용	인증수행	(사용자 인증정보) 사용자 ID, 패스워드, 주민등록번호
	쿠키정보 생성	(사용자 인증정보) 사용자 ID, 패스워드, 주민등록번호
	쿠키를 이용한 세션 인증	IP 주소, 웹사이트 접속내역
	예약현황 조회	(기호·성향정보) 시설 및 서비스 이용 내역 등
	예약정보 변경/취소	(기호·성향정보) 시설 및 서비스 이용 내역 등
	회원정보 전송	(회원신상정보) 성명, 주민등록번호, 주소, 전화번호 등 연락처, 생년월일, 이메일 주소, 가족관계 및 가족구성원 정보 등 (근로정보) 직장, 고용주, 근무처 등 (기호·성향정보) 시설 및 서비스 이용 내역 등
보관	회원정보 보관	(회원신상정보) 성명, 주민등록번호, 주소, 전화번호 등 연락처, 생년월일, 이메일 주소, 가족관계 및 가족구성원 정보 등 (근로정보) 직장, 고용주, 근무처 등 (기호·성향정보) 시설 및 서비스 이용 내역 등 (사용자 인증정보) 사용자 ID, 패스워드, 주민등록번호
폐기	회원정보 폐기	예약 서비스 이용내역 증빙과 관련한 최소한의 정보를 제외한 모든 개인정보

II. 예약시스템의 응용프로그램 보안

1. 개인정보 수집 시 응용 프로그램 보안

가. 보안 대상

- 예약시스템의 경우 개인정보 수집단계에서는 회원정보, 인증정보, 예약을 위한 정보, 결제정보 등이 입력되며, 관련 개인정보는 다음과 같다.

개인정보 생명주기	관련 개인정보
수집	(회원신상정보) 성명, 주민등록번호, 주소, 전화번호 등 연락처, 생년월일, 이메일 주소, 가족관계 및 가족구성원 정보 등 (근로정보) 직장, 고용주, 근무처 등 (사용자 인증정보) 사용자 ID, 패스워드, 주민등록번호 (의료·건강정보) 건강상태, 진료기록, 신체장애, 장애등급, 병력 등 (서비스 이용정보) 예약 서비스 상품 명, 서비스 이용일시 및 장소 (개인금융정보) 신용카드번호, CVS, 신용카드 비밀번호, 카드유효일자, 통장계좌번호, 계좌주 이름 등

- 개인정보 수집에 관련한 응용 프로그램 구현시 보안사항은 예측하지 못한 형태의 입력값에 대한 통제와 암호화가 있다.

나. 관리적 통제항목

사용자 동의

- 개인정보 수집을 위해서는 먼저 서비스 이용자의 동의를 얻어야 하며 이를 위한 동의는 일정한 형식과 내용을 갖춰야 한다.
- 동의 획득 시에 이용자가 명확히 인지하고 확인할 수 있도록 약관 및 개인정보취급방침과는 별도로 눈에 띄게 표시하고 이용자의 동의를 받아야 한다
 - (인터넷 사이트) 동의를 구하는 화면 또는 동의를 구하는 절차 상에서 동의 내용을 게재하고 이용자가 동의 여부를 표시하도록 하는 방법(회원가입화면, 로그인 화면 등)
 - (전자우편) 동의 내용이 기재된 전자우편을 발송하여 이용자로부터 동의의 의사표시가 기재된 전자우편을 전송하는 방법

<동의 획득 작성 예시>

□ 개인정보 수집, 이용에 대한 동의

1. 수집목적

○○은 이용자의 동의가 있거나 법령의 규정에 의한 경우를 제외하고는 본조에서 고지한 범위를 넘어 이용자의 개인정보를 이용하지 않습니다

<서비스 제공에 관한 계약 이행 및 서비스 제공에 따른 요금정산>

콘텐츠 제공, 예약·발권, 각종 물품배송 또는 청구서 발송, 금융거래 본인 인증 및 금융 서비스, 구매 및 요금결제, 요금추심

<회원관리>

회원제 서비스 이용에 따른 본인확인, 개인식별, 불량회원의 부정 이용 방지와 비인가 사용 방지 가입 의사 확인, 가입 및 가입횟수 제한, 만 14세 미만 아동 개인 정보 수집 시 법정 대리인 동의여부 확인 분쟁 조정을 위한 기록 보존, 불만처리 등 민원처리, 고지사항 전달

<마케팅 및 광고에 활용>

신규 서비스 개발 및 특화, 인구통계학적 특성에 따른 서비스 제공 및 광고 게재, 접속 빈도 파악, 이용자의 서비스 이용에 대한 통계 이벤트 등 광고성 정보 전달

2. 수집하는 개인정보 항목

○○은 회원가입, 상담, 서비스 신청 등등을 위해 아래와 같은 개인정보를 수집하고 있습니다.

- 수집항목 : 이름, 생년월일, 로그인ID, 비밀번호, 자택 전화번호, 자택 주소, 휴대전화번호, 이메일, 주민등록번호, 쿠키, 접속 IP 정보, 진찰권번호
- 개인정보 수집방법 : 홈페이지(회원가입,진료예약,고객의소리 등)

3. 보유 및 이용기간

이용자의 동의 하에 수집된 개인정보는 이용자가 ○○ 인터넷 웹사이트상의 서비스를 이용하는 동안 보유·이용됩니다.

당사는 아래와 같이 개인정보의 수집 및 이용 목적이 달성된 때 수집된 개인정보를 지체 없이 파기하겠습니다.

- 회원 가입 정보의 경우 : 회원 탈퇴 요청이 있거나 회원 자격을 상실한 때
- 설문조사, 이벤트 등 일시적 목적을 위하여 수집한 경우 : 당해 설문조사, 이벤트 등이 종료한 때
- 사업을 폐지하는 경우

다만, 개인정보의 수집 및 이용 목적이 달성된 경우에도 상법 전자상거래 등에서의 소비자 보호에 관한 법률 등 관계법령의 규정에 의하여 보존할 필요성이 있는 경우 및 사전에 보유기간을 이용자에게 고지하거나 명시한 경우 등은 그에 따라 개인정보를 보관할 수 있습니다.

동의함 동의하지 않음

□ 개인정보 취급 위탁 동의

○○은 아래와 같이 개인정보 취급 업무를 전문업체에 위탁하여 운영하고 있습니다.

▶ 업체명 : B 인포마케팅
▶ 위탁업무내용 : 예약서비스 확인 및 불편사항 접수를 위한 고객센터 운영

동의함 동의하지 않음

□ 개인정보 제3자 제공 동의

○○은 타사와의 제휴 마케팅을 통해 다양한 서비스 제공을 위해 아래와 같이 귀하의 개인정보를 제공하고 있습니다.

▶ 이름, 이메일, 핸드폰 번호, 주소, 생년월일
- 제공대상 : A 보험사
- 제공정보의 이용 목적·보험판매 텔레마케팅
- 제공정보의 보유 및 이용 기간 : 제공일로부터 1 개월후 파기

동의함 동의하지 않음

□ 결제환불정보입력/결제취소

- 결제는 결제 게이트웨이를 이용하여 결제한다.
- 결제정보는 결제 확인 및 취소를 위한 최소한의 정보만을 저장한다.
 - 결제카드번호, 금액, 결제여부 등을 저장한다.
 - 결제카드 비밀번호, 카드 유효일, CVS 등의 정보를 저장할 수 없다.
- 30만원 이상의 결제에 대해서는 공인인증서를 이용하여 결제를 수행한다.

□ 저장 값의 범위에 대한 통제

- 개인의 금융정보와 관련하여 거래 내역 확인을 위한 정보이외에 결제정

보에 대한 저장은 수행하지 않는다.

다. 기술적 통제항목

□ 입력값 범위 설정

- 개인정보등이 입력되는 모든 입력창에 대한 특수문자의 입력에 대한 허용은 SQL Injection, XSS 등의 공격을 유발할 수 있으므로 특수문자가 입력되지 않도록 필터링을 수행한다.
 - 특수문자의 예 : !@#\$%^&*()_+ \ | ~":<>/?
 - ※ SQL Injection : 데이터베이스와 연동되는 입력란에 공격자가 원하는 SQL 문을 삽입하여 수행하는 공격이다. SQL 삽입 공격을 통해 공격자는 로그인 인증을 우회하거나 다른 테이블의 내용을 열람할 수 있다.
 - 대응 방안은 사용자의 입력을 받아 DB와 연동하는 부분은 특수 문자 등의 입력 값을 필터링한다. 해당 공격에 사용되는 특수문자는 ', -, = 등이 있다.
 - ※ XSS(Cross Site Scripting) 웹 사이트가 사용자의 입력값을 받을 때 특정 악성 스크립트가 실행되어 사용자의 쿠키값과 같은 중요 정보가 공격자에게 추출당할 수 있는 취약점이다.
 - 대응방안은 사용자의 입력값에 대한 적절한 필터링 수행한다 해당 공격에 사용되는 특수문자는 <, >, ;, ", / 등이 있다.
- 주민등록번호, 계좌번호, 카드번호 등과 같이 숫자만을 입력하게 되어 있는 창에는 숫자만을 입력할 수 있도록 필터링한다.

□ 입력값 특성 적용

- 사용자 ID 등의 정보는 기존의 사용자 ID 와 동일한 ID 를 선택할 수 없도록 한다.
- 사용자 패스워드는 영문자와 특수문자 숫자를 조합하여 8 자리 이상으로 설정하도록 한다.
 - 패스워드 입력창에 특수문자입력을 기본적으로 허용하나 일부 특수문자 (", -, ;, ')의 입력은 통제한다.

□ 파일 업로드 통제

- 파일업로드시에 exe, dll 과 같은 실행파일과 html, jsp, asp, php, js 와 같은 웹 서버 실행코드를 업로드하지 못하도록 필터링을 수행한다.

- 파일업로드 필터링이 취약할 시에는 공격자가 악성코드를 서버에 업로드하여 웹 데몬의 권한을 획득할 수 있으며, 리버스 텔넷(Reverse Telnet)과 같은 공격으로 서버에 침투할 수 있다.

- ※ 리버스 텔넷 (Reverse Telnet) : 웹 해킹을 통해 시스템의 권한을 획득한 후 해당 시스템에 텔넷과 같이 직접 명령을 입력하고 확인할 수 있는 셸을 획득하기 위한 방법이다. 공격 대상인 서버에서 공격자인 클라이언트로 텔넷 접속을 넘겨주는 방식으로 텔넷 연결을 생성한다.

- 파일업로드 필터링시에 Active X, js 등을 이용한 클라이언트 측에서의 필터링 방법은 지양하고, 서버측에서 jsp, asp 등을 이용하여 필터링을 수행하도록 한다.
 - 클라이언트 측에서의 필터링은 패킷 변조를 통해 공격자에 의해 우회될 수 있다.

□ 입력값의 암호화

- 주민등록번호와 패스워드와 같이 인증에 사용되는 정보는 암호화 값이 아닌 해시 값으로 저장한다.

- 암호화는 DES, AES 등의 알고리즘을 이용한 것으로 알고리즘과 키값을 공격자가 알고 있는 경우 복호화가 가능하다. 따라서, 암호화 알고리즘을 사용하여 인증정보를 저장하지 않는다.

- ※ DES: 1977년 1월 NIST(National Institute of Standards and Technology)에 의해 암호화 표준으로 지정됐으며, 64비트의 블록 암호화 알고리즘이다. 56비트 크기의 키로 암호화한다. DES는 암호화 방식의 차이에 따라 Electronic Codebook(ECB), Cipher Block Chaining(CBC), Cipher Feedback(CFB), and Output Feedback(OFB)으로 나뉜다.

- ※ AES : 미국의 MARS, RC6, Twofish, 벨기에의 Rijndael, 영국·이스라엘·덴마크의 합작인 Serpent가 결선에 들어가는 알고리즘으로 선정되었다.

- 해시는 SHA, MD5 등의 알고리즘을 사용하며 복호화가 불가능하다. 인증정보를 암호화하여 이에 대한 해시값을 구하여 저장할 수도 있다.

- ※ 해시의 특성

- 입력되는 평문의 길이가 달라도 결과값의 길이는 같다.
- 입력되는 평문의 내용이 조금만 바뀌어도 해시값은 완전히 다른 값이 출력된다.

- ※ MD5(Message Digest function 95): RSA와 함께 공개키 기반 구조(Public Key

■ 개인정보보호관리체계 인증준비 안내서(부 록)

Infrastructure)를 만들기 위해 개발되었다. 32비트 컴퓨터에 최적화되었다.

※ SHA(Secure Hash Algorithm): 160비트 값을 생성하는 해시 함수다. 데이터는 512비트의 크기의 블록으로 입력한다.

2. 개인정보 이용시 응용 프로그램 보안

가. 보안 대상

- 예약시스템의 경우 개인정보 이용 단계에서는 인증정보, 회원신상정보, 기호 성향정보등이 이용되거나 생성되며 관련 개인정보는 다음과 같다

개인정보 생명주기	관련 개인정보
이용	(사용자 인증정보) 사용자 ID, 패스워드, 주민등록번호 (회원신상정보) 성명, 주민등록번호, 주소, 전화번호 등 연락처, 생년월일, 이메일 주소, 가족관계 및 가족구성원 정보 등 (근로정보) 직장, 고용주, 근무처 등 IP 주소, 웹사이트 접속내역 (기호·성향정보) 시설 및 서비스 이용 내역 등

- 개인정보 이용과 관련한 응용 프로그램 구현시 보안사항은 인증정보를 이용한 세션관리와 접근제어가 있다.

나. 관리적 통제항목

□ 유희세션에 대한 관리

- 일정시간동안 서비스에 대한 접근이 없을 시에 사용하는 쿠키를 만료시키고, 세션을 종료한다.
- 세션을 종료한 뒤, 접근을 시도할 시에는 재인증을 거치도록 한다.

□ 권한 관리

- 조직 변경 및 인사이동으로 인한 권한의 변경사항은 시스템에 즉시 반영되어야 한다.
- 주기적으로 시스템에 존재하는 권한의 적절성을 검토한다.

□ 예약정보에 대한 접근관리

- 개인의 예약 정보는 전체적인 예약현황을 확인하는 정보와 개별 예약건에 대한 상세 정보를 분리하여 시스템에 저장하고, 개별 예약건에 대한 접근은 개인정보의 소유자와 관련 담당자만이 접근할 수 있도록 통제한다

□ 개인정보 접근 시에 인증의 재수행

- 사용자의 회원가입 정보와 같은 개인정보에 접근할 시에는 패스워드를 재입력하도록 한다.
- 예약정보 변경 및 취소시에는 패스워드를 재입력하도록 한다.

다. 기술적 통제항목

□ 인증정보의 전송

- 인증을 위해 서버로 전송되는 패스워드 또는 생체인식 정보는 암호화되어 전송 한다.

□ 인증

- 암호화되어 전송된 인증정보에 대한 해시값을 이용하여 인증테이블에서 해당 해시값의 일치여부를 확인하는 것으로 인증을 수행한다

□ 인증 우회에 대한 통제

- 로그인 과정을 거치면 사용자 세션이 생성되는데 각 서비스 웹 페이지 별로 세션 체크를 지속적으로 수행하지 않을 경우, 서비스 이용자 또는 공격자에 의해 임의의 페이지에 접근함으로써 개인정보 또는 기밀정보가 유출될 수 있으므로, 쿠키 등을 이용하여 각 웹 페이지별로 인증을 수행한다.

- 관리자 페이지의 경우 별도의 인증 정보를 이용하여 접근할 수 있도록 하며, IP 등을 통하여 접근제어를 수행한다.

※ 쿠키는 사용자가 인터넷 웹 사이트에 방문할 때 생기는 4KB 이하의 파일로서, 웹 사이트의 방문하면 그 접근 기록이 클라이언트에 파일로서 남게 된다. 이 파일은 사용자와 웹 사이트를 연결해 주는 정보를 담고 있다 따라서 나중에 다시 클라이언트가 그 사이트에 접속할 때 쿠키 내용을 이용해 클라이언트는

■ 개인정보보호관리체계 인증준비 안내서(부 록)

웹 서버에 접근을 시도하고, 서버는 클라이언트의 신분을 알 수 있다.

□ 쿠키 생성 요소

- 쿠키는 접속 시간 정보, 사용자 ID 및 인증정보들을 이용한 해시값으로 생성하여 사용한다.
- 쿠키에는 사용자 ID 및 패스워드, 주민등록번호 등 개인정보중 개인을 식별하기 위한 정보를 암호화 또는 해시를 적용하지 않은 상태로 사용하지 않는다.
 - ※ 암호화 또는 해시를 적용하지 않은 정보를 쿠키로서 사용할 경우 쿠키가 노출됨으로써 해당 인증정보 또는 개인정보가 노출되는 위험이 있다
- 쿠키는 재사용이 불가능하도록 시간정보를 포함 한다.

□ 쿠키의 재사용에 대한 통제

- 쿠키를 공격자가 가로채어 해당 쿠키로 동 웹사이트에 재접속시 인증을 수행하지 않도록 쿠키에는 시간 정보 또는 사용 내역에 대한 사항을 확인할 수 있는 정보를 담고 있어야 한다.

3. 개인정보 보관 시 응용 프로그램 보안

가. 보안 대상

- 개인정보 보관 단계에서는 회원신상정보, 기호 성향정보등이 보관될 수 있으며 관련 개인정보는 다음과 같다.

개인정보 생명주기	관련 개인정보
이용	(회원신상정보) 성명, 주민등록번호, 주소, 전화번호 등 연락처, 생년월일, 이메일 주소, 가족관계 및 가족구성원 정보 등 (근로정보) 직장, 고용주, 근무처 등 (기호·성향정보) 시설 및 서비스 이용 내역 등 (사용자 인증정보) 사용자 ID, 패스워드, 주민등록번호

- 개인정보 보관 관련한 응용 프로그램 구현시 보안사항은 암호화와 접근제어가 있다.

나. 관리적 통제항목

서버 상에 존재하는 개인정보에 대한 보안

- 서버에 존재하는 개인정보의 경우 데이터베이스의 일반 계정이 접근할 수 없도록 권한관리를 수행한다.

서버에서 다운로드 받은 개인정보에 대한 보안

- 서버에서 개인정보를 다운로드 받는 서비스에 대한 접근은 관련 담당자만이 가능하도록 한다.
- 파일을 다운로드 받는 경우에는 파일다운로드시 패스워드를 설정하도록 강제한다.

4. 개인정보 파기 시 응용 프로그램 보안

가. 보안 대상

- 개인정보 파기 단계에서는 법적으로 보호되는 정보 이외의 모든 개인정보가 대상이다.

개인정보 생명주기	관련 개인정보
파기	예약 서비스 이용내역 증빙 등 법적으로 보존하게 되어 있는 최소한의 정보를 제외한 모든 개인정보

- 개인정보 파기와 관련하여서는 완전한 삭제에 대한 문제가 있다.

나. 관리적 통제항목

서버상의 개인정보 삭제

- 사용자 서비스 탈퇴나 종료 후에는 개인정보를 삭제한다
 - 개인정보 삭제시 비활성화 플래그를 두어 이를 변경하는 방식을 사용하지 않고, 해당 레코드를 제거한다.
- 법적으로 해당 정보를 남기게 되어 있는 경우에는 해당 개인정보를 웹 서비스에서 열람하지 못하도록 비활성화한다.

□ 서버 미디어 폐기

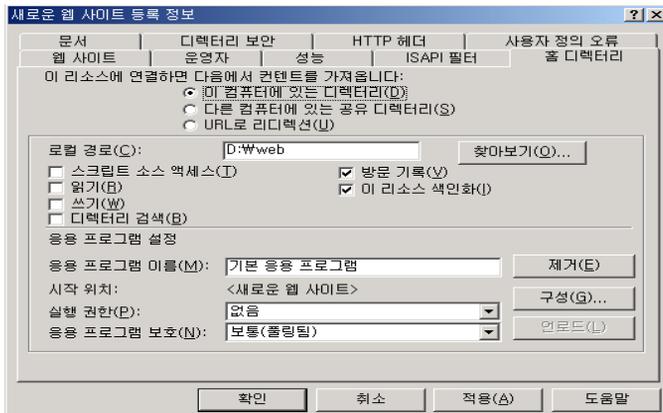
- 서버 교체 또는 서버 폐기 등의 이유로 개인정보가 저장된 하드와 테이프 등의 미디어를 폐기할 시에는 개인정보를 모두 삭제한 뒤, 폐기한다.
- 파일을 삭제하거나 하드디스크를 포맷한 경우에도 데이터 영역이 완전하게 삭제되지 않고 복구가 가능하여 저장된 개인정보가 오·남용 될 수 있으므로
 - 정보의 중요성에 따라 자기 소거 장치를 이용하여 데이터를 삭제하거나
 - 임의의 대용량의 데이터를 전체에 다시 덮어쓰는 Raw 포맷을 수행할 수 있는데, 별도의 데이터 복구 방지프로그램을 사용하는 것이 좋다
- ※ 데이터 복구 방지 프로그램 (예시)
 - 상용 프로그램 : 파이널데이터의 “파이널 이레이저”
 - 공개용 무료 프로그램
 - ObjectWipe (<http://www.objectwipe.com/products/objectwipe/>)
 - XL Delete (<http://www.xldevelopment.net/index.php>)
 - BCWipe (<http://www.jetico.com/>)

III. 예약시스템의 인프라 보안

1. 웹 서비스 보안

가. 웹 데몬 권한 관리

- 웹 해킹 발생시 공격자는 웹 데몬의 실행권한과 같은 권한을 가지게 되므로 웹 데몬의 권한을 웹 서비스 제공에 문제가 없는 수준에서 최소화한다.
- IIS 웹 서버의 권한관리 설정
 - 프로세스의 권한 설정에 관한 항목으로 낮음(IIS 프로세스), 보통(폴링됨), 높음(격리됨) 이렇게 세 가지 중의 하나의 권한을 설정하게 되어 있는데 IIS 최초 설치 시의 권한은 ‘보통’이다. 문제가 되지 않을 경우 ‘높음(격리됨)’으로 설정한다.



o 아파치 서버의 권한관리 설정

- 아파치의 서비스 계정은 기본계정으로 'apache' 로 생성되어 실행되며, apache 계정은 nobody 권한으로 생성되어야 한다.

나. 웹 서버 보안 설정

o 디렉토리 리스팅 금지

- 디렉토리 인덱스가 되지 않도록 설정한다.

o 샘플 파일 및 디렉토리를 삭제

- IIS 서버의 경우 기본 웹 디렉토리(C:\inetpub\ wwwroot) 변경하고, IISHelp, IIAdmin 등의 가상 디렉토리 및 샘플 디렉토리 제거한다.
- 아파치 서버의 경우 /var/www/manual(구 버전의 아파치의 경우 htdocs) 디렉토리와 /var/www/cgi-bin 등의 디렉토리를 삭제한다.

o 기본문서 설정

- 웹 서버 접근시 보여주는 기본페이지를 Default.asp, index.jsp 등 중에 하나로 한정한다.

o 불필요한 문서 삭제

- 불필요한 소스나 취약점이 있던 과거 버전의 소스가 해당 웹 디렉토리에 존재하지 않도록 한다.
- 웹 소스가 존재하는 디렉토리에는 zip, alz 와 같은 소스를 압축하거나 관련 문서를 압축해놓은 파일들을 저장하지 않는다.
- 웹 소스가 존재하는 디렉토리에서 편집기를 사용하여 변경함으로 해서 bak

파일등을 생성하지 않도록 한다.

o 접근제어의 설정

- 필요한 경우 IP, 네트워크, 그리고 도메인 주소에 따라 접근을 제한하거나 허용한다.

다. SSL(Security Socket Layer) 설정

- o 개인정보 누출을 막기 위해 금융서비스처럼 온라인 결제를 요하는 부문은 반드시 SSL을 적용하며, 그 이외에도 기밀정보이용 및 중요 개인정보에 대한 확인 등의 서비스 이용시에는 SSL 을 적용하도록 한다.

※ SSL은 사이버 공간에서 전달되는 정보의 안전한 거래를 보장하기 위해 넷스케이프사가 정한 인터넷 통신규약 프로토콜을 말한다. 확대 적용하고 있다. SSL 규약은 서버와 클라이언트의 진위 확인이 가능하도록 해준다 암호화키와 관련된 협상을 할 수 있을 뿐 아니라 상위 응용프로그램이 정보를 서버와 교환하기 전에 서버의 진위를 확인해 줄 수 있다.

라. 로그

- o 웹 서비스사용시에 해당 로그를 남기도록 한다.

- 윈도우 IIS 웹 서버의 경우 W3C, Microsoft IIS 로그, NCSA 로그 형식중에 하나를 선택하여 적용할 수 있다.

※ W3C 확장 로그 : c:\winnt\system32\logfiles 디렉토리에 yymmlog 파일 형식으로 로그를 생성하고 다음과 같은 항목을 선택하여 로그를 생성할 수 있다

- 시간 (time)
- 클라이언트 IP 주소 (c-ip)
- 사용자 이름 (cs-username)
- 서버 IP 주소(s-ip)
- 서버 포트(s-port)
- 메서드 (cs-method)
- URI 스템 (cs-uri-stem)
- 프로토콜 상태(sc-status)
- 사용자 에이전트(cs, user-agent)

※ Microsoft IIS 로그 : 사용자가 별도로 그 양식을 지정할 수 없다 기본 형식은 클라이언트의 IP 주소, 사용자 이름 요청 날짜 및 시간 HTTP 상태 코드, 받은 바이트 수 등의

기본 항목과 함께, 경과 시간, 전송 바이트 수, 메소드, 대상 파일 등의 세부 항목으로 구성된다.

※ NCSA 로그 : NCSA 공통 로그 파일 형식 역시 별도로 그 양식을 지정할 수 없다. 그 양식이 무척 간단하여, 클라이언트의 IP, 사용자 이름 날짜, 시간, 요청 형식, HTTP 상태 코드, 전송 바이트 수로 구성된다.

- 아파치 웹 서버의 경우 httpd.conf 파일에서 logformat 을 이용하여 생성할 로그의 형식을 설정할 수 있다. 아파치 웹 서버에서 사용할 수 있는 로그 포맷의 인자는 다음과 같다.

인 자	내 용
%a	클라이언트의 IP 주소
%A	로컬 IP 주소
%b	헤더 장보를 제외하고서 전송된 데이터의 크기, 전송된 데이터의 크기가 0 일 때 '-'로 표시
%c	응답이 완료되었을 때의 연결 상태 X : 응답이 완료되기 전에 연결이 끊김 + : 응답이 보내진 후에도 연결이 지속됨 - : 응답이 보내진 후 연결이 끊김
%[Header]e	환경변수 헤더의 내용
%f	요청된 파일이름
%h	클라이언트의 도메인 또는 IP 주소
%H	요청 프로토콜의 종류
%l	클라이언트 측에서 identd를 실행하고 있을 때 클라이언트의 로그인 명이지만, %u 와 마찬가지로 100 % 신뢰할 수 없다.
%m	요청 메소드
%p	서버가 요청을 받아들이는 포트 번호
%P	요청을 처리하는 자식 프로세스의 ID
%q	질의에 사용된 문자
%r	요청의 첫 번째 라인
%s	서버가 클라이언트에게 보내는 상태코드다. 이 정보는 (2로 시작하는 코드) 요청이 성공하였는지, (4로 시작하는 코드) 클라이언트에 오류가 있는지, (5로 시작하는 코드) 서버에 오류가 있는지 알려주므로 매우 중요하다.
%{format}t	웹 서버에 작업을 요구한 시간
%T	웹 서버가 요청을 처리하는데 소요된 시간 (초)
%u	클라이언트의 사용자(상태 코드 401 을 리턴할 경우 등록되지 않은 사용자)로서 사용되지만 100 % 신뢰할 수 있는 데이터는 아니다.
%U	요청된 URL 경로
%v	요청을 처리하는 서버의 이름

마. 패치 관리

- 패치 버전관리
 - 패치 대상 웹 서버를 목록화하고 각 웹 서버에 대해 적용한 패치와 적용일을 기록하여, 패치 적용에 대한 이력관리가 이루어질 수 있도록 한다

2. 서버 보안

가. 계정 및 패스워드 관리

- 관리자 계정은 최소한의 인원에게 부여한다
 - 윈도우 시스템의 경우 administrators 그룹에 포함되는 계정을 확인하고, 불필요한 계정의 경우 권한을 변경한다.
 - 유닉스/리눅스 시스템의 경우 root 와 같이 UID 가 0 인 계정을 확인하고, UID 인 계정이 root 이외에 존재할 경우 해당계정의 적절성을 확인하고 권한을 변경한다.
- 시스템에 존재하는 계정 목록을 주기적으로 확인하고 불필요한 계정은 삭제한다.
 - 윈도우의 경우 명령창에서 'net users' 명령으로 사용자 계정목록을 확인할 수 있으며, 관리자 그룹에 해당하는 계정목록을 확인하고자 할 경우, 'net localgroup administrators' 명령을 사용한다.
 - 리눅스/유닉스 시스템의 경우 /etc/passwd 파일에서 시스템에 존재하는 계정목록을 확인할 수 있다.
- 패스워드 관리
 - 패스워드는 영문자와 숫자, 특수문자를 조합하여 생성한다.
 - 패스워드는 주기적으로 변경되도록 한다.
 - 잘못된 패스워드를 이용한 접근시 해당 접근을 거부할 수 있도록 설정한다

나. 서비스 관리

- 시스템에서 구동중인 네트워크 서비스 목록을 확인하고 불필요한 서비스의 경우 서비스를 제거한다.
 - 네트워크 서비스 목록을 확인하기 위해서는 운영체제에 관계없이 명령창 또는 터미널에서 'netstat -an' 명령을 실행한다.

다. 파일 및 디렉토리 권한

- 웹 서비스를 구동하기 위한 소스코드에 대한 접근은 시스템관리자와 웹 서비스 관리자만이 접근이 가능하도록 한다.

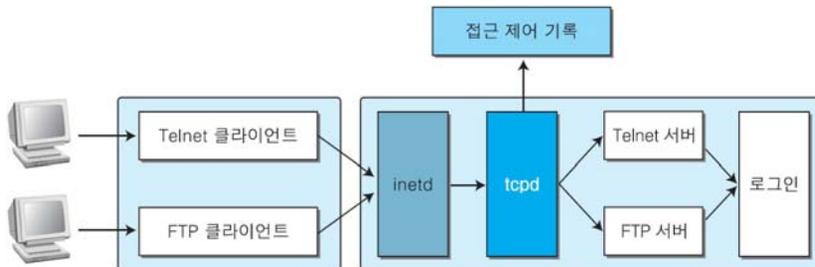
마. 접근제어

- 서버에서 사용하는 주요 관리 인터페이스에 대해서 접근제어를 수행한다

운영체제	서비스 이름	사용 포트	비고
유닉스(리눅스 포함)	Telnet	23	텔넷
	SSH	22	SFTP 가능
	XDMCP	6000	유닉스용 GUI(XManager)
	FTP	21	파일 전송 서비스
윈도우	터미널 서비스	3389	포트 변경 가능
	GUI 관리용 툴	-	VNC, Radmin 등

- 윈도우 시스템의 경우 접근제어를 위한 서버에 방화벽을 설치하여 운영하도록 한다.
 - 방화벽이 네트워크상에 별도로 존재할 경우에는 서버에 방화벽을 설치할 필요성은 낮다.
- 유닉스/리눅스의 경우 TCP Wrapper 등을 이용하여 적절한 접근제어를 수행하도록 한다.

※ TCP Wrapper 가 설치되면 수퍼 데몬인 inetd 데몬은 연결을 TCPWrapper의 데몬인 tcpd 데몬에 넘겨준다. tcpd 데몬은 접속을 요구한 클라이언트에 적절한 접근 권한이 있는지를 확인하고, 해당 데몬에 연결을 넘겨준다. 이때 연결에 대한 로깅도 실시할 수 있다.



- 리눅스인 경우 ipfilter, ipchains 같이 자체 내장된 침입차단 프로그램을 이용하여 침입차단기능을 구현할 수 있다.

바. 보안툴

- 윈도우 시스템의 경우 악성 코드에 대응하기 위해 백신을 설치하여 운영하도록 한다.
- 유닉스/리눅스의 경우 일반적으로 그 필요성은 낮으나, 침해사고 발생위험이 높은 경우 SecureOS 의 도입을 검토할 수 있다.

※ SecureOS : 컴퓨터 운영 체제의 보안상 결함으로 인하여 발생 가능한 각종 해킹으로부터 시스템을 보호하기 위하여 기존의 운영 체제(OS) 내에 보안 기능이 추가된 운영 체제. 서버의 보호, 시스템 접근 제한, 시스템 관리자에 의한 권한 남용 제한 사용자의 권한 내 정보 접근 허용, 응용 프로그램 버그를 악용한 공격으로부터 보호 등이 요구되는 운영 체제이다

사. 로그

- 로그는 회사내의 정책에 따라 일정기간에 걸쳐 남기도록 하며 해당 로그는 적절하게 백업되어야 한다.
- 윈도우에서는 이벤트 뷰어라는 로그 열람 기능을 제공하는데, 윈도우에서 운영체제 수준에서 남길 수 있는 거의 모든 로그를 이 기능을 통해 볼 수 있다.
 - 이벤트 뷰어의 로그를 구성하는 항목은 다음과 같다.

항목	설명
종류	성공감사와 실패감사가 있다. 성공감사는 어떤 시도에 대해 성공한 경우, 실패 감사는 어떤 시도에 대해 실패한 경우에 남기는 로그다.
날짜, 시간	로그가 남은 날짜와 시간
원본, 범주	로그와 관계있는 영역
이벤트	윈도우에서는 각 로그별로 고유한 번호를 부여하고 있다. 로그를 분석할 때 이러한 번호를 알고 있으면 빠르고 효과적인 로그 분석이 가능하다.
사용자	관련 로그를 발생시킨 사용자
컴퓨터	관련 로그를 발생시킨 시스템

- 이벤트 로그는 다음과 같은 정책의 선택에 따라 남기는 로그의 범위를 결정할 수 있다. 최소한 계정 로그인 이벤트 감사, 로그인 이벤트 감사를 수행하도록 한다.

로그 정책	설명
개체 액세스 감사	개체로 표현되는 파일과 시스템의 각 자원에 대한 접근 기록을 로그로 남긴다.
계정 관리 감사	사용자 계정 생성, 암호 변경 시도, 사용자 계정 잠김, 사용자 관련 정책 변경에 대한 로그를 남긴다.
계정 로그인 이벤트 감사	로그인 성공/실패 정보에 대한 로그를 남긴다.
권한 사용 감사	공격자가 계정을 생성하여 관리자 권한을 부여하거나 이에 준하는 일을 수행할 경우에 여기에 로그를 남긴다.
디렉토리 서비스 액세스 감사	액티브 디렉토리와 관련된 로그를 남긴다.
로그인 이벤트 감사	계정 로그인 이벤트 감사와 비슷한 역할을 하지만, 좀 더 상세한 정보를 로그로 남긴다.
시스템 이벤트 감사	시스템의 시동과 종료, 보안 로그 삭제 등 시스템의 주요 사항에 대한 로그를 남긴다.
정책 변경 감사	정책 변경 이벤트에 대한 사항으로서 사용자 권한 할당/제거, 감사 정책 변경에 대한 로그를 남긴다.
프로세스 추적 감사	프로그램 작동, 프로세스 종료, 핸들 복제 및 간접 개체 액세스와 같은 사항을 로그로 남긴다.

o 유닉스/리눅스에서의 로그는 다음과 같다.

로그 파일명	기능
aculog	다이얼 아웃 모뎀 관련 로그를 기록
lastlog	사용자의 로그인 아이디, 포트, 최근 로그인 시간을 기록
loginlog	실패한 로그인 시도를 기록한다.
messages	부트 메시지 등 시스템의 콘솔에서 출력된 결과를 기록하고 syslog에 의해 생성된 메시지를 기록
sulog	su 명령어 사용 내용을 기록
utmp	현재 로그인한 사용자의 아이디, 사용자 프로세스, 실행 레벨, 로그인 종류 등이 기록
utmpx	utmp 기능을 확장한(extended utmp)한 로그
wtmp	사용자의 로그인/로그아웃 시간과 IP, 세션 지속 시간을 기록, 시스템의 종료 시간/시작 시간 역시 기록
wtmpx	wtmp 기능을 확장
vo아이디.log	플로피 디스크나 CD-ROM과 같은 외부 매체의 사용에서 발생하는 에러를 기록
xferlog	FTP 접속을 기록

아. 패치

- 서버는 보안 설정을 잘 해주어도 시스템 자체에 취약점이 존재하면 시스템 운영자 수준에서는 이를 막을 수 있는 방법이 없다 대표적인 예가 시스템 자체의 취약점으로 웜이나 바이러스에 노출되는 경우다. 이럴 때는 운영체제나 데이터베이스와 같은 응용 프로그램을 만든 제작사가 만들어 배포하는 패치(Patch) 또는 서비스 팩을 적용해주어야 한다.

※ 윈도우 시스템의 경우 마이크로소프트사에서는 시스템의 보안 취약점을 확인하기 위한 MBSA(Microsoft Baseline Security Analyzer)와 같은 툴을 배포하고 있다.
(<http://www.microsoft.com/technet/security/tools/mbsahome.mspx>). MBSA에서 현재 윈도우 시스템의 취약점 및 적용되어 있지 않은 패치 목록을 확인할 수 있다

3. 데이터베이스 보안

가. 계정 및 패스워드 관리

- 관리자 계정은 최소한의 인원에게 부여한다
 - MS-SQL 의 경우 sa(system administrator) 계정과 dbadmin 톨을 부여 받은 계정을 확인하고, 불필요한 계정의 경우 권한을 변경한다.
 - 오라클의 경우 sysadmin 유닉스/리눅스 시스템의 경우 root 와 같이 UID 가 0 인 계정을 확인하고, UID 인 계정이 root 이외에 존재할 경우 해당계정의 적절성을 확인하고 권한을 변경한다
- 시스템에 존재하는 계정 목록을 주기적으로 확인하고 불필요한 계정은 삭제한다.
 - 오라클의 경우 scott 와 같이 기본으로 생성되는 계정을 패스워드를 변경하거나 사용불가능하도록 설정한다.

기본 사용자 계정	기본 패스워드
sys	Change_on_install
system	Manager
scott	tiger
dbsnmp	Dbsnmp
demo	Demo
MDSYS	MDSYS

- 오라클의 경우 새로운 모듈 설치시에 해당 계정이 생성되어 운영되므로 해당 계정들의 권한에 대해 검토한 후 권한변경을 고려한다

○ 패스워드 관리

- 패스워드는 영문자와 숫자, 특수문자를 조합하여 생성한다.
- 패스워드는 주기적으로 변경되도록 한다.
- 잘못된 패스워드를 이용한 접근시 해당 접근을 거부할 수 있도록 설정한다

나. 접근제어

- 데이터베이스에 대한 접근은 DBA 와 연동되는 웹 서버, 어플리케이션 서버만이 허용되어야 한다.
- MS-SQL 은 자체적으로 접근제어를 적용할 수 없으므로, 서버에 설치된 방화벽 또는 네트워크에서 접근제어를 수행하도록 한다.
- 오라클의 경우 \$ORACLE_HOME/network/admin/sqlnet.ora 파일에서 접근제어를 설정한다.

※ sqlnet.ora 파일에서 200.200.200.100과 200.200.200.200라는 두 IP의 접근을 허용하고 싶으면 다음과 같이 추가한다.

```
tcp.invited_nodes=(200.200.200.100, 200.200.200.200)
```

반대로, 200.200.200.150의 접근을 차단하고 싶으면 다음을 입력한다.

```
tcp.excluded_nodes=(200.200.200.150)
```

다. 테이블 권한 관리

- 테이블 구성시에는 정보의 중요도에 따라 권한을 부여할 수 있도록 설계되어야 한다.
- 개인정보를 담고 있는 테이블은 권한관리를 통하여 데이터베이스의 일반계정 등이 접근할 수 없도록 권한관리를 수행한다

라. 패치

○ 패치 버전관리

- 패치 대상 웹 서버를 목록화하고 각 웹 서버에 대해 적용한 패치와 적용일을 기록하여, 패치 적용에 대한 이력관리가 이루어질 수 있도록 한다
- 항상 최신버전의 패치가 적용되도록 한다.

마. 백업관리

- 데이터베이스에 대한 백업 정책은 수립되어야 한다

■ 개인정보보호관리체계 인증준비 안내서(부 록)

- 백업된 미디어는 소산하여 보관하여야 한다.

4. 네트워크 보안

가. 접근제어

- 외부에서 내부의 네트워크에 대한 접근을 통제하고자 할 때에는 VPN을 설치하여 운영할 수 있다.
- 정보통신망을 통해 개인정보처리시스템에 불법하게 접근하는 행위(해킹)를 방지, 차단하기 위해 방화벽을
 - ※ 방화벽: 네트워크로 들어오는 권한을 IP주소, 포트 등으로 제한하여 인가받지 않은 접근을 제한하는 기능을 제공한다.

나. 침입탐지

- 침입탐지시스템(IDS : Intrusion detection system), 침입차단시스템(IPS : Intrusion Prevention System)을 설치·운영함으로써 네트워크를 통한 외부의 침입 또는 웜/바이러스에 대해 효과적으로 대응한다.
 - ※ 침입탐지시스템 : 침입차단시스템을 통과한 접속을 재 분석하여 불법적인 자료 유출 시도 등을 탐지하여 관리자에게 알리는 기능을 제공한다.
 - ※ 침입차단시스템 : 침입탐지시스템에 패킷분석을 통해 공격에 대해 능동적인 차단을 수행할 수 있도록 한 시스템이다.

부 록 4

법률준수 통제항목

※ 개인정보보호지침 고시가 폐지될 경우에 해당항목은 일반통제항목으로 변경될 예정임

영역	도메인	통제사항	점검항목	법률근거				
				정통 방법	시행령	시행 규칙	보호 조치	보호 지침
개인정보 관리과정 요구사항	1. 개인정보 정책수립	1.1.3 내부 관리 계획의 수립	내부관리계획에 개인정보보호 조직구성 및 운영 등의 세부 사항이 명시되어 있는가? 제28조	제 15 조 1항	제9조	제 3 조 1 항		
		2.1.2 개인정보관리책임자(CPO) 지정	이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보관리책임자가 지정되었는가? 제27조	제 13 조 2항	제 7 조 2 항	제3조 1 항	제 15 조 1 항	
개인정보 보호대책 요구사항	2. 개인정보 보호조직	2.1.2 개인정보관리책임자(CPO) 지정	개인정보관리책임자의 자격 요건을 정하여 이에 적합한 자를 지정하고 있는가? 제27조	제 13 조 1항	제 7 조 1 항	제 3 조 1 항	제 15 조 2 항	

■ 개인정보보호관리체계 인증준비 안내서(부 록)

영역	도메인	통제사항	점검항목	법률근거			
				정통 방법	시행령	시행 규칙	보호 조치
			개인정보관리책임자의 개인정보보호에 관한 역할 및 책임이 정의되었는가?		제9조	제3조1항	
		2.2.1 역할 및 책임	개인정보취급자의 개인정보보호에 관한 역할과 책임 및 권한이 정의되었는가?			제3조1항	
			교육·훈련의 대상은 개인정보관리책임자(CPO), 개인정보 취급자 및 개인정보 취급부서 책임자 및 관리 담당자 등을 포함하고 있는가?			제3조2항	제25조
	4. 교육 및 훈련	4.1.1 교육 및 훈련 대상	조직이 보유한 개인정보를 공유, 제공 받거나 접근 권한을 부여받은 외부 직원에 대한 교육훈련을 제공 하는가?			제3조2항	
		4.1.2 교육 및 훈련내용	교육내용은 개인정보보호 관련 법률 및 제도, 사내 규정, 관리적 기술적 조치사항 및 이를 수행하기 위한 방법 등 개인정보취급자가 필수적으로 알아야 하는 사항을 포함하는가?			제3조2항	

영역	도메인	통제사항	점검항목	법률근거			
				정통 방법	시행령	시행 규칙	보호 조치
			개인정보보호 교육시 교육대상자의 직위 및 담당하는 업무의 특성에 따라 교육 내용을 차별화하여 적합한 교육을 실시하고 있는가?			제3 조 2항	
		교육 및 훈련 시행	교육 및 훈련이 계획에 따라 년2회 이상 시행되고, 이에 대한 기록을 유지 하는가?			제3 조 2항	
		개인정보 취급자 감독	업무상 개인정보를 취급해야 하는 사람들을 최소한으로 제한하고 있는가? 인사규정 또는 채용계약서 등에 개인정보 취급자가 직무상 취득한 개인정보를 훼손·침해 또는 누설하는 경우 관계법령상의 책임 및 처벌규정에 대해 명시하고 있는가?	제28조 2항			제10조
	5. 인적보안	5.1.2 인사규정	개인정보취급자의 퇴직 및 직무변동 시, 인사부서와 개인정보 관련부서 간에 상호 공지가 이루어지는가?	제28조 2항			제11조

■ 개인정보보호관리체계 인증준비 안내서(부 록)

영역	도메인	통제사항	점검항목	법률근거				
				정통 방법	시행령	시행 규칙	보호 조치	보호 지침
			내부직원(정규직/계약직/임시직)의 개인정보 취급 업무 시작 시 개인정보보호 관한 책임 및 의무를 고지한 개인정보 보호서약서를 징구하는가? 제3자등 외부 인원에게 개인정보처리시스템 접근권한을 부여하는 경우 개인정보보호에 관련된 사항이 계약서에 포함 되어 있으며, 개인정보를 취급하는 인원에 대해서는 개인정보보호 서약서를 받 는가?			제3 조 1 항		
		5.2.1 개인정보보호서약		제25조 제4항				제11조
			개인정보 사고보고시 법률이나 규정 등 에 의해 관련 기관에 보고해야 할 경우 보고되고 있는가?	제48조 의3 1 항				
	6. 침해사고 처리 및 대 응절차	6.3.1 침해사고 분석 및 정보공유	개인정보사고가 종결된 후 개인정보사고 의 원인을 분석하고 있는가?	제48조 4 1항				
	7. 기술적 보 호조치	7.1.3 개인 정보 취급 자 권한관리	개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 최소한의 인원에게 부여하고 있는가?	제28조 2항			제4 조 1 항	제10조

영역	도메인	통제사항	점검항목	법률근거			
				정통 방법	시행령	시행 규칙	보호 조치
			개인정보취급자의 업무 내용에 따라 접근 권한을 제한하고 있는가?			제 4 조 1 항	
			개인정보처리시스템의 접근 권한 부여 현황, 변경 또는 말소 내역 등을 기록하고 최소 5년 이상 보관하는가?			제 4 조 3 항	
		이용자 패스워드 관리 7.1.4	다음 사항을 포함하는 이용자 패스워드 관리절차가 존재하고, 이에 따라 이행되고 있는가? - 안전한 패스워드 사용기준 - 초기 패스워드 할당 후의 변경 - 패스워드의 암호화 - 패스워드의 재발급 등			제 4 조 6 항	
			정보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 개인 정보처리시스템의 접근권한을 지체없이 변경 또는 말소하는가?			제 4 조 2 항	

■ 개인정보보호관리체계 인증준비 안내서(부 록)

영역	도메인	통제사항	점검항목	법률근거				
				정통 방법	시행령	시행 규칙	보호 조치	보호 지침
			개인정보처리시스템 및 패스워드 관리지침을 제공하고 있는가? 암호정책은 법적 요건을 만족하고 있는가?			제 4 조 7 항		
			암호정책에 따라 암호화가 필요한 경우, 적절한 알고리즘과 키 길이를 결정하여 사용하고 있는가? 개인정보취급자가 이용자의 개인정보를 개인용컴퓨터(PC)에 저장할 때 암호화하여 저장하고 있는가?	제28조 제 15조 1항4	제 15 조 4항	제 6 조 1 항,2항,3 항		
		7.2.2 암호사용	취급 중인 개인정보가 권한 없는자에게 공개되지 않도록 개인정보취급자의 PC 및 개인정보처리시스템의 네트워크 설정에 대한 정책이 수립되어 있는가? - 인터넷 연결시 네트워크 구성 정책 - 이메일, 인터넷 사이트의 접속, 메신저, P2P 등을 통한 파일 전송 제한 - 공유 설정 제한	제28조 제 15조 1항4	제 15 조 4항	제 6 조 4 항		
		7.3.5 인터넷 접속 관리	개인정보처리시스템은 침입차단시스템에 의해 보호되는가?	제28조	제 15 조	제 4 조 5 항	제 4 조 8 항	제17조

영역	도메인	통제사항	점검항목	법률근거				
				정통 방법	시행령	시행 규칙	보호 조치	보호 지침
			침입차단시스템을 우회한 인터넷 접속을 금지하고 있는가?				제 4 조 5 항	
			침입을 확인하기 위해 침입차단시스템의 로그가 수집되고, 정기적으로 점검되는가?				제 4 조 5 항	
			개인정보처리시스템 접속 시 외부망에서의 직접접속은 차단되고, 가상사설망(VPN) 등을 통해 접근하도록 통제되는가?				제 4 조 4 항	
			침입기록의 자동기록, 비인가자 접속 시 자동차단, 자동경보기능 및 분석정보제공 기능을 보유하고 있는 침입탐지시스템을 설치 운영하고 있는가?			제 15 조 2항2호		
			네트워크를 통해서 시스템을 운영하는 경우 시스템 관리는 특정터미널을 통해서만 수행할 수 있도록 제한되는가?				제 4 조 5 항	
	7.3.6	원격운영관리	원칙적으로 인터넷 등 외부망을 통해 내부 시스템을 관리하는 것을 금지하고 있으며, 부득이 하게 이를 허용할 경우 강력한 사용자 인증, 암호 및 접근통제 기능을 설정하는가?				제 4 조 4 항, 제4 조5항	

■ 개인정보보호관리체계 인증준비 안내서(부 록)

영역	도메인	통제사항	점검항목	법률근거			
				정통 방법	시행령	시행 규칙	보호 조치
			허기되지 않거나 불분명한 소스, 네트워크 등으로 부터의 다운로드를 금지하고, 부특이 하게 다운로드 받을 경우 다운로드 받은 소프트웨어는 바이러스 검사를 하는가? 전자우편의 첨부파일에 대해 전자우편서버 등에서 바이러스 검사를 수행하는가? 주기적으로 바이러스 스캐닝이 이루어지고 있는가?	제28조 1항	제15조 5항	제7조	제17조
			바이러스 프로그램은 최신버전으로 업데이트 되는가?	제28조 1항	제15조 5항	제7조	제17조
			바이러스 감염이 발견되었을 경우에 바이러스 확산 및 피해 최소화를 위한 절차가 있는가? 원격작업을 통해 내부 시스템 접근 시 접근통제, 암호화 대책이 수립되어 있는가? (ID/Password외 추가인증, VPN 은 타 점검항목 참조)				제17조
						제4조4 항	

영역	도메인	통제사항	점검항목	법률근거				
				정통 방법	시행령	시행 규칙	보호 조치	보호 지침
				공개 서버는 내부망과 분리하여 설치되며, 침입차단 시스템 등에 의해 보호되는 네트워크 보호 대책이 수립되고 운영되고 있는가?			제 4 조 5 항	
				공개 서버 내에 보호되어야 할 주요 개인정보를 정의하며, 주요 개인정보 전송 시 비밀성과 무결성을 보장하는 보안서버 구축 등의 조치를 적용하고 있는가?	제 28 조	제 15 조 4 항	제 28 조 제 6 조 3 1 항 4 조 항	
				개인정보처리시스템에서 개인정보의 인쇄물 출력시 용도에 따른 출력 항목을 최소화하는가?			제 8 조 1 항	
		7.5.1 출력, 복사 시 용 도 특정		개인정보처리시스템에서 화면에 개인정보를 출력할 때 기능을 메뉴화하여 업무 내용 및 취급자의 권한에 따라 필요한 최소한의 정보만을 표시하는가?			제 8 조 1 항	
		7.5.2 출력, 복사 시 기 록 및 승인		개인정보취급자가 테이프, 디스크, 출력물, 이동식 저장 장치 등에 복사할 경우 필요한 사항을 기록하는가?			제 8 조 2 항	

■ 개인정보보호관리체계 인증준비 안내서(부 록)

영역	도메인	통제사항	점검항목	법률근거				
				정통 방법	시행령	시행 규칙	보호 조치	보호 지침
			개인정보를 출력하거나 이동 가능한 저장매체에 복사할 경우 사전에 개인정보 관리책임자의 승인을 받는가?				제8 조 4 항	
			출력물, 복사물에는 조직의 명칭 및 기록된 출력, 복사물의 일련번호를 표시하는가?				제8 조 2 항 제8 조 3 항	
			출력물, 복사물로부터 다시 출력 또는 복사하는 경우에도 조직의 명칭 및 새로운 일련번호를 표시하며 이에대한 로그가 기록되는가?				제8 조 2 항	
			개인정보의 출력, 복사에 대한 승인 시 승인받고자 하는 개인정보취급자에게 불법 유출 시 법적 책임을 지게 됨을 주지 시키는가?				제8 조 4 항	
		7.6.1 개인정보 마스킹	개인정보의 조회, 출력 시 개인정보를 마스킹하여 표시제한을 수행하는가?				제9조	

영역	도메인	통제사항	점검항목	법률근거			
				정통 방법	시행령	시행 규칙	보호 조치
8. 물리적 보 호조치	8.1.1 물리적 보호구역	개인정보 취급 공간과 개인정보처리, 저장시설 및 장비를 보호하기 위한 보호구역 역을 정의하였는가? 개인정보 장비의 폐기 시에는 저장 매체를 물리적으로 파괴하거나, 저장된 정보가 완전히 삭제되어 복구가 불가능한지 확인하고 있는가? 개인정보 취급자 등의 의무자 외 위탁업체 및 제3자의 개인정보처리시스템에 대한 접속 일시 및 내역 등 접속기록을 최소 6개월 이상 저장하는가? 개인정보 처리 기록 검토 및 위변조 방지	28조 1항	제 9 조 1항	제 9 조 1항	제 19 조 2항	
			제 9 조 1항	제 5 조 1항 제 5 조 2항	제 5 조 1항	제 26 조	
9. 내부검토 및 감사	9.3.3 개인정보 처리 기록 검토 및 위변조 방지	개인정보처리시스템 접속 기록을 월1회 이상 정기적으로 확인 및 감독 하는가? 개인정보처리시스템의 접속기록이 위·변조되지 않도록 별도 저장장치에 백업 보관하는가?			제 5 조 3항		
			제 9 조 1항				
	9.4.1 보안감사 계획 및 이행	개인정보보호 감사에 대한 정책 및 공적인 계획이 수립되어 있고 계획에는 다음과 같은 사항을 포함하는가? - 대상, 범위, 주기, 방법, 절차, 감사자, 감사도구		제 9 조 1항		제 26 조	

■ 개인정보보호관리체계 인증준비 안내서(부 록)

영역	도메인	통제사항	점검항목	법률근거			
				정통 방법	시행령	시행 규칙	보호 조치
생명주기준거 요구사항	1. 개인정보 수집에 따른 조치		개인정보보호감사는 정기적으로 수행되는가? 감시결과에 따른 지적사항이 이행 되도록 사후관리가 이루어 지는가? 서비스 제공을 위해 필요한 최소한의 정보를 수집하고 있으며, 이 외의 개인 정보를 제공하지 않는다는 이유로 해당 서비스의 제공을 거부하지 않고 있는가? 서비스 제공을 위해 필요한 최소한의 정보 이외의 정보 수집할 경우, 정보주체가 선택 제공할 수 있도록 하고 있는가?			제9조1 항	제26조 제 26조 2항 제 8 조 2 항 제 8 조 4 항
		1.1.1	중요 정보 수집 제한	개인정보 수집 시 아이디 등 주민등록번호를 대체하는 수단을 제공 하는가?	제23조 2항	제 9 조 의 2 1 항	제 8 조 3 항
		1.1.2	중요 정보 수집 제한	중요한 개인정보를 수집하는 경우, 법적 근거가 있거나, 본인의 동의를 받는가?	제23조 1항		제 8 조 1 항
		1.2.1	정보주체의 동의	수집하는 개인정보에 대하여 이용자에게 알리고 동의를 받는가?	제22조		제6조

영역	도메인	통제사항	점검항목	법률근거				
				정통 방법	시행령	시행 규칙	보호 조치	보호 지침
			개인정보 수집 시 이용자가 쉽고 명확하게 이해할 수 있는 방법으로 이용자의 동의를 받고 있는가?	제 2 조, 제 12 조 제 26조 1항 의2			제5조	
			동의를 얻어야 할 내용을 이용자가 명확히 인지하고 확인할 수 있도록 표시하는가?	제22조			제5조	
			만14세 미만 아동의 개인정보를 수집하는 경우 법정 대리인에게 필요한 사항에 대하여 고지하는가?	제31조 1항			제22조1항 제 23 조 2항	
	1.2.2	법정대리인 동의 획득 및 고지	만14세 미만 아동의 개인정보를 수집하는 경우 법정 대리인의 동의를 받고 있는가?	제31조 1항			제22조1항 제 23 조 3항	
			만14세 미만 아동의 동의를 얻을 경우 아동이 쉽게 이해할 수 있는 평이한 표현으로 고지 하는가?				제22조2항	

■ 개인정보보호관리체계 인증준비 안내서(부 록)

영역	도메인	통제사항	점검항목	법률근거				
				정통 방법	시행령	시행 규칙	보호 조치	보호 지침
			개인정보취급방침이 법적 요구사항 및 운영에 필요한 사항을 포함하여 정의되었는가?	제27조의2 2항				
		1.3.1 개인정보취급방침	개인정보취급방침을 이용자가 언제든지 쉽게 확인할 수 있도록 적절한 방법으로 공개하였는가?	제27조 2 1항	제14조 1항 제14조 3항	제8조 1항		
			개인정보취급방침을 변경하는 경우에는 그 이유 및 변경 내용을 지정된 방법에 따라 지체 없이 공지하고, 이용자가 언제든지 변경된 사항을 쉽게 알아 볼 수 있도록 조치하는가?	제27조 3항	제14조 2항	제8조 2항		제7조
	2. 개인정보 이용 및 제 공에 따른 조치	2.1.1 목적 내 개인정보 이용	이용자 및 이용자의 법정대리인으로부터 수집한 개인정보를 동의한 범위를 벗어 나 이용하지 않는가?	제24조			제9조 1항 제9조 2항 제22조 4항	

영역	도메인	통제사항	점검항목	법률근거			
				정통 방법	시행령	시행 규칙	보호 조치
			개인정보 수집 시 고지하거나 이용약관에 명시한 목적범위를 벗어난 개인정보의 이용 또는 제3자 제공이 발생할 경우, 정보주체로부터 추가적인 동의를 받는 절차와 방법이 마련되어 있는가?	제24조 의2 1 항			제9조3 항
	2.2.1	이용자의 불만 처리	이용자로부터의 개인정보에 관한 의견과 불만을 접수하고 처리하는 상담창구를 운영하고 있는가?				제27조
			이용자 및 이용자의 법정 대리인으로서 이용자 자신의 개인정보에 대한 열람 또는 이용 및 제공내역을 요구할 수 있는 방법 또는 절차를 제공하는가?	제30조 2항			제21조1 항 제21조2 항
	2.2.2	열람정정요구권 보장 및 처리	이용자 자신의 개인정보 열람, 개인정보의 이용 및 제공 내역, 또는 정정에 대한 요구가 있는 경우 지체없이 필요한 조치를 취하는가?	제30조 4항 제31조 3항			제21조1 항,2항
			이용자 및 이용자의 법정 대리인이 이용자 자신의 개인정보에 오류가 있는 경우 정정을 요구할 수 있는 방법 및 절차를 제공하는가?	제30조 2항 제31조 2항			제21조3 항 제24조1 항

■ 개인정보보호관리체계 인증준비 안내서(부 록)

영역	도메인	통제사항	점검항목	법률근거			
				정통 방법	시행령	시행 규칙	보호 조치
			이용자의 열람, 이용, 정정 및 제공내역 요청을 받은 경우 본인여부를 확인하는 절차가 있는가?				제21조1항, 2항
			이용자 및 이용자의 법정대리인은 이용자 개인정보를 대한 오류 정정을 요구할 경우 오류를 정정할 때까지 해당 이용자의 개인정보를 이용 및 제공을 중단하고 있는가?	제30조 5항 제31조 3항			제21조4항 제24조2항
			외부위탁 또는 제3자에게 제공한 개인정보가 있을 경우 이에 대해서도 정정 및 동의철회에 대한 조치를 취하고 결과를 확인하는가?	제30조 4항			
			이용자 및 법정대리인이 언제든지 개인정보 사용에 대한 동의를 철회할 수 있는 방법 및 절차가 있는가?	제30조 1항 제31조 2항			제20조2항 제24조2항
		2.2.3 동의철회	이용자 및 이용자의 법정대리인이 이용자의 개인정보 수집·이용·제공 등의 동의철회를 요청할 경우 지체없이 수집된 개인정보를 파기하는 등 필요한 조치를 취하는가?	제30조 3항 제31조 3항			제20조1항, 3항 제24조2항

영역	도메인	통제사항	점검항목	법률근거					
				정통 방법	시행령	시행 규칙	보호 조치	보호 지침	
			이용자가 동의의 철회, 개인정보의 열람·제공 또는 오류의 정정을 요구하는 방법은 개인정보의 수집 방법보다 쉬운가? 이용자가 개인정보 수집·이용·제공 등의 동의철회 또는 개인정보의 열람·제공, 오류의 정정 등을 요구할 경우 지연 또는 거절 시 타당한 사유에 근거하고 있는가?	제30조 6항				제21조6 항	
		2.2.4 이용자 요청의 처리							제25조 1,2항
		2.3.1 이용자 고지 및 동의	제3자에게 이용자의 개인정보를 처리 업무를 위탁하는 경우 관련 사항을 이용자에게 알리는가? 개인정보 취급위탁에 대한 동의 획득시, 개인정보 수집시와 동일한 방법으로 동의를 받는가? 개인정보 취급 위탁 시 수탁업체 변동 또는 위탁업무 범위 및 계약상의 변동사항이 발생할 경우 이용자로부터 별도의 동의절차를 거치고 있는가?	제25조 1항					제12조1 항

■ 개인정보보호관리체계 인증준비 안내서(부 록)

영역	도메인	통제사항	점검항목	법률근거			
				정통 방법	시행령	시행 규칙	보호 조치
			위탁사는 개인정보 취급 목적을 미리 정하고, 위탁사가 취급목적을 벗어나서 이용자의 개인정보를 취급하지 않도록 관리하는가?	제25조 3항			제12조3 항
		2.3.2 위탁자 책임	수탁사가 개인정보취급 시 법규정을 위반하였을 경우 처리 및 배상에 관한 절차가 있는가?	제25조 5항			제12조6 항
			수탁업체로부터 개인정보보호와 관리상황을 주기적으로 보고 받고, 정기 또는 수시점검을 통해 관리감독하고 있는가?	제25조 4항			제12제3 항
		2.3.3 외부위탁관리 감 독	외부위탁 계약시 개인정보보호와 관련한 법적 요건 및 조직의 개인정보보호정책을 만족하기 위한 요구사항을 계약서에 명시하였는가?				제12조2 항

영역	도메인	통제사항	점검항목	법률근거				
				정통 방법	시행령	시행 규칙	보호 조치	보호 지침
			이용자의 개인정보를 제3자에게 제공하는 경우 다음 각 호의 사항에 대하여 이 용자에게 알리고 동의를 얻는가? 1. 개인정보를 제공하는 자 2. 개인정보를 제공하는 자의 개인정보 이용 목적 3. 제공하는 개인정보의 항목 4. 개인정보를 제공하는 자의 개인정보 보유 및 이용 기간	제24조 2 1항				
	2.4.1 제3자 제공시 동의		개인정보의 제3자 제공과 관련하여 사전에 이용자에게 고지한 사항 중 변경이 발생한 경우 이용자에게 알리고 동의를 얻는가?	제24조 2 1항				
	2.4.2 제공받은 개인 정보의 관리		개인정보를 제공받은 경우 제공받은 목적 외의 용도로 이용하지 않는가? 제공받은 개인정보를 또 다른 제3자에게 제공할 경우, 법률에 근거한 사항이거나 이용자의 동의를 받고 있는가?	제24조 2 2항			제12조5 항	
				제24조 2 2항			제12조5 항	

■ 개인정보보호관리체계 인증준비 안내서(부 록)

영역	도메인	통제사항	점검항목	법률근거			
				정통방법	시행령	시행규칙	보호조치
			<p>법규정 혹은 이용자의 동의에 따라 개인 정보를 제공할 경우 사안 별 적법성을 확인하고 승인 및 기록을 남기는 등의 절차가 있는가?</p> <p>제3자에 개인정보를 제공 시, 제공 후에도 보안요구사항이 준수될 수 있도록 이와 관련된 항목을 계약서 상에 명시하고 있는가?</p>				제 9 조 1,2항
			<p>영업의 양도, 합병 등으로 개인정보를 이전할 경우 필요한 사항을 이용자에게 미리 통지하는가?</p>	제26조 1항			제13조1 항
	2.5.1	개인정보를 이전하는 경우 보호조치	<p>영업의 양도, 합병 등으로 개인정보를 이전하려는 경우 전자우편, 서면, 팩스, 전화 또는 이와 유사한 방법으로 통지하는가?</p>	제26조 1항	제 11 조 1 항 , 2 항,3항		제14조1 항
	2.5.2	개인정보를 이전받는 경우 보호조치	<p>양도자가 이전한 사실을 통지하지 않고 영업의 양도, 합병등으로 개인정보를 이전했다면, 지체없이 그 사실을 이용자에게 통지하였는가?</p>	제26조 2항			제13조2 항

영역	도메인	통제사항	점검항목	법률근거				
				정통 방법	시행령	시행 규칙	보호 조치	보호 지침
			영업의 양도, 합병 등으로 개인정보를 이전받은 경우 양도자가 이용자의 개인정보를 이용하거나 제공할 수 있는 당초의 목적 범위 안에서만 개인정보를 이용하거나 제공하는가? 영업의 양도, 합병 등으로 개인정보를 이전받아 양도자가 이용자의 개인정보를 이용하거나 제공할 수 있는 당초의 목적 범위 외로 개인정보를 이용하거나 제공하고 하는 경우, 별도로 이용자의 동의를 얻는가?	제26조 3항				
			개인정보의 해외 이전시 국내법 및 해당 국가의 법을 만족하는 공식적인 계약을 체결하였는가?	제63조 1항	제67조 2항			
	2.6.1	해외 이전 시 보호조치	개인정보의 해외 이전 시 이전 목적을 사전에 이용자에게 고지하고 동의를 얻었는가?	제63조 2,3항				제32조
			해외 이전된 개인정보에 대하여 기술적, 관리적 보호조치를 취하고 있는가?	제63조 4항	제67조 1항			

■ 개인정보보호관리체계 인증준비 안내서(부 록)

영역	도메인	통제사항	점검항목	법률근거			
				정통 방법	시행령	시행 규칙	보호 조치
3. 개인정보 관리 및 파 기에 따 른 조 치	3.1.1	개인정보의 저장 및 관리	수집된 개인정보는 정확하고 최신의 상 태로 유지되는가?				제16조
			개인정보의 수집 및 이용목적이 달성된 경우 지체없이 개인정보를 파기하는가?	제29조			제19조1 항
	3.1.3	파기시점	사업을 폐지하는 경우 지체없이 개인정 보를 파기하는가?	제29조			
			개인정보를 파기하여야 하는 경우, 위탁 또는 제3자에게 제공한 개인정보도 함께 지체없이 파기하는가?	제29조			
3.1.4	파기방법	저장 매체에 저장된 개인정보 파기 시 복구할 수 없는 방법으로 파기하였는가?				제19조2 항	
		개인정보가 기재된 종이문서의 경우 쇄 질, 소각 등을 통해 파기하였는가?				제19조2 항	

부 록 5

개인정보취급방침 작성 예시

목 차

개인정보취급방침 작성 시 유의사항	135
I. 개인정보취급방침 개요	136
II. 개인정보취급방침	138
가. 수집하는 개인정보의 항목	138
나. 개인정보 수집방법	140
다. 개인정보의 수집 및 이용목적	141
라. 개인정보 제공 및 공유	143
마. 수집한 개인정보의 취급위탁	145
바. 개인정보의 보유 및 이용기간	147
사. 개인정보 파기절차 및 방법	149
아. 이용자 및 법정대리인의 권리와 그 행사방법	151
자. 개인정보 자동 수집 장치의 설치·운영 및 그 거부에 관한 사항	154
차. 개인정보관리책임자 등	156

개인정보취급방침 작성시 유의사항

개정 『정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 “정보통신망법”)』에서는 회원가입 등의 방법으로 개인정보를 수집하고자 할 경우 개인정보 수집 및 이용목적, 보유 및 이용기간, 위탁 업무의 내용 및 수탁자 등 개인정보 취급 관련 내용을 개인정보취급방침에 포함하여 공개하도록 하고 있습니다(제27조의 2).

동 안내서에서는 이러한 개인정보취급방침을 작성·공개하는 방법에 대한 안내서를 제시하고자 합니다. 그러나 동 안내서의 내용은 개인정보취급방침의 작성 기준으로써, 정보통신망법에서 규정하고 있는 기본적인 사항만을 규정하고 있습니다.

따라서 이를 참조하여 귀사의 개인정보취급방침을 작성·게시하고자 하는 경우에는 귀사가 제공하는 서비스 내용 및 특성을 고려하여 방침의 내용을 수정·보완하여야 합니다.

개인정보취급방침은 개인정보의 수집·이용·보호 방법에 대한 공개적인 약속을 의미합니다. 잘 수립되고 이행되는 개인정보취급방침은 개인정보 수집·이용에 대한 이용자의 궁금증과 불안을 해소하여 귀사 웹사이트에 대한 신뢰를 향상시킬 수 있을 것입니다.

개인정보취급방침을 게시한 경우에는 그 내용을 준수하여야 하며 이를 위반할 경우에는 행정적 제재가 따르거나 손해배상 소송 및 형사고발에 처해질 수 있음을 유의하시기 바랍니다.

◆ 개인정보취급방침 내용 중 개인정보 수집항목, 개인정보 수집 및 이용목적, 개인정보 보유 및 이용기간(정보통신망법 제22조), 개인정보 제3자 제공(정보통신망법 제24조2), 개인정보취급 위탁(정보통신망법 제25조)의 경우,

- 개인정보취급방침에 공개할 뿐 아니라, 개인정보 수집 시 별도의 동의 또한 득하여야 합니다.

I. 개인정보취급방침의 개요

정보통신망법 제27조의 2(개인정보취급방침의 공개)에서는 정보통신서비스 제공자등이 이용자의 개인정보를 취급하는 경우 **개인정보취급방침**을 정하고 이를 이용자가 언제든지 쉽게 확인할 수 있도록 공개하도록 하고 있습니다

☞ 동 취급방침에는 **다음 각 호의 사항이 모두 포함되어** 있어야 합니다.

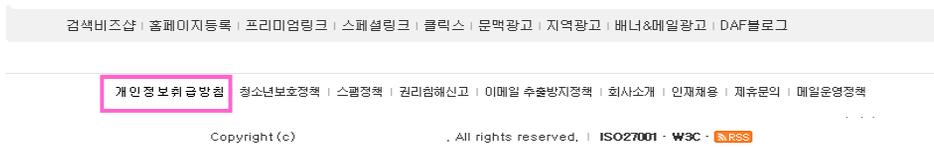
- 개인정보의 수집 및 이용목적 수집하는 개인정보의 항목 및 수집방법
- 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법인의 경우 법인의 명칭), 제공받는 자의 이용목적 및 제공하는 개인정보 항목
- 개인정보의 보유 및 이용기간 개인정보의 파기절차 및 방법제29조 단서의 규정에 따라 개인정보를 보존하려는 경우에는 그 보존근거 및 보존하는 개인정보 항목을 포함)
- 개인정보취급위탁을 하는 업무의 내용 및 수탁자(해당되는 경우에 한)
- 이용자 및 법정대리인의 권리와 그 행사방법
- 인터넷 접속정보파일 등 개인정보 자동 수집 장치의 설치·운영 및 그 거부에 관한 사항
- 개인정보관리책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처

그리고 개인정보취급방침을 변경할 경우에는 전자우편을 통해 변경된 내용을 개별적으로 이용자에게 고지하거나, 팝업창 등을 통해 홈페이지에 접속한 **이용자가 쉽게 변경된 내용을 알 수 있도록 적절한 조치**를 취하여야 합니다.

☞ 또한 개인정보취급방침에 변경일자를 기재하여 정보주체가 쉽게 변경 여부를 확인할 수 있도록 하는 것이 좋습니다.

개인정보취급방침은 정보주체의 권리 및 사업자의 개인정보 취급에 대한 전반적인 방침에 대한 내용을 담고 있는 만큼, 정보주체가 알기 쉽고 접근하기 쉽게 공개되어야 합니다.

개인정보취급방침은 **이용자가 언제든지 용이하게 확인할 수 있는 홈페이지 첫 화면 하단¹⁾**에 게시되도록 하시고, 화면이 바뀌더라도 홈페이지 화면 제일 하단에 항상 보일 수 있도록 하는 것이 좋습니다.



[그림 1] 홈페이지 첫화면 하단 게시 예

회원가입 화면 등 개인정보를 수집하는 다른 웹페이지에서도 하이퍼링크, 팝업창 등을 통하여 손쉽게 볼 수 있는 조치를 취하여야 합니다.

- 1) 1. 인터넷 홈페이지의 경우 홈페이지 첫화면 또는 첫화면과의 연결화면을 통해 내용을 이용자가 볼 수 있도록 하고 이용자가 개인정보취급방침을 쉽게 찾을 수 있도록 글자 크기, 색상 등을 활용
2. 일반 매장의 경우 점포·사무소 내의 보기 쉬운 장소에 게시 또는 비치하여 열람토록 하는 방법
3. 이용자에게 월 단위 이내마다 정기적으로 배포하는 간행물, 소식지, 홍보지, 청구서 등에 지속적으로 게재 하는 방법 등

II. 개인정보취급방침의 내용

가. 수집하는 개인정보 항목

《예시》

○○는 회원가입, 상담, 서비스 신청 등을 위해 아래와 같은 개인정보를 수집하고 있습니다.

▶ 이름, 이메일, 주민등록번호, 주소, 연락처, 핸드폰 번호, 월소득, 직업

또한 서비스 이용과정이나 사업 처리 과정에서 아래와 같은 정보들이 생성되어 수집될 수 있습니다.

▶ 서비스 이용기록, 접속 로그, 쿠키, 접속 IP 정보, 결제기록, 이용정지 기록

《해설》

☞ 개인정보란 생존하는 개인에 관한 정보로서 성명 · 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호, 문자, 음성, 음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에는 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말합니다.

- 따라서 회원가입, 물건 구매 및 배송, 상담 및 견적 등의 서비스 이용을 위해, 이름, 이메일, 연락처 등 **하나 이상의 개인정보를 제공할 것을 요청할 경우 이는 개인정보 수집에 해당합니다.**

☞ 홈페이지에 게시하는 개인정보취급방침은 귀사 전체의 개인정보취급에 대한 방침을 의미하는 것으로,

- 단순히 ▶웹사이트 상으로 수집하는 개인정보 뿐 아니라 ▶오프라인 신청서 등을 통한 수집, ▶인터넷상에 공개되어 있는 정보의 수집, ▶제휴사로부터의 제공, ▶로그 기록 수집 등

- 자사가 수집 혹은 이용자가 직접 입력하는 모든 개인정보 수집항목 및 방법에 대해 상세히 기재하셔야 합니다.

☞ 또한 서비스 이용과정이나 사업자에 의한 처리과정에서 생성되는 생성정보도 모두 빠짐없이 기재하셔야 합니다.

※ 생성정보의 예 : 서비스 이용기록, 접속 로그, 쿠키, 접속 IP 정보, 결제기록, 이용정지 기록, 사업자가 마케팅 등에 이용할 목적으로 가공한 회원정보 등(다만, 접속로그, 쿠키 등은 식별정보와 연계하여 개인의 프라이버시를 침해할 소지가 있는 경우라야 합니다)

※ 사용자 동의 획득(개정방법 제22조)

◆ 개인정보 수집항목은 개인정보 수집 시 이용자의 동의를 획득하여야 하는 항목 중 하나입니다.

- 그러나 생성정보의 경우 자동적으로 수집 또는 생성되어 이용자에게 매번 고지하고 동의를 받는 것이 경제적·기술적 사유로 통상의 동의를 받는 것이 현저히 곤란한 경우(정보통신망법 제22조제2항제1호)로 해석되어 동의없이 취급방침에 공개하시기만 하면 됩니다.

- 단, 생성정보라 하더라도, '정보통신서비스 제공에 관한 계약의 이행을 위해 필요'한 경우가 아님에도 불구하고 마케팅 등을 목적으로 수집하려는 경우 또는 동의 획득시 미리 예상할 수 있는 정보의 수집·생성에 관한 사항인 경우 사전에 고지하고 동의를 득하여야 합니다.

◆ 또한 정보통신망법 제22조제2항제3호에서 규정하고 있는 또 다른 동의 예외 사항 즉, '이 법 또는 다른 법률에 특별한 규정이 있는 경우에는 다음과 같은 예들이 있습니다.

- 정보통신서비스제공자가 만14세 미만 아동의 개인정보 수집 등을 위해 법정 대리인의 동의를 얻어야 하는 경우(정보통신망법 제31조제1항)
- 신용정보 제공·이용자로부터 채권추심업무를 위탁받은 신용정보업자가 채권 추심업무 수행을 위해 특정인의 소재를 탐지하는 행위(신용정보의 이용 및 보호에 관한 법률 제26조제5호 단서)
- 미성년자와의 거래에 있어 법정 대리인의 동의여부 확인을 위한 경우전자 상거래 등에서의 소비자 보호에 관한 법률 제21조제1항제6호) 등

나. 개인정보 수집 방법

《예시》

○○는 다음과 같은 방법으로 개인정보를 수집합니다.

- ▶ 홈페이지, 서면양식, 전화·팩스를 통한 회원가입, 상담 게시판, 경품 행사 응모, 배송 요청
- ▶ 제휴사로부터의 제공
- ▶ 생성정보 수집 툴을 통한 수집

《해설》

☞ 일반적으로 회사가 이용자의 개인정보를 수집하는 방법은 ▶홈페이지 회원가입, 상담 게시판 등을 통한 온라인상에서의 개인정보 수집 ▶전화, 팩스, 점포 내에서의 신청서 등을 통한 오프라인 상에서의 수집, ▶제휴사로부터의 제공, ▶인터넷상에서의 공개된 정보의 수집 ▶로그 분석 프로그램 등을 통한 생성정보 수집 등 매우 다양합니다.

☞ 동 항목에서는 귀사가 개인정보를 수집하는 모든 방법을 명확히 그리고 빠짐없이 게시하셔야 합니다.

다. 개인정보의 수집 및 이용목적

《예시》

○○는 수집한 개인정보를 다음의 목적을 위해 활용합니다.

- ▶ **서비스 제공에 관한 계약 이행 및 서비스 제공에 따른 요금정산**
 - 콘텐츠 제공, 물품배송 또는 청구서 등 발송, 금융거래 본인 인증 및 금융 서비스, 구매 및 요금 결제, 요금추심
- ▶ **회원 관리**
 - 회원제 서비스 이용에 따른 본인확인, 개인식별, 불량회원의 부정 이용 방지와 비인가 사용 방지, 가입 의사 확인, 가입 및 가입횟수 제한, 만14세 미만 아동 개인정보 수집 시 법정 대리인 동의여부 확인 추후 법정 대리인 본인확인 분쟁 조정을 위한 기록보존, 불만처리 등 민원처리, 고지사항 전달
- ▶ **마케팅 및 광고에 활용**
 - 신규 서비스(제품) 개발 및 특화, 인구통계학적 특성에 따른 서비스 제공 및 광고 게재, 접속 빈도 파악, 회원의 서비스 이용에 대한 통계, 이벤트 등 광고성 정보 전달
- ▶ **기타**
 - 0000, 0000, 0000...

《해설》

☞ 개인정보를 수집하여 이용하는 사업자는 정보통신서비스 제공을 위하여 필요한 최소한의 정보를 수집하여야 하며, 필요한 최소한의 정보 외의 개인정보를 제공하지 아니한다는 이유로 그 서비스 제공을 거부하여서는 안 됩니다.(정통방법 제23조 제2항)

☞ 따라서 사업자는 개인정보를 수집하는 목적을 명확히 규정하여 동 목적에 필요한 정보만을 최소한으로 수집할 의무가 있으며, 개인정보취급방침을 통하여 해당 수집 및 이용목적은 구체적이고 명확하게 고지하여야 합니다.

※ 단순히 “서비스 제공을 위한 개인정보 수집” 또는 “회원 가입을 통한 다양한 콘텐츠 이용” 등의 추상적인 목적으로는 충분하지 않습니다.

■ 개인정보보호관리체계 인증준비 안내서(부 록)

- ◆ 고지한 수집 및 이용목적과 다르게 개인정보를 이용할 경우 **5년 이하의 징역 또는 5천만원 이하의 벌금**에 처해질 수 있으니, 수집 및 이용목적은 최대한 **상세히 그리고 정확하게 기재**하셔야 합니다.
- ◆ 작성 예시에서 분류된 카테고리 및 용어는 사업자들의 실제 관행의 조사를 통하여 많이 사용되고 있는 예들을 분류하여 샘플화한 것입니다.
 - 따라서 개인정보를 수집하여 이용하는 사업자의 경우 **귀사 사업 특성에 맞게 카테고리의 추가 · 삭제 및 변경을 통하여 개인정보취급방침을 작성**하셔야 합니다.

※ **이용자 동의획득(개정방법 제22조)**

- ◆ 개인정보 수집 및 이용목적은 개인정보를 이용하기 위해 수집하는 때에 **이용자에게 알리고 동의를 얻어야 하는 사항**입니다
- ◆ 내용이 변경될 경우에도 이에 대한 동의를 득해야 합니다

라. 개인정보 제3자 제공

《예시》

[제3자 제공 안할 경우]

OO는 이용자의 개인정보를 원칙적으로 외부에 제공하지 않습니다 다만, 아래의 경우에는 예외로 합니다.

- 이용자들이 사전에 동의한 경우
- 법령의 규정에 의거하거나 수사 목적으로 법령에 정해진 절차와 방법에 따라 수사기관의 요구가 있는 경우

[제3자 제공할 경우]

oo사는 회원에 대하여 보다 더 질 높은 서비스 제공 등을 위해 아래와 같이 귀하의 개인정보를 제공하고 있습니다.

- ▶ 제공정보의 이용 목적 : 제휴 마케팅
 - 제공 대상 : 제휴 업체(oo 레스토랑, oo 스파게티)
 - 제공 정보 : 이름, 이메일, 핸드폰 번호, 주소, 생년월일
 - 제공 정보의 보유 및 이용 기간 : oo사 회원 탈퇴 시까지
- ▶ 제공정보의 이용 목적 : 보험판매 및 카드발급 등의 TM
 - 제공 대상 : oo 보험, oo 카드
 - 제공 정보 : 이름, 주민등록번호, 전화번호, 주소, 이메일
 - 제공 정보의 보유 및 이용 기간 : 제휴계약 종결 시까지

다만, 아래의 경우에는 예외로 합니다.

- 이용자들이 사전에 동의한 경우
- 법령의 규정에 의거하거나 수사 목적으로 법령에 정해진 절차와 방법에 따라 수사기관의 요구가 있는 경우

《해설》

☞ 개인정보를 제3자에게 제공하거나 공유(열람 포함)하는 경우, 개인정보취급방침에 ▶제공받는 자의 성명(법인의 경우에는 법인의 명칭), ▶제공받는 자의 이용 목적 ▶제공하는 개인정보 항목 및 ▶제공정보의 보유 및 이용기간을 상세히 기재하여야 합니다.

■ 개인정보보호관리체계 인증준비 안내서(부 록)

☞ ‘제3자’란 당해 서비스를 제공하는 정보통신서비스제공자·수탁자·영업양수자 등과 그 서비스를 이용하고 있는 정보주체 이외의 모든 자연인과 법인을 의미합니다.

- 따라서 모자(母子)회사, 그룹 계열사 사이, 프랜차이즈 조직의 본부와 가맹점 사이에서 개인정보를 제공한 경우도 모두 제3자 제공에 해당합니다.

☞ 또한 ‘제공’에는 ‘열람할 수 있도록 허용하는 것’과 ‘공유’ 모두가 포함됩니다.

<개인정보 제3자 제공의 예>

- 모자(母子)회사, 그룹 계열사 사이, 프랜차이즈 조직의 본부와 가맹점 사이에서 개인정보를 제공한 경우
- 제휴사에 특정한 개인정보를 제공한 경우
- 고객의 개인정보를 정당한 관리자가 아닌 제3자에게 열람할 수 있도록 허용하고 있는 경우
- 고객의 개인정보를 제3자와 공유하고 있는 경우 등

※ 따라서 패밀리사이트(하나의 아이디로 패밀리사이트를 구성하고 있는 개별 웹사이트들을 이용할 수 있는 웹사이트 연합체를 운영할 경우, 회원 가입 시 이용자에게 해당 사실을 명확히 알리고 이용자가 개별 또는 일괄 가입 여부를 선택할 수 있는 절차를 제공해야 합니다.

◆ 이름이나 여타 개인정보와 별도로 전화번호나 이메일 주소만을 외부에 제공하는 행위도 개인정보 제3자 제공에 해당한다는 해석이 있습니다.

◆ 정통방법 제24조(개인정보의 이용제한), 제24조의2(개인정보의 제공 동의 등) 또는 제26조제3항(영업의 양수등에 따른 개인정보의 이전의 규정을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알고 영리 또는 부정한 목적으로 개인정보를 제공받은 자는

- 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해질 수 있으니 개인정보 제3자 제공 및 공유에 대한 정확한 의미를 이해하시어 명확히 고지 및 동의받으시고 동 범위 내에서만 활용하시기 바랍니다.

마. 수집한 개인정보 취급위탁

《예시》

[업무위탁 안 할 경우]

oo는 고객님의 동의없이 고객님의 개인정보 취급을 외부 업체에 위탁하지 않습니다. 향후 그러한 필요가 생길 경우, 위탁 대상자와 위탁 업무 내용에 대해 고객님에게 통지하고 필요한 경우 사전 동의를 받도록 하겠습니다.

[업무위탁 할 경우]

oo는 서비스 이행을 위해 아래와 같이 개인정보 취급 업무를 외부 전문업체에 위탁하여 운영하고 있습니다.

▶ oo 서비스

- 위탁업무 내용 : 이동통신사 신규고객 및 번호이동 가입 고객 유치

▶ oo 컨설팅

- 위탁업무 내용 : 상담업무 효율성 제고를 위한 고객센터 운영

《해설》

☞ ‘위탁’이란 계약의 형태와 종류를 불문하고 인터넷 사업자가 타인에게 개인정보 취급의 전부 또는 일부를 대행하게 하는 것을 내용으로 하는 계약 일체를 포함합니다.

☞ “개인정보 취급 위탁”이란 서비스 제공자가 이용자의 개인정보에 대한 수집, 보관, 처리, 이용, 제공, 관리, 파기 등을 할 수 있도록 해당 서비스 제공자 이외의 제3자에게 업무를 위탁하는 것을 의미합니다.

- 개인정보 취급 위탁의 예로는 대리점 콜센터, AS센터, 요금의 회수·결제를 대행하는 자(채권추심업자 등), 배송업체 등에 개인정보의 수집, 보관, 처리, 이용, 제공, 관리, 파기의 전 과정 혹은 일부를 할 수 있도록 업무를 위탁하는 것을 들 수 있습니다.

■ 개인정보보호관리체계 인증준비 안내서(부 록)

☞ 정보통신서비스 제공에 관한 **계약의 이행을 위해 필요하여 업무를 위탁하는 경우**(예, 물품배송, 요금추심, 청구서 발송, 구매업무, 검색서비스 운영대행, 고객센터 운영, AS 처리, 시스템 유지 및 관리 등) 개인정보취급 방침에 위탁 대상자와 위탁 내용을 **공개**하시면 됩니다.

◆ 계약 이행을 위한 것이 아닌 **다른 여타 목적을 위한 업무 위탁의 경우**, 이용자에게 미리 서면 전자우편, 전화 또는 홈페이지를 통하여 수탁자(위탁을 받는 자)와 **위탁 업무에 대해 고지하고 동의를 얻어야**합니다.

- 계약 이행 이외의 목적을 위한 업무 위탁의 예 : 텔레마케팅(보험상품 등 연관 혹은 비연관 상품 및 서비스 안내, 가입고객 유치 등), 광고, 이벤트 등

바. 개인정보의 보유·이용기간

《예시》

원칙적으로, 개인정보 수집 및 이용목적이 달성된 후에는 해당 정보를 지체없이 파기합니다. 단, 다음의 정보에 대해서는 아래의 이유로 명시한 기간 동안 보존합니다.

<내부 방침에 의한 정보보유 사유>

▶ 회원 ID

- 보존 이유 : 서비스 이용의 혼선방지
- 보존 기간 : oo

<관련법령에 의한 정보보유 사유>

그리고 ~법, ~에 관한 법률 등 관계법령의 규정에 의하여 보존할 필요가 있는 경우 회사는 관계법령에서 정한 일정한 기간 동안 회원정보를 보관합니다. 이 경우 회사는 보관하는 정보를 그 보관의 목적으로만 이용하며 보존기간은 아래와 같습니다.

▶ ~에 관한 기록

- 보존 이유 : ~에 관한 법
- 보존 기간 : oo

▶ ~에 관한 기록

- 보존 이유 : ~에 관한 법
- 보존 기간 : oo

《해설》

☞ 이용자는 자신의 개인정보가 언제까지 이용·보유되는지를 알 수 있어야 하므로, 사업자는 이용자의 개인정보에 대한 보유 및 이용기간을 구체적으로 고지하여야 합니다.

그리고 정보주체가 개인정보 수집의 동의를 철회하거나 개인정보의 수집 목적을 달성한 때에는 당해 개인정보를 지체 없이 파기하여야 합니다. 단, 타 법률에서 의무화하고 있을 경우는 예외로 합니다.

■ 개인정보보호관리체계 인증준비 안내서(부 록)

☞ 개인정보를 파기해야하는 경우(정보통신망법 제29조(개인정보의 파기))는 회원탈퇴(개인정보의 이용 및 제공에 대한 동의철회), 정보 주체의 개인정보 삭제 또는 파기 요청 시, 수집목적의 달성, 수집 시 동의받은 보유 및 이용 기간 종료, 사업폐지 등이 있습니다.

☞ 수집 목적을 달성한 때의 구체적인 예

- 회원가입정보 : 회원탈퇴하거나 회원에서 제명된 때
- 대금 지급정보 : 대금의 완제일 또는 채권소멸시효기간이 만료된 때
- 배송정보 : 물품 또는 서비스가 인도되거나 제공된 때
- 설문조사, 이벤트 등 일시적 목적을 위하여 수집한 경우 : 당해 설문 조사, 이벤트 등이 종료한 때
- 본인 확인 정보 : 본인임을 확인 한 때

※ 이용자 동의획득(개정방법 제22조)

◆ 개인정보 보유 및 이용기간은 개인정보 수집 시 이용자의 동의를 획득하여야 하는 항목 중 하나입니다.

- 따라서, 이용자의 동의를 받아 수집한 개인정보의 경우에는 이용자에게 알리고 동의받은 '개인정보의 보유 및 이용기간이 종료한 경우에 파기하여야 합니다.

◆ 이용자 동의없이 개인정보를 수집한 경우(정보통신망법 제22조 제2항 각호의 예외사유에 해당하는 경우)에는 개인정보취급방침에 공개한 '개인정보의 보유 및 이용기간이 종료한 경우 파기하여야 합니다.

사. 개인정보의 파기절차

《예시》

oo는 원칙적으로 개인정보 수집 및 이용목적이 달성된 후에는 해당 정보를 지체없이 파기합니다. 파기절차 및 방법은 다음과 같습니다.

▶ 파기절차

- 회원님이 회원가입 등을 위해 입력하신 정보는 목적이 달성된 후 내부 방침 및 기타 관련 법령에 의한 정보보호 사유에 따라(보유 및 이용기간 참조) 일정 기간 저장된 후 파기되어집니다.

동 개인정보는 법률에 의한 경우가 아니고서는 보유되어지는 이외의 다른 목적으로 이용되지 않습니다.

▶ 파기방법

- 종이에 출력된 개인정보는 분쇄기로 분쇄하거나 소각을 통하여 파기하고
- 전자적 파일형태로 저장된 개인정보는 기록을 재생할 수 없는 기술적 방법을 사용하여 삭제합니다.

☞ 정통방법에서는 개인정보의 수집 및 이용목적이 달성된 후 등 개인정보를 파기하여야 할 경우 지체없이 파기하도록 하고 있습니다.

- ‘지체없이’란 ‘즉시’ 파기를 의미하진 않으며, 합리적 이유 및 근거에 따라 가장 빠른 시기를 의미합니다.

☞ 따라서 ‘파기절차’에서는 사업자 내부에서 개인정보 수집 및 이용목적이 달성된 후 정보가 즉시 파기되지 않을 경우, ‘지체없이 파기’에 대한 구체적인 절차를 명기하셔야 합니다.

- 즉, 어떤 내부 절차 및 방법으로 해당 개인정보가 특정 시점까지 관리 저장되는지에 대한 구체적인 절차 및 근거를 기재하셔야 합니다.

◆ 동 예시는 개인정보를 즉시 파기하지 않고 내부 절차에 따라 일정기간 보관 후 파기되어지는(지체없이 파기되어지는) 경우에 대한 가정으로, 사업자는 각 사업장 내의 실제 절차 및 방법을 기재하시면 됩니다.

■ 개인정보보호관리체계 인증준비 안내서(부 록)

- 한 예로, DB에서 바로바로 삭제되시는 경우 동 사항을 명기하시면 됩니다.

☞ 인터넷 사업자는 수집·보관하던 개인정보를 파기할 때에는 다음과 같은 방법으로 하여야 합니다.

- 종이에 출력된 개인정보 : 분쇄기로 분쇄하거나 소각
- 전자적 파일형태로 저장된 개인정보 : 기록을 재사용할 수 없는 기술적 방법을 사용하여 삭제

◆ 이 때 전자적 파일 형태의 경우, 파기된 개인정보의 복원을 방지하기 위해 '로우포맷' 명령으로 포맷하거나, 일반 포맷을 한 뒤 불필요한 정보를 여러번 덮어쓰우는 방법으로 재생할 수 없도록 하는 조치를 취할 수 있습니다.

☞ 파기대상 정보는 정보주체가 제공한 개인정보 뿐 아니라 인터넷 사업자가 정보주체로부터 제공받은 정보를 기반으로 서비스 제공 과정에서 생성한 개인정보 및 백업파일에 수록된 개인정보도 포함됩니다.

아. 이용자 및 법정대리인의 권리와 그 행사방법

《예시》

이용자 및 법정 대리인은 언제든지 등록되어 있는 자신 혹은 당해 만4세 미만 아동의 개인정보를 조회하거나 수정할 수 있으며 가입해지를 요청할 수도 있습니다.

이용자 혹은 만 14세 미만 아동의 개인정보 조회·수정을 위해서는 ‘개인정보변경’(또는 ‘회원정보수정’ 등)을, 가입해지(동의철회)를 위해서는 “회원탈퇴”를 클릭하여 본인 확인 절차를 거치신 후 직접 열람, 정정 또는 탈퇴가 가능합니다.

혹은 개인정보관리책임자에게 서면, 전화 또는 이메일로 연락하시면 지체없이 조치하겠습니다.

귀하가 개인정보의 오류에 대한 정정을 요청하신 경우에는 정정을 완료하기 전까지 당해 개인정보를 이용 또는 제공하지 않습니다. 또한 잘못된 개인정보를 제3자에게 이미 제공한 경우에는 정정 처리결과를 제3자에게 지체없이 통지하여 정정이 이루어지도록 하겠습니다.

oo는 이용자 혹은 법정 대리인의 요청에 의해 해지또는 삭제된 개인정보는 “oo가 수집하는 개인정보의 보유 및 이용기간”에 명시된 바에 따라 처리하고 그 외의 용도로 열람 또는 이용할 수 없도록 처리하고 있습니다.

《해설》

☞ 사이트 이용자가 자신이 등록한 개인정보를 열람하고 수정사항이 발생한 경우 이를 수정하며, 자신의 개인정보의 이용에 대해 이미 동의한 사항을 철회할 수 있는 권리와 그 방법 등에 대해 의무적으로 고지해야 하는 사항을 입력하는 부분입니다.

개인정보의 열람·정정·삭제 등을 위해서는 개인정보를 수집하는 방법보다 용이하게 할 수 있도록 웹사이트 내에 관련 메뉴를 제공하거나 개인정보관리책임자나 고객센터 등에 전자우편, 전화, 모사전송 등으로 요구를 할

수 있는 절차를 마련하고 개인정보취급방침에 게재하여야 합니다.

☞ 다음의 이유로 개인정보의 전부 또는 일부에 대하여 열람 또는 정정을 거절하는 경우가 있는 때에는 그 이유 및 근거를 명시하여야 합니다.

- 본인 또는 제3자의 생명, 신체, 재산 또는 권익을 현저하게 해할 우려가 있는 경우
- 당해 서비스 제공자의 업무에 현저한 지장을 미칠 우려가 있는 경우
- 법령에 위반하는 경우 등

▶ 개인정보의 열람 및 정정

웹사이트는 개인정보의 열람 및 정정을 요구하는 사이트 이용자의 정당한 권한여부를 확인할 수 있는 절차를 마련하여야 합니다.

열람요구를 받는 경우에 지체 없이 필요한 조치를 취하고 그 결과를 사이트 이용자에게 통지하여야 하고, 정정요구를 받은 경우에는 당해 개인정보를 정정할 때 까지 이용하거나 제 3자에게 제공하여서는 안 됩니다.

만약 정정요구를 받은 개인정보를 제3자에게 이미 제공한 경우에는 그 제3자에게 지체 없이 당해 개인정보의 정정을 요구하거나 또는 사이트 이용자 스스로 정정요청을 할 수 있도록 개인정보를 제공받은 제3자를 사이트 이용자에게 알려주어야 합니다.

다만, 사이트 이용자가 제3자에 대한 정정 요청을 거부함을 사이트에 명시적으로 표시한 때에는 그러지 아니합니다.

※ 개인정보의 열람 및 정정은 수집 및 이용목적 범위 내의 개인정보의 처리를 위한 경우나 다른 법령 등에 특별한 규정이 있는 경우가 아니면 원칙적으로 인터넷 이용자 본인에 대한 사항만을 허용하도록 합니다

▶ 개인정보의 동의 철회의 권리와 방법

또한 동의철회를 요구하는 자의 정당한 권한 여부를 확인할 수 있는 절차를 마련하여야 하며, 개인정보보호방침 등을 통해 사이트 이용자가 동의를 철회할 수 있는 방법을 쉽게 알 수 있도록 하여야 합니다.

- ☞ 정보통신서비스제공자등이 만 14세 미만의 아동으로부터 개인정보 수집·이용·제공 등의 동의를 얻고자 하는 경우에는 그 법정 대리인의 동의를 얻어야 합니다.

- ☞ 법정 대리인은 당해 아동의 개인정보에 대하여 위의 이용자와 동일한 권리를 가집니다.

자. 개인정보 자동 수집 장치의 설치·운영 및 그 거부에 관한 사항

《예시》

oo는 귀하의 정보를 수시로 저장하고 찾아내는 '쿠키(cookie)', xx 등 개인정보를 자동으로 수집하는 장치를 설치·운영합니다. 쿠키란 oo의 웹사이트를 운영하는데 이용되는 서버가 귀하의 브라우저에 보내는 아주 작은 텍스트 파일로서 귀하의 컴퓨터 하드디스크에 저장됩니다. xx는 ~이며, ~ 운영됩니다.

oo은(는) 다음과 같은 목적을 위해 쿠키 등을 사용합니다.

▶ 쿠키 등 사용 목적

- 회원과 비회원의 접속 빈도나 방문 시간 등을 분석, 이용자의 취향과 관심분야를 파악 및 자취 추적, 각종 이벤트 참여 정도 및 방문 회수 파악 등을 통한 타겟 마케팅 및 개인 맞춤 서비스 제공

귀하는 쿠키 설치에 대한 선택권을 가지고 있습니다. 따라서, 귀하는 웹브라우저에서 옵션을 설정함으로써 모든 쿠키를 허용하거나, 쿠키가 저장될 때마다 확인을 거치거나, 아니면 모든 쿠키의 저장을 거부할 수도 있습니다.

▶ 쿠키 설정 거부 방법

예: 쿠키 설정을 거부하는 방법으로는 회원님이 사용하시는 웹 브라우저의 옵션을 선택함으로써 모든 쿠키를 허용하거나 쿠키를 저장할 때마다 확인을 거치거나, 모든 쿠키의 저장을 거부할 수 있습니다.

설정방법 예(인터넷 익스플로어의 경우)

: 웹 브라우저 상단의 도구 > 인터넷 옵션 > 개인정보

단, 귀하께서 쿠키 설치를 거부하였을 경우 서비스 제공에 어려움이 있을 수 있습니다.

▶ xx 설정 거부 방법

-

《해설》

☞ 쿠키 등과 같이 개인정보를 자동으로 수집하는 장치를 설치 및 운영할 경우, 이의 설치·운영 및 그 거부에 관한 사항을 개인정보취급방침에 공개하여야 합니다.

☞ 쿠키란 웹 서버가 웹 브라우저에 보내어 저장했다가 서버의 부가적인 요청이 있을 때 다시 서버로 보내 주는 문자열 정보를 말합니다.

- 예를 들면, 어떤 사용자가 특정 웹 사이트에 접속한 후 그 사이트 내에서 어떤 정보를 보았는지 등에 관한 기록을 남겨 놓았다가, 다음에 접속했을 때 그것을 읽어 이전의 상태를 유지하면서 검색할 수 있게 하는 역할을 하는 것입니다.

☞ 이러한 쿠키처럼 개인정보를 자동으로 수집하는 장치의 경우 편의성을 제공하는 측면도 있지만, 이용자가 인터넷에서 어떤 내용을 봤는지 어떤 상품을 샀는지 등 모든 정보가 기록되기 때문에 프라이버시 침해의 가능성 또한 존재합니다.

☞ 따라서 귀사가 쿠키와 같은 개인정보를 자동으로 수집하는 장치를 설치·운영하실 경우, 그 사실과 사용 목적을 고지하시고 거부를 원할 경우 정보주체가 취할 수 있는 방법을 구체적으로 기재하셔야 합니다.

- 쿠키 등 자동 수집 장치를 운영하지 않으실 경우, 그 사실을 기재하시면 됩니다.

차. 개인정보관리책임자 또는 개인정보담당 부서

《예시》

oo는 고객의 개인정보를 보호하고 개인정보와 관련한 불만을 처리하기 위하여 아래와 같이 관련 부서 및 개인정보관리책임자를 지정하고 있습니다.

▶ 개인정보관리책임자

성명 :
전화번호 :
이메일 :

또는

▶ 개인정보담당부서

성명 :
전화번호 :
이메일 :

귀하께서는 oo사의 서비스를 이용하시며 발생하는 모든 개인정보보호 관련 민원을 개인정보관리책임자 혹은 담당부서로 신고하실 수 있습니다. 회사는 이용자들의 신고사항에 대해 신속하게 충분한 답변을 드릴 것입니다.

《해설》

☞ 개인정보를 수집·처리하는 모든 기업은 정보주체의 개인정보를 보호하고 개인정보와 관련한 정보주체의 불만을 처리하기 위하여 개인정보 취급 부서의 장 이상의 지위에 있는 자를 개인정보관리책임자로 지정하여야 합니다.

◆ 5인 미만의 영세 사업자의 경우 개인정보관리책임자를 별도로 임명하지 않으시고 대표자로 기재하셔도 됩니다.

<붙임> 개인정보취급방침 작성예시

○○의 개인정보취급방침은 다음과 같은 내용을 담고 있습니다

- 가. 수집하는 개인정보 항목 및 수집방법
- 나. 개인정보의 수집 및 이용목적
- 다. 수집한 개인정보의 공유 및 제공
- 라. 개인정보취급 위탁
- 마. 수집한 개인정보의 보유 및 이용기간
- 바. 개인정보의 파기절차 및 방법
- 사. 이용자 및 법정대리인의 권리와 그 행사방법
- 아. 개인정보 자동 수집 장치의 설치·운영 및 그 거부에 관한 사항
- 자. 개인정보 관리책임자 및 담당자의 소속성명 및 연락처

가. 수집하는 개인정보 항목 및 수집방법

○○는 회원가입, 상담, 서비스 신청 등을 위해 아래와 같은 개인정보를 수집하고 있습니다.

- ▶ 이름, 이메일, 주민등록번호, 주소, 연락처, 핸드폰 번호, 월소득, 직업

또한 서비스 이용과정이나 사업 처리 과정에서 아래와 같은 정보들이 생성되어 수집될 수 있습니다.

- ▶ 서비스 이용기록, 접속 로그, 쿠키, 접속 IP 정보, 결제기록, 이용정지 기록

○○는 다음과 같은 방법으로 개인정보를 수집합니다

- ▶ 홈페이지, 서면양식, 전화·팩스를 통한 회원가입, 상담 게시판, 경품 행사 응모, 배송 요청
- ▶ 제휴사로부터의 제공
- ▶ 생성정보 수집 툴을 통한 수집

나. 개인정보 수집 및 이용목적

○○는 수집한 개인정보를 다음의 목적을 위해 활용합니다

■ 개인정보보호관리체계 인증준비 안내서(부 록)

▶ 서비스 제공에 관한 계약 이행 및 서비스 제공에 따른 요금정산

- 콘텐츠 제공, 물품배송 또는 청구서 등 발송, 금융거래 본인 인증 및 금융 서비스, 구매 및 요금 결제, 요금추심

▶ 회원 관리

- 회원제 서비스 이용에 따른 본인확인, 개인식별, 불량회원의 부정 이용 방지와 비인가 사용 방지, 가입 의사 확인, 가입 및 가입횟수 제한, 만14세 미만 아동 개인정보 수집 시 법정 대리인 동의여부 확인 추후 법정 대리인 본인확인 분쟁 조정을 위한 기록보존, 불만처리 등 민원처리, 고지사항 전달

▶ 마케팅 및 광고에 활용

- 신규 서비스(제품) 개발 및 특화, 인구통계학적 특성에 따른 서비스 제공 및 광고 게재, 접속 빈도 파악, 회원의 서비스 이용에 대한 통계, 이벤트 등 광고성 정보 전달

▶ 기타

- 0000, 000, 000

다. 개인정보의 공유 및 제공

[제3자 제공 안할 경우]

OO는 이용자의 개인정보를 원칙적으로 외부에 제공하지 않습니다 다만, 아래의 경우에는 예외로 합니다.

- 이용자들이 사전에 동의한 경우
- 법령의 규정에 의거하거나 수사 목적으로 법령에 정해진 절차와 방법에 따라 수사기관의 요구가 있는 경우

[제3자 제공할 경우]

oo사는 회원에 대하여 보다 더 질 높은 서비스 제공 등을 위해 아래와 같이 귀하의 개인정보를 제공하고 있습니다.

▶ 제공정보의 이용 목적 : 제휴 마케팅

- 제공 대상 : 제휴 업체(oo 레스토랑, oo 스파게티)
- 제공 정보 : 이름, 이메일, 핸드폰 번호, 주소, 생년월일
- 제공 정보의 보유 및 이용 기간 : oo사 회원 탈퇴 시까지

▶ 제공정보의 이용 목적 : 보험판매 및 카드발급 등의 TM

- 제공 대상 : oo 보험, oo 카드
- 제공 정보 : 이름, 주민등록번호, 전화번호, 주소, 이메일
- 제공 정보의 보유 및 이용 기간 : 제휴계약 종결 시까지

다만, 아래의 경우에는 예외로 합니다.

- 이용자들이 사전에 동의한 경우
- 법령의 규정에 의거하거나 수사 목적으로 법령에 정해진 절차와 방법에 따라 수사기관의 요구가 있는 경우

라. 수집한 개인정보 취급 위탁

[업무위탁 안 할 경우]

oo는 고객님의 동의없이 고객님의 개인정보 취급을 외부 업체에 위탁하지 않습니다. 향후 그러한 필요가 생길 경우, 위탁 대상자와 위탁 업무 내용에 대해 고객님의 통지하고 필요한 경우 사전 동의를 받도록 하겠습니다.

[업무위탁 할 경우]

oo는 서비스 이행을 위해 아래와 같이 개인정보 취급 업무를 외부 전문업체에 위탁하여 운영하고 있습니다.

▶ oo 서비스

- 위탁업무 내용 : 이동통신사 신규고객 및 번호이동 가입 고객 유치

▶ oo 컨설팅

- 위탁업무 내용 : 상담업무 효율성 제고를 위한 고객센터 운영

마. 수집한 개인정보의 보유 및 이용기간

원칙적으로, 개인정보 수집 및 이용목적이 달성된 후에는 해당 정보를 지체없이 파기합니다. 단, 다음의 정보에 대해서는 아래의 이유로 명시한 기간 동안 보존합니다.

■ 개인정보보호관리체계 인증준비 안내서(부 록)

<내부 방침에 의한 정보보유 사유>

▶ 회원 ID

- 보존 이유 : 서비스 이용의 혼선방지
- 보존 기간 : oo

<관련법령에 의한 정보보유 사유>

그리고 ~법, ~에 관한 법률 등 관계법령의 규정에 의하여 보존할 필요가 있는 경우 회사는 관계법령에서 정한 일정한 기간 동안 회원정보를 보관합니다. 이 경우 회사는 보관하는 정보를 그 보관의 목적으로만 이용하며 보존기간은 아래와 같습니다.

▶ ~에 관한 기록

- 보존 이유 : ~에 관한 법
- 보존 기간 : oo

▶ ~에 관한 기록

- 보존 이유 : ~에 관한 법
- 보존 기간 : oo

바. 개인정보 파기절차 및 방법

oo는 원칙적으로 개인정보 수집 및 이용목적이 달성된 후에는 해당 정보를 지체 없이 파기합니다. 파기절차 및 방법은 다음과 같습니다.

▶ 파기절차

- 회원님이 회원가입 등을 위해 입력하신 정보는 목적이 달성된 후 내부 방침 및 기타 관련 법령에 의한 정보보호 사유에 따라(보유 및 이용기간 참조) 일정 기간 저장된 후 파기되어집니다.

동 개인정보는 법률에 의한 경우가 아니고서는 보유되어지는 이외의 다른 목적으로 이용되지 않습니다.

▶ 파기방법

- 종이에 출력된 개인정보는 분쇄기로 분쇄하거나 소각을 통하여 파기하고
- 전자적 파일형태로 저장된 개인정보는 기록을 재생할 수 없는 기술적 방법을 사용하여 삭제합니다.

사. 이용자 및 법정 대리인의 권리와 그 행사방법

이용자 및 법정 대리인은 언제든지 등록되어 있는 자신 혹은 당해 만14세 미만 아동의 개인정보를 조회하거나 수정할 수 있으며 가입해지를 요청할 수도 있습니다.

이용자 혹은 만 14세 미만 아동의 개인정보 조회·수정을 위해서는 ‘개인정보변경’(또는 ‘회원정보수정’ 등)을, 가입해지(동의철회)를 위해서는 “회원탈퇴”를 클릭하여 본인 확인 절차를 거치신 후 직접 열람, 정정 또는 탈퇴가 가능합니다.

혹은 개인정보관리책임자에게 서면, 전화 또는 이메일로 연락하시면 지체없이 조치하겠습니다.

귀하가 개인정보의 오류에 대한 정정을 요청하신 경우에는 정정을 완료하기 전까지 당해 개인정보를 이용 또는 제공하지 않습니다. 또한 잘못된 개인정보를 제3자에게 이미 제공한 경우에는 정정 처리결과를 제3자에게 지체없이 통지하여 정정이 이루어지도록 하겠습니다.

oo는 이용자 혹은 법정 대리인의 요청에 의해 해지 또는 삭제된 개인정보는 “oo가 수집하는 개인정보의 보유 및 이용기간”에 명시된 바에 따라 처리하고 그 외의 용도로 열람 또는 이용할 수 없도록 처리하고 있습니다.

아. 개인정보의 자동 수집 장치의 설치·운영 및 그 거부에 관한 사항

oo는 귀하의 정보를 수시로 저장하고 찾아내는 ‘쿠키(cookie)’, xx 등 개인정보를 자동으로 수집하는 장치를 설치·운영합니다. 쿠키란 oo의 웹사이트를 운영하는 데 이용되는 서버가 귀하의 브라우저에 보내는 아주 작은 텍스트 파일로서 귀하의 컴퓨터 하드디스크에 저장됩니다. xx는 ~이며, ~ 운영됩니다.

oo은(는) 다음과 같은 목적을 위해 쿠키 등을 사용합니다.

▶ 쿠키 등 사용 목적

- 회원과 비회원의 접속 빈도나 방문 시간 등을 분석, 이용자의 취향과 관심분야를 파악 및 자취 추적, 각종 이벤트 참여 정도 및 방문 회수 파악 등을 통한 타겟 마케팅 및 개인 맞춤 서비스 제공

귀하는 쿠키 설치에 대한 선택권을 가지고 있습니다. 따라서, 귀하는 웹브라우저에서 옵션을 설정함으로써 모든 쿠키를 허용하거나, 쿠키가 저장될 때마다 확인을 거치거나, 아니면 모든 쿠키의 저장을 거부할 수도 있습니다.

■ 개인정보보호관리체계 인증준비 안내서(부 록)

▶ 쿠키 설정 거부 방법

예: 쿠키 설정을 거부하는 방법으로는 회원님이 사용하시는 웹 브라우저의 옵션을 선택함으로써 모든 쿠키를 허용하거나 쿠키를 저장할 때마다 확인을 거치거나, 모든 쿠키의 저장을 거부할 수 있습니다.

설정방법 예(인터넷 익스플로어의 경우)

: 웹 브라우저 상단의 도구 > 인터넷 옵션 > 개인정보

단, 귀하께서 쿠키 설치를 거부하였을 경우 서비스 제공에 어려움이 있을 수 있습니다.

▶ xx 설정 거부 방법

-

자. 개인정보 관리 책임자

oo는 고객의 개인정보를 보호하고 개인정보와 관련한 불만을 처리하기 위하여 아래와 같이 관련 부서 및 개인정보관리책임자를 지정하고 있습니다.

▶ 개인정보관리책임자

성명 :
전화번호 :
이메일 :

또는

▶ 개인정보담당부서

성명 :
전화번호 :
이메일 :

귀하께서는 oo사의 서비스를 이용하시며 발생하는 모든 개인정보보호 관련 민원을 개인정보관리책임자 혹은 담당부서로 신고하실 수 있습니다. 회사는 이용자들의 신고사항에 대해 신속하게 충분한 답변을 드릴 것입니다.

공고일자 : 2007년 03월 14일

시행일자 : 2007년 03월 22일

이전 개인정보보호정책 보기 (2006년 11월 6일 - 2007년 3월 21일 적용)

<개인정보 수집·동의 절차>



▶ 개인정보수집, 이용 등에 대한 사전동의

개인정보를 수집하기 위해서는 이용자에게 알리고 동의를 얻어야 합니다. 내용이 변경된 경우에도 이에 대한 동의를 득 해야 합니다.

개인정보란 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호, 문자, 음성, 음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에는 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말합니다.

따라서 회원가입, 물건 구매 및 배송, 상담 및 견적 등의 서비스 이용을 위해, 이름, 이메일, 연락처 등 하나 이상의 개인정보를 제공할 것을 요청할 경우 이는 개인정보 수집에 해당합니다.

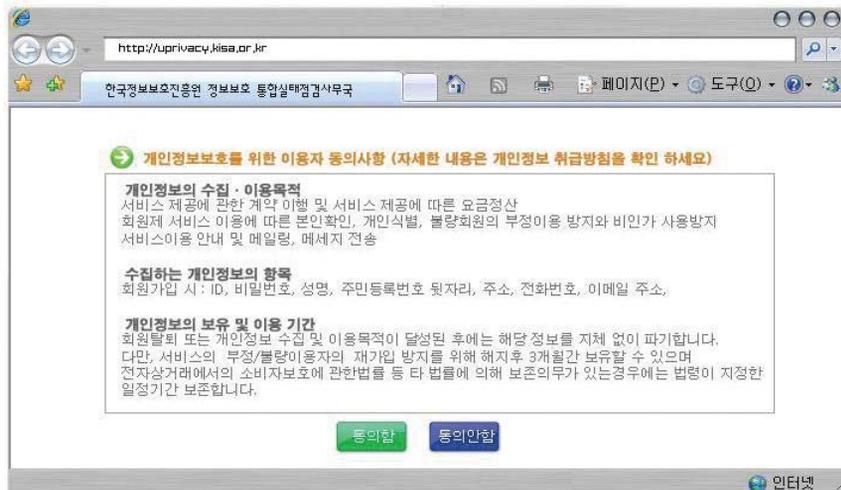
1 개인정보 수집경로에는 사용자의 동의를 받는 절차를 마련해야 합니다.



2 동의를 받을 때는 다음 세가지 항목에 대해 동의받으세요.

- ① 개인정보의 수집 - 이용목적 (예) 본인 확인, 고지 사항 전달, 콜센터배송 등)
 - ② 수집하는 개인정보의 항목 (예) 이름, 전화번호, IP 정보 등)
 - ③ 개인정보의 보유 및 이용 기간 (예) 회원탈퇴 등 서비스 목적 달성 후 즉시 파기)
- ※ 이때 이용자가 동의를 하지 않는 경우 개인정보를 수집할 수 없습니다.

3. 동의절차 구축. 예)



개인정보 수집·동의 절차 예시(쇼핑몰1)

Join ■■■■

- 다음은 회원가입을 위한 필수입력 항목입니다.

아이디	<input type="text"/> 아이디중복확인 * (영문소문자/숫자, 4~16자)
비밀번호	<input type="password"/> (영문자/숫자, 4~16자)
비밀번호 확인	<input type="password"/>
비밀번호 확인시 질문	기억에 남는 추억의 장소? <input type="text"/>
비밀번호 확인시 답변	<input type="text"/>
이름	<input type="text"/>
주민등록번호	<input type="text"/> - <input type="text"/> 실명인증하기 *
주소	<input type="text"/> - <input type="text"/> 우편번호찾기 * <input type="text"/> 기본주소 <input type="text"/> 나머지주소
유선전화	<input type="text"/> - <input type="text"/> - <input type="text"/>
휴대전화	없음 <input type="checkbox"/> - <input type="text"/> - <input type="text"/>
SMS 수신여부	SMS 문자메시지로 이벤트 및 유용한 쇼핑정보를 받으시겠습니까? <input checked="" type="radio"/> 예 <input type="radio"/> 아니오
이메일	<input type="text"/> @ <input type="text"/> 선택 <input type="text"/> * 주문 및 배송확인 정보 등이 E-mail로 발송되므로 반드시 수신가능한 E-mail 주소를 입력 하여주십시오. * 판매일은 입력할 수 없습니다.(@hanmail.net, @daum.net)
뉴스메일	뉴스 메일을 받으시겠습니까? <input checked="" type="radio"/> 동의 <input type="radio"/> 동의안함 <input type="radio"/> 절대수신안함

이용약관 동의

제2조(정의)

① "몰"이란 회사가 재화 또는 용역(이하 "재화등"이라 함)을 이용자에게 제공하기 위하여 컴퓨터등 정보통신설비를 이용할 수 있도록 설정한 가상의 영업장을 말하며, 아울러 사이버몰을 운영하는 사업자의 의미로도 사용됩니다.

② "이용자"란 "몰"에 접속하여 이 약관에 따라 "몰"이 제공하는 서비스를 받는 회원 및 비회원을 말합니다.

③ "회원"이라 함은 "몰"에 개인정보를 제공하여 회원등록을 한 자로서, "몰"의 정보를 지속적으로 제공받으며, "몰"이 제공적으로 이용할 수 있는 자를 말합니다.

④ "비회원"이라 함은 회원에 가입하지 않고 "몰"이 제공하는 서비스를 이용하는 자를 말합니다.

이용약관에 동의하십니까? 동의함

개인정보취급방침 동의

■ 수집하는 개인정보 항목

회사는 회원가입, 상담, 서비스 신청 등등을 위해 아래와 같은 개인정보를 수집하고 있습니다.

- 수집항목 : 이름, 생년월일, 성별, 로그인ID, 비밀번호, 비밀번호 질문과 답변, 자택 전화번호, 자택 주소, 휴대전화번호, 쿠키, 결제기록
- 개인정보 수집방법 : 홈페이지(회원가입)

■ 개인정보의 수집 및 이용목적

개인정보취급방침에 동의하십니까? 동의함

JOIN-US
회원가입

DELETE
탈퇴하기

개인정보 수집·동의 절차 예시(포털)

회원약관 확인

안녕하세요. 항상 새로운 서비스를 위해 노력하고 있는 [회사명]입니다.
[회사명] 회원으로 가입하시면, [회사명] 제공하는 다양한 서비스를 제공받으실 수 있습니다.

[회사명] 이용약관

제 1 조 (목적)

이 약관은 [회사명] (이하 "회사")가 제공하는 [서비스명] 및 [서비스명] 관련 제반 서비스의 이용과 관련하여 회사와 회원과의 권리, 의무 및 책임사항, 기타 필요한 사항을 규정함을 목적으로 합니다.

제 2 조 (정의)

이용약관에 동의 합니다.

개인정보 수집 및 이용에 대한 안내

수집하는 개인정보의 항목

가. 회사는 회원가입, 원활한 고객상담, 각종 서비스의 제공을 위해 최초 회원가입 당시 아래와 같은 개인정보를 수집하고 있습니다.

<일반 회원가입 시>

- 필수항목 : 성명, 주민등록번호, 외국인등록번호 또는 여권번호(외국인에 한함), 아이디, 비밀번호, 본인확인문
다. 이메일 주소, 전화번호, 이메일 주소, 비밀번호, 본인확인 정보

수집하는 개인정보 항목에 동의합니다.

개인정보의 수집 및 이용 목적

가. 서비스 제공에 관한 계약 이행 및 서비스 제공에 따른 요금정산
콘텐츠 제공, 특정 맞춤 서비스 제공, 물품배송 또는 청구서 등 발송, 본인인증, 구매 및 요금 결제, 요금추심

나. 회원관리

회원제 서비스 이용 및 제한적 본인 확인제에 따른 본인확인, 개인식별, 불량회원(네이버이용약관 제20조 1항 중

개인정보 수집 및 이용목적에 동의합니다.

개인정보의 보유 및 이용기간

이용자의 개인정보는 원칙적으로 개인정보의 수집 및 이용목적이 달성되면 지체 없이 파기합니다. 단, 다음의 정보에 대해서는 아래의 이유로 명시한 기간 동안 보존합니다.

가. 회사 내부 방침에 의한 정보보유 사유

보유기간

개인정보 보유 및 이용기간에 동의합니다.

동의

동의하지 않습니다

개인정보 수집·동의 절차 예시(초고속통신)

회원가입

[] 홈페이지의 회원이 되시면 보다 편리하게 [] 서비스를 이용하실 수 있습니다. 인터넷 빌링, 온라인 상담 등을 빠르고 편하게 이용하실 수 있습니다.

개인 기업

● [] 홈페이지의 회원이 되시면 보다 편리하게 [] 서비스를 이용하실 수 있습니다. 인터넷 빌링, 온라인 상담 등을 빠르고 편하게 이용하실 수 있습니다.

이용약관

[]는 가입자(이하 "회원")의 이용 조건 및 재반결처에 관한 사항을 정하는데 목적이 있습니다.

제2조 회원의 가입 및 서비스 이용
회원의 가입
[] 홈페이지의 회원이 되고자 할 경우에는 본 약관의 동의와 회원가입신청서를 작성하여 운영자의 이용승낙이 있어야 합니다.

가입 신청서를 검토한 결과 부적합 한 사유가 발생 하면 "회원"가입이 거부 될 수도 있습니다.

동의 합니다. 동의하지 않습니다.

개인정보 수집 및 이용안내

[] (이하 "회사")는 고객님의 개인정보를 중요시하며, "정보통신망 이용촉진 및 정보보호"에 관한 법률을 준수하고 있습니다. 회사는 개인정보취급방침을 통하여 고객님의께서 제공하시는 개인정보가 어떠한 용도와 방식으로 이용되고 있으며, 개인정보보호를 위해 어떠한 조치가 취해지고 있는지 알려드립니다. 회사는 개인정보취급방침을 개정하는 경우 웹사이트 공지사항(또는 개별공지)을 통하여 공지할 것입니다.

○ 본 방침은 2008년 10월 10일 부터 시행됩니다

1. 수집하는 개인정보의 수집 및 이용목적

동의 합니다. 동의하지 않습니다.

개인정보 제3자 제공 안내

본인은 신청란에 기재된 개인정보를 다음과 같이 귀사 []가 수집, 이용, 제3자제공함에 동의합니다.

회사는 고객의 개인정보를 개인정보취급방침의 「개인정보의 이용목적」에서 고지한 범위 또는 서비스이용약관에 명시한 범위 내에서 사용하며, 동 범위를 넘어 이용하거나 제3자에게 제공하지 않습니다. 다만, 고객의 동의가 있거나 다음사항의 경우 예외로 합니다.

- 서비스 제공에 따른 요금 정산을 위해 필요한 경우
- 서비스의 제공에 관한 계약의 이행을 위해 필요한 개인정보로서 경제적·기술적인 사유로 통상의 동의

동의 합니다. 동의하지 않습니다.

개인정보 취급위탁 안내

회사는 보다 나은 서비스 제공과 고객님의 제공 등 업무수행을 원활하게 하기 위해 고객님의 개인정보를 다음과 같이 외부 전문업체에 취급위탁(수집, 보관, 처리, 이용, 제공, 관리, 폐기 등)하여 처리하고 있습니다. 위탁자에 대해서는 "개인정보위탁합의서" 등을 통하여 관련 법규 및 지침의 준수, 제3자 제공 금지, 사고시 책임부담, 위탁기간 종료 즉시 개인정보의 반납/파기 의무 등을 규정하여 관리하고 있습니다.

위탁 받은 자	위탁 업무내용
[]	고객유치, 개통, AS, 품질관리, 신상품소개, 리텐션 등

동의 합니다. 동의하지 않습니다.

※ 자세한 내용은 "개인정보취급방침"을 확인하시기 바랍니다.

제3자 제공 및 위탁 작성 예시(초고속통신1)

이용 약관

제 1 장 총칙

제 1 조 (목적)

이 약관은 주식회사 [] (이하 "회사"라 합니다)이 제공하는 [], 사이버고객센터 [] 서비스(이하 "서비스"라 합니다)의 이용조건 및 절차 등에 관한 사항을 규정함을 목적으로 합니다.

이용약관에 동의 합니다.

개인정보의 수집 및 이용안내

1) 개인정보의 수집 및 이용목적

① 회사는 수집한 개인정보를 다음의 목적을 위해 활용합니다.

② 서비스 제공에 관한 계약 이행 및 서비스 제공에 따른 요금정산

- 콘텐츠 제공, 구매 및 요금 결제, 물품배송 또는 청구서 등 발송, 금융거래 본인 인증 및 금융 서비스, 요금추심 등

③ 고객관리

- 회원제 서비스 이용에 따른 본인확인, 개인 식별, 불량회원의 부정 이용 방지와 비인가 사용 방지, 가입 의사 확인, 연령확인, 만14세 미만 아동 개인정보 수집 시 법정 대리인 동의여부 확인, 불만처리 등 민원처리,

개인정보의 수집 및 이용에 동의합니다.

개인정보 취급 위탁 안내

① 회사는 서비스 이행을 위해 아래와 같이 외부 전문업체에 위탁하여 운영하고 있습니다.

위탁 협력회사	위탁업무 내용
[] 및 대리점 [세부내용 링크]	고객유치 및 유지관리
[]	채권추심, 요금상당, 실명확인
[]	청구대행 업무(우편, 이메일),

개인정보 취급 위탁에 동의 합니다.

그룹사 공동마케팅 활용 동의 안내

① 서비스 가입화면에 입력한 고객님의 개인정보는 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』에 따라 당사(KTF)가 제 3자에게 제공 시 고객님의 동의를 얻어야 하는 정보입니다. 회사는 고객님의 개인정보를 가입신청서, 서비스 이용약관 및 개인정보취급방침에 고지 또는 명시한 범위 내에서 사용합니다.

② 회사는 특정한 서비스 가입, 이용 등 해당고객에 한하여 제공에 동의하신 고객님의 정보를 제공합니다.

1. 제공받는자:

[]

KTF 그룹사 공동마케팅 활용을 위한 개인정보를 제공하는데 동의 합니다.

제휴사 제공 동의 안내

① 회사는 고객님의 개인정보를 가입신청서, 서비스이용약관 및 개인정보취급방침에 고지 또는 명시한 범위 내에서 사용합니다.

② 회사는 고객님의 동의가 있거나 통신비밀보호법, 전기통신사업법, 국제기본법 등의 관계법령에 특별한 규정이 있는 경우, 법령에 정해진 절차와 방법에 따라 제한적으로 이용 제공합니다.

③ 회사는 특정한 서비스 가입, 이용 또는 별도동의 등 해당고객에 한하여 다음과 같이 제공합니다.

제공받는자	제공하는 개인정보항목	제공정보의 이용목적
[]	[]	콘텐츠 제공, 구매 및 요금 결제, 회원제 서비스

서비스의 가입/이용 시 필요한 개인정보를 제공하는데 동의 합니다.

동의합니다 동의하지않습니다

제3자 제공 및 위탁 작성 예시(초고속통신2)

HOME > 가이드센터 > 회원가입

회원가입

홈페이지의 회원이 되시면 보다 편리하게 서비스를 이용하실 수 있습니다. 인터넷 빌링, 온라인 상담 등을 빠르고 편하게 이용하실 수 있습니다

개인 기업

홈페이지의 회원이 되시면 보다 편리하게 서비스를 이용하실 수 있습니다. 인터넷 빌링, 온라인 상담 등을 빠르고 편하게 이용하실 수 있습니다.

이용약관

제1조 목적
 이 약관은 홈페이지(http://)가(이하 "운영자") 제공하는 정보서비스를 이용하는 가입자(이하 "회원")의 이용 조건 및 제반절차에 관한 사항을 정하는데 목적이 있습니다.

제2조 회원의 가입 및 서비스 이용
 회원의 가입
 홈페이지의 회원이 되고자 할 경우에는 본 약관의 동의와 회원가입신청서를 작성하여 운영자의 이용승낙이 있어야 합니다.

동의 합니다. 동의하지 않습니다.

개인정보 수집 및 이용안내

은 (이하 '회사')는 고객님의 개인정보를 중요시하며, "정보통신망 이용촉진 및 정보보호"에 관한 법률을 준수하고 있습니다. 회사는 개인정보취급방침을 통하여 고객님께서 제공하시는 개인정보가 어떠한 용도와 방식으로 이용되고 있으며, 개인정보보호를 위해 어떠한 조치가 취해지고 있는지 알려드립니다. 회사는 개인정보취급방침을 개정하는 경우 웹사이트 공지사항(또는 개별공지)을 통하여 공지할 것입니다.

o 본 방침은 2008년 10월 10일 부터 시행됩니다.

1. 수집하는 개인정보의 수집 및 이용목적

동의 합니다. 동의하지 않습니다.

개인정보 제 3자 제공 안내

본인은 신청란에 기재된 개인정보를 다음과 같이 귀사()가 수집, 이용, 제 3자제공함에 동의합니다.

회사는 고객의 개인정보를 개인정보취급방침의 「개인정보의 이용목적」에서 고지한 범위 또는 서비스이용약관에 명시한 범위 내에서 사용하며, 동 범위를 넘어 이용하거나 제3자에게 제공하지 않습니다. 다만, 고객의 동의가 있거나 다음사항의 경우 예외로 합니다.

- 서비스 제공에 따른 요금 정산을 위해 필요한 경우
- 서비스의 제공에 관한 계약의 이행을 위해 필요한 개인정보로서 경제적·기술적인 사유로 통상의 동의

동의 합니다. 동의하지 않습니다.

개인정보 취급위탁 안내

회사는 보다 나은 서비스 제공과 고객님의 제공 등 업무수행을 원활하게 하기 위해 고객님의 개인정보를 다음과 같이 외부 전문업체에 취급위탁(수집,보관,처리,이용,제공,관리,폐기 등)하여 처리하고 있습니다. 수탁자에 대해서는 "개인정보위탁합의서" 등을 통하여 관련 법규 및 지침의 준수, 제3자 제공 금지, 사고시 책임부담, 위탁기간 종료 즉시 개인정보의 반납/파기 의무 등을 규정하여 관리하고 있습니다.

위탁 받은 자	위탁 업무내용
	고객유치, 개통, AS, 품질관리, 신상품소개, 리텐션 등

동의 합니다. 동의하지 않습니다.

※ 자세한 내용은 "개인정보취급방침"을 확인하시기 바랍니다.

동의철회 작성 예시(포털)

회원약관 확인

안녕하세요. 항상 새로운 서비스를 위해 노력하고 있는 [회사명]입니다.
[회사명] 회원으로 가입하시면, [회사명] 제공하는 다양한 서비스를 제공받으실 수 있습니다.

[회사명] 이용약관

제 1 조 (목적)

이 약관은 [회사명] (이하 "회사")가 제공하는 [서비스명] 및 [서비스명] 관련 제반 서비스의 이용과 관련하여 회사와 회원과의 권리, 의무 및 책임사항, 기타 필요한 사항을 규정함을 목적으로 합니다.

제 2 조 (정의)

이용약관에 동의 합니다.

개인정보수집 및 이용에 대한 안내

수집하는 개인정보의 항목

가. 회사는 회원가입, 원활한 고객상담, 각종 서비스의 제공을 위해 최초 회원가입 당시 아래와 같은 개인정보를 수집하고 있습니다.

<일반 회원가입 시>

- 필수항목 : 성명, 주민등록번호, 외국인등록번호 또는 여권번호(외국인에 한함), 아이디, 비밀번호, 본인확인문
다. 이메일 주소, 연락처, 비밀번호 변경관리 정보

수집하는 개인정보 항목에 동의합니다.

개인정보의 수집 및 이용 목적

가. 서비스 제공에 관한 계약 이행 및 서비스 제공에 따른 요금정산
콘텐츠 제공, 특정 맞춤 서비스 제공, 물품배송 또는 청구서 등 발송, 본인인증, 구매 및 요금 결제, 요금추심

나. 회원관리

회원제 서비스 이용 및 제한적 본인 확인제에 따른 본인확인, 개인식별, 불량회원(네이버이용약관 제20조 1항 중

개인정보 수집 및 이용목적에 동의합니다.

개인정보의 보유 및 이용기간

이용자의 개인정보는 원칙적으로 개인정보의 수집 및 이용목적이 달성되면 지체 없이 파기합니다. 단, 다음의 정보에 대해서는 아래의 이유로 명시한 기간 동안 보존합니다.

가. 회사 내부 방침에 의한 정보보유 사유

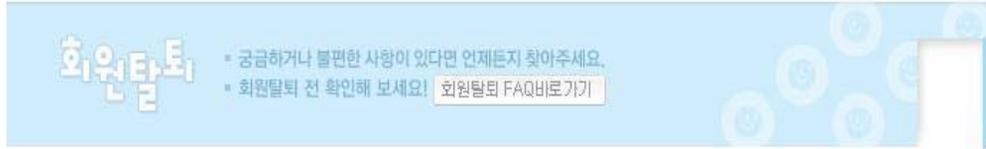
보유이용기간

개인정보 보유 및 이용기간에 동의합니다.

✔ 동의

동의하지 않습니다

동의철회 작성 예시(초고속통신)



1. 회원탈퇴 전, 아래의 사항을 반드시 확인하시기 바랍니다.

- 회원탈퇴를 신청하시면 해당 아이디는 즉시 탈퇴 처리되며, 탈퇴 후에는 회원님의 개인정보와 보유하신 아이템, , 블로그는 모두 삭제되며 복구 및 환불이 불가능합니다.
- 이메일을 에 연동하여 이용한 회원님께서 회원탈퇴 시 친구목록, 주소록, 뮤직앨범 등 서비스도 이용하실 수 없습니다.
- 클럽장인 경우, 클럽장 양도 또는 클럽삭제 후에 탈퇴할 수 있습니다.
 - Q. 클럽장 양도는 어떻게 하나요?
 - Q. 클럽 삭제는 어떻게 하나요?
- 모바일 정액제를 사용하고 있는 경우, 해지 후 탈퇴할 수 있습니다.
 - Q. 모바일 알라미 정액제 해지는 어떻게 하나요?
- 이용 회원님은 환불받으실 쇼핑머니가 있는지 반드시 확인해주세요.
 - Q. 환불받을 쇼핑머니 확인하기

2. 이럴 땐, 회원탈퇴를 하지 않으셔도 됩니다.

- 개인정보 변경(이메일, 비밀번호)을 하기 위해서라면 회원탈퇴를 하지 않으셔도 됩니다.
 - Q. 이메일, 비밀번호는 어디서 변경 하나요?
- 블로그를 삭제하기 위해서라면 회원탈퇴를 하지 않으셔도 됩니다.
 - Q. 블로그는 어디서 삭제 하나요?

부 록 6

개인정보보호 현황분석을 위한 체크리스트

개인정보보호관리과정 요구사항

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
1. 개인정보 정책수립	1.1 개인정보보호 관련 정책 및 내부관리계획 수립을 통해 명확한 지원 및 방향제시를 보증하여야 한다.	1.1.1 개인정보 보호 정책 수립	조직 내 개인정보 침해 가능성의 관리 및 책임을 기술한 개인정보보호 관련 정책을 수립하여야 하며, 동 정책은 국가나 관련 산업에서 정하는 법규제를 만족하여야 한다.	조직 내 개인정보보호정책이 마련되어 있는가?	조직의 경영목표를 지원할 수 있도록 개인정보보호의 법적, 규제적 요건과 전략적이고 조직적인 관리 방안을 기술한 개인정보보호관리체계 및 개인정보보호정책을 마련해야 한다.	필수	
		1.1.2 조직 및 책임 설정	개인정보보호활동에 대한 경영총의 명확한 지원 및 방향제시를 보증할 수 있는 조직을 구성하여야	개인정보보호정책이 국가나 관련 산업에서 정하는 개인정보보호 관련 법과 규제사항을 포함하여 수립하였는가?	중대한 보안사고 발생, 새로운 위협 또는 취약상의 발생, 개인정보보호 환경에 중대한 변화 등이 발생했을 경우에는 관련 사항의 타당성을 추가로 검토하여 이러한 내용을 빠짐없이 반영할 수 있도록 하는 절차를 마련하여야 한다.	필수	
		1.1.2 조직 및 책임 설정	개인정보보호활동에 대한 경영총의 명확한 지원 및 방향제시를 보증할 수 있는 조직을 구성하여야	개인정보보호 조직과 관련 직무의 역할 및 책임, 상호 연관관계가 개인정보보호 정책에 포함되어 있는가?	개인정보보호 조직 및 관련 직무의 명확한 역할 및 책임 등의 규명을 통해 개인정보보호 활동이 책임성있게 수행되어야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	관련 근거 여부
			한다. 또한 개인정보 보호 관리활동을 수행하고 검증하는 행들에 대한 역할 및 책임, 상호 연관관계 등을 정의하고 문서화하여야 한다.	조직의 특성을 반영하여 개인정보 보호 인적절히 활동하였는가?	개인정보보호활동을 원활히 수행하기 위해서는 적절한 규모의 개인정보보호 인력이 할당되어야 한다.	필수	
		1.1.3 내부관리계획 수립	개인정보보호 정책에 따른 개인정보보호 조직구성 및 운영 등이 포함된 내부관리계획을 수립하여 이행하여야 한다.	내부관리계획에 개인정보보호 조직구성 및 운영 등의 세부 사항이 명시되어 있는가?	내부관리계획 수립 시에는 다음 각 호의 사항이 포함되도록 하여야 한다. 1. 개인정보관리책임자의 자격요건 및 지정에 관한 사항 2. 개인정보관리책임자와 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. 그 밖에 개인정보보호를 위해 필요한 사항	필수	0

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	불필수 여부
2. 관리체계 범위설정	2.1 개인정보처리체계의 범위를 설정하고, 개인정보 및 개인정보를 관리 자산을 분류하고 식별하여야 한다.	2.1.1 개인정보 식별	신청기관의 개인정보 및 개인정보 관리 제산을 분류 및 식별하고 개인정보 자산의 형태, 소유자, 관리자, 특성 등을 포함하여 목록을 만들어야 한다.	개인정보 관련 업무 및 서비스를 식별하고 관련 자산을 파악하였는가? 조직의 업무 수행과 관련된 주요 개인정보 자산을 식별하여 목록을 관리하고 있는가?	개인정보처리체계 범위내 조직의 개인정보 관련 업무 및 업무를 분류하고 식별하여야 한다. 개인정보처리체계 범위내 조직의 개인정보 관련 업무와 유관자산을 식별하고, 개별 개인정보 자산 뿐만 아니라, 개인 정보 취급에 따라 분석된 흐름도를 포함하여야 한다.	필수	
				개인정보 목록은 개인정보 및 개인정보 자산 항목별, 업무처리별 자산분류 및 조기에 기초하여 작성되었는지, 해당 자산항목별 형태, 소유자, 관리자, 특성 등을 포함하였는지?	개인정보 목록은 일반적으로 개인정보 관련 서비스 및 업무별, 업무처리별 처리 및 취급 시스템 등의 분류 기준으로 조사하여 작성되는 것이 일반적이며 각 분류별 소유자, 관리자, 사용자 명시되어야 한다. 또한, 개인정보 자산목록에는 자산의 Type, 형태, 위치, 백업정보, 라 이센스 정보 및 가치 등이 포함 되어야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	관련 근거
		개인정보 보호관리 체계 범위 설정	신청사업자의 특성, 기술, 자산 등 내·외적 환경에 대한 영향을 미치는데 고려하여 개인정보 보호관리 체계의 범위를 설정하여야 한다.	개인정보보호관리의 범위가 명확하게 정의되어 있고 문서화 되어 있는가? - 개인정보의 정의와 대상이 명시되어 있는가 - 개인정보를 보호하기 위한 관리체계 범위가 명시되어 있는가	개인정보보호관리체계 범위를 정은 조직의 핵심업무기능을 수행하거나 위험이 높은 부분을 반드시 포함하여 선정해야 한다. 또한, 개인정보보호관리체계 범위 선정시 개인정보 처리를 취급하는 업무부서 및 개인정보취급시스템, 관련서비스, 개인정보취급자등을 포함하도록 한다.	필수	
		2.1.2		정의된 범위 내에서 예외가 있을 경우, 그 예외 이유가 명확히 설명되어 있는가?	조직이 가지고 있는 여러 제약적, 시간적, 기술적 제약조건으로 개인정보보호관리체계의 범위에 예외가 있을 수 있으며, 따라서 해당사항에 대한 이유를 분명히 명시하여야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	관련 근거 여부
3. 위험관리	3.1 신청사업자는 개인정보 취급 서비스에 적합한 위험 관리 계획을 수립하고, 위험관리 계획에 따라 보호 대책을 수립하여야 한다.	3.1.1 위험 관리 계획 수립	신청사업자의 목표 및 정책, 법적 요구사항 등을 고려하여 조직, 역할, 책임, 주요 과정을 포함한 위험 관리 계획을 수립하고, 신청기관에 적합한 위험관리 방법을 선택하여야 한다. 이 위험관리 방법은 조직과 개인정보보호 환경변화에 대응할 수 있도록 지속적으로 검토하여야 한다.	신청사업자의 목표 및 정책, 법적 요구사항 등을 고려하여 조직, 역할, 책임, 주요 과정을 포함한 위험 관리 계획을 수립하고, 신청기관에 적합한 위험관리 방법을 선택하여야 한다. 1. 위험관리 방법론은 상세위험분석접근법, 베이스라인접근법(Baseline approach) 등 있다. 2. 위험관리 방법론은 사업자(신청기관) 업종유형, 개인정보취급서비스 종류, 조직구조 등에 따라 사업자가 선택할 수 있다.	위험관리 계획은 신청사업자 목표 및 정책, 법적 요구사항 등을 고려하여 작성되어야 한다. 1. 위험관리 방법론은 상세위험분석접근법, 베이스라인접근법(Baseline approach) 등 있다. 2. 위험관리 방법론은 사업자(신청기관) 업종유형, 개인정보취급서비스 종류, 조직구조 등에 따라 사업자가 선택할 수 있다.	필수	
		3.1.2 위험평가	위험관리계획에 따라 위험평가를 수행하고 개인정보침해를 방지할 수 있는 목표위험 수준이 설정되어 관리되어야 한다.	위험관리 방법은 환경변화에 대응할 수 있도록 지속적인 검토가 이루어지고 있는가? 수립된 위험관리계획에 따라 위험평가를 수행하고 있는가?	위험관리 방법은 신청사업자의 위험관리 방법에 대응할 수 있도록 지속적인 검토가 이루어져야 한다. 수립된 위험관리계획에 따라 위험평가를 수행하여야 하며, 변경사항은 적합한 승인 절차를 거쳐야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	관련 근거
				개인정보침해사고의 방지 가능한 합리적인 목표 위험 수준을 설정하였는가?	식별된 위험을 전부 제거할 수 없는 경우 조직의 임무 및 개인정보 자산에서 수용 가능한 목표 위험수준이 설정되어 있다. · 목표 위험수준은 개인정보침해사고를 방지할 수 있는 합리적인 수준이 되어야 한다.	필수	
		3.1.3 위험 관리를 위한 보호 대책 및 이행 계획 수립	신장기관의 위험관리를 위한 보호대책과 목적에 부합하도록 위험을 수용 가능한 수준으로 감소시켜야 한다. 이를 위해, 위험평가에 의거한 위험처리, 위험 수용, 위험회피, 위험전가 등의 전략을 설정하고, 이에 적절한 보호대책을 선정하여야 한다. 선정된 대책을 구현하기 위한 구체적인 일정계획을 수립하고 최고경영진의 승인을 받아야 한다.	위험관리 계획에 따른 보호 대책이 선정되었는가?	위험관리를 위한 보호대책의 이행계획에 보호대책 구현을 위한 책임, 예산, 일정, 운영 방법 등이 명확히 정의되어야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	관련 근거
4. 구현	4.1 개인정보보호 대책의 이행 계획에 따라 보호 대책을 구현하고, 대 책의 효과성 에 대하여 주 기적인 검토 를 수행하여 야 한다.	보호 대책 의 효과적 구현	개인정보보호대책의 이행 계획에 따라 대 책을 구현하여야 한 다. 구현 후 검토 계 획에 따라 일정 시간 이 흐른 후 구현 성 과를 검토 및 보고 하여야 한다.	위험관리를 위한 보호대책 의 이행계획에 대한 최고경 영자 또는 CPO의 승인이 있는가?	위험관리를 위한 보호대책의 이행계획에 대한 효율적, 호 영자 또는 CPO의 승인이 있는가? 영자의 승인이 있어야 한다.	필수	
	4.1.1 개인정보보호 대책의 이행 계획에 따라 보호 대책을 구현하고, 대 책의 효과성 에 대하여 주 기적인 검토 를 수행하여 야 한다.	개인정보보호대책의 이행 계획에 따라 보호대책이 구현되었는가?	개인정보보호대책의 이행 계획에 따라 보호대책이 구현되었는가? 구현된 보호대책의 정확성 및 효과성을 검토하였는가?	개인정보보호대책의 이행 계획에 따라 보호대책이 구현되었는가? 구현된 보호대책의 정확성 및 효과성을 검토하였는가? 구현된 보호대책의 정확성 및 효과성에 대한 평가가 지속적 으로 수행되어야 한다. 그러 나, 구현의 효과성 평가는 모 안조직에서 지속적으로 관리 되고 있는 상황일 수 있으므 로 특정 이벤트에 의한 검토 내역이 존재하지 않을 경우 이에 대한 검증이 가능한 회 사 시스템 등을 파악하여 확 인하여야 한다.	개인정보보호대책의 이행계획 에 따라 보호대책이 일관성 있게 구현되어야 하며, 구현 여부 및 변경관리 내역이 문 서화 되어 있어야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	관련 근거 여부
5. 사물관리	5.1 개인정보보호관리체계에 대한 지속적인 개선 활동이 문서화되고, 정기적으로 점검되어야 한다.	5.1.1 모니터링 및 개선	개인정보보호관리체계는 지속적으로 모니터링하여 관련 문헌 자료를 검토하고, 개선점을 도출하며, 개선할 수 있도록 하며, 결과를 기록하여 분석한 후, 이를 평가하여 지속적인 개선 활동을 수행한다.	신청사업자의 개인정보보호 정책과 목적을 충족시키기 위해 개인정보보호와 관련된 법적 요건 및 환경변화 등의 목적과의 일치성을 만족시키기 위하여 지속적인 모니터링 시행하고 있는가?	개인정보보호관리체계는 지속적으로 모니터링되어 법적 요건 및 개인정보보호정책과 조적의 일치성을 만족시켜야 한다.	필수	
		5.1.2 개인정보 보호관리체계의 재검토	신청기관의 목표, 기술 등 내·외부의 변화와 내부감사 결과, 보안사고 등을 고려하여, 개인정보보호관리체계의 효율성, 범위의 적절성, 잔류위험의 수준, 절차 등의 문서를 공식적이고 정기적으로 재검토하여야 한다.	모니터링 결과에 따른 교정 및 사전 대책이 마련되어 구형되었으며, 그 결과가 평가되고 있는가?	교정 및 사전 대책이 구현되어야 하며 그 결과가 평가되어야 지속적인 개선활동이 이루어질 수 있다.	필수	
				공식적이고 정기적인 개인정보보호관리체계의 재검토를 위한 절차 또는 규정이 존재하는가?	조직의 업무, 개인정보시스템, 법/제도 등의 대내외적 환경 변화와 내부 이행점검 및 모니터링, 보안사고 결과 등을 반영하여 개인정보보호관리체계를 공식적이고 정기적으로 재검토하여야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	관련 근거
				개인정보관리체계의 제 개인정보의 효율성, 정확성, 건전성이 조기에 미치는 영향 범위의 적절성, 수준 등을 고려하여 다음의 내용을 고려 보안사고의 영향 등을 반영할 하고 있는가? - 개인정보의 내용 및 흐름 계 재검토 절차가 수립되어야 - 적용 기술상의 내 외부의 변화 - 내부이행점검 결과 - 모니터링 결과	개인정보보호 관련 대내외의 환경 변화가 조기에 미치는 영향 분석하고, 이행점검 결과, 보안사고의 영향 등을 반영할 수 있는 개인정보관리체	필수	

개인정보보호대책 요구사항

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
1. 개인정보 보호정책	1.1 개인정보 보호정책은 최고경영자의 승인을 득하고 접근용이한 형태로 공표되어야 한다.	1.1.1 정책의 승인	문서화된 개인정보 보호정책은 최고경영자의 승인을 받아야 한다.	개인정보보호정책이 최고경영자의 검토를 거쳐 승인되었는가?	개인정보의 적법한 수집과 이용, 안전한 관리 등에 대한 최종 책임은 최고경영자에게 있으므로, 정책의 내용은 최고경영자의 검토를 거쳐 최고경영진 또는 그로부터 권한을 위임받은 자에 의해 승인되어야 한다.	필수	
		1.1.2 정책의 공표	개인정보 보호정책은 이용자, 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.	개인정보보호정책은 조직 내 모든 임직원 및 관련자를 통해 이용자에게 공표되어야 하는가? 개인정보취급 부서장들의 검토를 거쳐 동의할 것인가?	정책의 내용은 이를 실행하여야 할 책임이 있는 관련 부서장들의 검토를 거쳐 동의를 얻어야 한다.	필수	
		1.1.2 정책의 공표	개인정보 보호정책은 이용자, 임직원 및 관련자에게 이해하기 쉬운 형태로 전달하여야 한다.	개인정보보호정책은 조직 내 모든 임직원 및 관련자를 통해 이용자에게 공표되어야 하는가? 개인정보취급 부서장들의 검토를 거쳐 동의할 것인가?	정책의 내용은 이를 실행하여야 할 책임이 있는 관련 부서장들의 검토를 거쳐 동의를 얻어야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부	
1.2	개인정보보호정책은 개인정보관리체계를 체계적으로 수립할 수 있도록 구성되어야 한다.	1.2.1	지침, 절차 및 표준 수립	개인정보보호정책을 시행하기 위한 지침, 절차 및 표준을 수립하여야 한다.	개인정보보호정책 하위 관련자에 대해 필요한 문서가 적절하게 배포되고, 배포 대상자는 이를 이해하고 있는가?	개인정보보호정책 및 이를 실행하기 위한 지침, 절차 표준 등의 관련문서는 알 필요 및 할 필요에 근거하여 용이하게 참조할 수 있도록 필요한 형태(소책자, 전자문서 등) 개발되어 적절한 관련자에게 배포되어야 하고, 대상자는 이를 이해하고 있어야 한다.	필수	
			1.2.2	정책 간의 일관성	개인정보보호정책을 시행하기 위한 지침, 절차 및 표준은 체계적으로 구성되어 있으며, 관련	개인정보보호정책을 구체적으로 시행하기 위한 지침, 절차 및 표준은 체계적으로 구성되어 있는가?	정책의 내용을 구현하기 위해서는 모범적 실무사례나 접근방법을 제시하는 지침이나 구체적 기술, 방법론, 구현 절차 등을 정의한 표준과 특정 활동 수행에 필요한 구체적이며 단계적인 절차 등이 개발되어야 한다.	필수

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
			정책 간의 일관성이 유지되어야 한다.	개인정보보호정책은 정책 간 일관성을 유지하고 있는가?	개인정보보호정책은 관련 정책 간 일관성을 유지하여야 한다.	필수	
1.3	개인정보보호 정책의 주기적인 타당성을 검토하고, 최신분으로 유지 및 관리하여야 한다.	정책의 주기 검토 검토	정기적으로 개인정보 보호정책의 타당성을 검토하여야 하며, 중요한 개인정보 사고 발생, 새로운 위협 또는 취약성의 발생, 기업환경의 중대한 변화 등이 발생했을 경우에는 관련된 사항의 타당성을 추가로 검토하여야 한다.	정기적으로 정책의 타당성을 검토하는 절차가 정의되고 있는가?	정기적으로 정책의 타당성을 검토하여 필요시 수정 보완하는 절차가 마련되어 있어야 된다.	필수	
				다음의 경우가 발생했을 시에는 개인정보보호정책과 관련된 사항의 타당성을 추가로 검토하는가? - 관련 법,규제상의 변화 - 기업의 비즈니스 환경에 대한 중대한 변화 - 중대한 보안사고 발생 - 새로운 위협 또는 취약성의 발생 등	중대한 보안사고 발생, 새로운 취약성의 발생, 개인정보보호 환경에 중대한 변화 등이 발생했을 경우에는 관련된 사항의 타당성을 추가로 검토하여야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		1.3.2	개인정보보호정책과 정책 시행을 위한 관련 문서를 마련하고, 주기적으로 검토하여 최신본으로 유지하여야 한다.	개인정보보호정책과 시행을 위한 관련 문서를 마련하고, 주기적으로 검토하여 최신본으로 유지하여야 한다.	준수해야 할 문서의 전체 목적이 확인되기 어려우면 관련된 문서에서 규정된 사항을 준수할 수 없다. 또한 최신본을 확인하지 못하면 변경 사항에 대한 준수를 보장할 수 없다.	필수	
				개인정보보호정책과 시행을 위한 관련 문서의 변경, 개정상태 식별, 배포, 폐기 등의 절차가 마련되어 있는가?	적절한 문서관리 절차가 마련되어 있어야지만 직원들이 자신에게 관련된 사항을 명시한 문서를 확인할 수 있고 변경 사항을 즉시 인지하여 준수하도록 보장할 수 있다.	필수	
2. 개인정보 보호조직	2.1 개인정보보호 조직체계를 구성하여 개인정보 관리 책임자 및 개인정보 취급부서별 책임자, 담당자를 지정하여야 한다.	2.1.1 개인정보 보호 조직 체계 구성	개인정보보호 업무를 체계적으로 이행하기 위한 내부조직 체계 위함 내부조직체계가 구축되어 있어야 한다.	조직 내 개인정보보호 업무를 수행하기 위한 내부조직 체계가 구축되어 있는가?	개인정보보호활동에 대한 경영층의 명확한 지원 및 방향 제시를 보증할 수 있는 조직을 구성하여야 한다. 또한 개인정보보호관리 활동을 수행하고 검증하는 인력들에 대한 책임, 권한 및 상호 연관 관계를 정의하고 문서화하여야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		2.1.2 개인정보 관리책임자(CPO) 지정	이용자의 개인정보 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보관리책임자를 지정하여야 한다.	이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보관리책임자가 지정되었는가?	조직의 개인정보를 책임지고, 이용자의 개인정보 보호 고충처리를 담당하는 개인정보 관리책임자를 지정하여야 한다. 상시 종업원 수가 5명 미만인 정보통신서비스 제공자들의 경우에는 지정하지 않을 수 있다. 이 경우에는 그 시업주 또는 대표자가 개인정보관리책임자가 된다. (인터넷으로 정보통신서비스를 제공하는 것을 주된 업으로 하는 정보통신서비스 제공자들의 경우에는 상시 종업원 수가 5명 미만으로서 전년도 말 기준으로 직전 3개월간의 일일평균이 용자가 1천명 이하인 자를 말함)	필수	○
				개인정보관리책임자의 자격 요건을 정하여 이에 적합한 자를 지정하고 있는가?	개인정보관리 활동을 계획, 관리하는 개인정보관리책임자는 충분한 권한을 가진 임원급 또는 개인정보와 관련하여 이용자의 고충처리를 처리할 수 있는 부서장이거나만 의사 결정에 따른 시행이 이루어질 수 있다.	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		2.1.3 개인정보취급부서별 책임자 및 담당자 지정	개인정보취급부서의 개인정보보호 관련 업무 및 범규정 준수 여부를 감독하고 관리할 책임자 및 담당자가 지정되어 있어야 한다.	개인정보취급부서별 책임자를 지정하고 담당자를 지정하는가?	개인정보취급부서의 업무가 법 규정 및 조직의 정책을 준수하도록 할 책임은 해당 부서에게 있다. 또한 취급부서별로 개인정보보호 업무를 수행할 관리자 수준의 담당자가 지정되어야 원활한 시행을 기대할 수 있다. * 개인정보취급부서가 존재할 경우 개인정보보호책임자 및 관리자가 전 사업부서의 개인정보취급자를 관리할 수 있다. 그러나 개인정보취급부서가 존재하지 않고, 개인정보취급부서의 관리가 자체적으로 이루어져야 한다면 개인정보취급부서별 책임자 및 담당자의 역할/책임이 중요하다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
2.2	개인정보 관련 책임자, 담당자에 대한 역할 및 책임을 정의하고, 상호 의사소통할 수 있는 보고 체계를 수립하여야 한다.	역할 및 책임 2.2.1	개인정보관리책임자 및 개인정보를 취급하는 담당자에게는 다양한 부서에서의 역할 및 책임이 정의되어야 한다.	개인정보관리책임자 시 최고경영자가 승인하였는가? 개인정보관리책임자의 개인 정보보호에 관한 역할 및 책임이 정의되었는가?	개인정보관리책임자 지정 시 최고경영자가 승인하여야 한다. 일반적으로 조직내 역할과 책임을 통해 개인정보관리책임자가 지정되고 있으므로, 인사/조직 변경도 경영진의 승인으로 간주할 수 있다. 개인정보관리 책임자의 역할 및 책임이 문서로 정의되어 승인되어야 하며, 다음과 같은 사항을 포함하여야 한다. - 개인정보보호 활동의 총괄 - 개인정보영향평가 총괄 - 개인정보보호 계획의 수립 총괄 - 관련 부서의 법적 요건 만족의 모니터링 - 개인정보 침해행위 예방 및 점검 활동 감독 - 정보주체의 개인정보 관련 요청 등 민원의 처리 및 감독 - 임직원, 개인정보 취급자, 수탁업체, 협력 업체에 대한 교육 등	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				<p>개인정보 취급부서의 책임이 명시되고 개인정보 취급 부서별 책임자 및 관리 담당자의 역할 및 책임을 정의하였는가?</p>	<p>- 이러한 행위를 수행하기 위해 필요한 소집, 감독, 감사, 결정 등의 역할</p> <p>개인정보에 관련된 모든 사항들이 자신의 책임을 인식하고 문제 발생시 책임을 지게 할 수 있도록 취급 부서장, 담당자, 취급자의 책임이 정의되어야 한다.</p> <p>* 개인정보취급부서가 존재할 경우 개인정보보호책임자 및 관리자가 전 사업부서의 개인정보취급자를 관리할 수 있다. 그러나 개인정보취급부서가 존재하지 않고, 개인정보취급부서의 관리가 자체적으로 이루어져야 한다면 개인정보취급부서별 책임자 및 담당자의 역할/책임이 중요하다.</p>		

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				개인정보취급자의 개인정보 보호에 관한 역할과 책임 및 권한이 정의되었는가?	개인정보취급자의 역할 및 책임이 문서로 정의되어 승인되어야 하며, 다음과 같은 사항을 포함하여야 한다. - 개인정보보호 활동 참여 - 내부관리계획의 준수 및 이행 - 개인정보의 기술적·관리적 보호조치 기준 이행 - 소속 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검 등	필수	○
		보고 및 의사소통 체계	개인정보관리책임자 및 개인정보를 취급하는 다양한 부서와 담당자가 상호 의사소통할 수 있는 보고라인, 방법 및 절차가 정의되어 있어야 한다.	개인정보관리책임자와 부서별 책임자 및 담당자와 의사소통할 수 있는 보고라인, 방법 및 역할과 책임이 정의되어 있는가?	모든 개인정보 취급 부서에 상관성 있게 개인정보 보호를 수행하기 위하여 보고 및 의사소통 체계와 각자의 역할과 책임이 정의되어 있어야 한다.	필수	
		2.2.2					

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
3. 개인정보 분류	3.1 개인정보 취급 차별하고, 자산 별 중요도를 결정하여 책임 소재를 명확히 하여야 한다.	3.1.1 개인정보 조사	신청사업자의 개인정보 및 개인정보 관리 조사를 조사하고 개인 정보 및 개인정보 관리 자산별로 신청기관에서의 가치, 업무 영향, 법적 준수사항 등을 고려하여 중요도를 결정하여야 한다.	식별된 개인정보 및 개인정보 관리 자산에 대해 법적 준수사항이나 업무에 미치는 영향 등을 고려하여 중요도를 결정하였는가?	식별된 개인정보 및 개인정보 관리 자산의 가치를 결정하여 보호 우선순위를 부여함으로써 보다 효과적인 개인정보보호대책을 수립할 수 있다.	필수	
		3.1.2 개인정보 및 개인 정보 관리 자산 별 책임 할당	조사된 개인정보 및 개인정보 관리 자산에 대하여 소유자, 관리자, 사용자, 신청자를 확인하고, 적절한 통제 조치를 위해 책임 소재를 명확히 하여야 한다.	중요한 개인정보 및 개인정보 관리 자산에 대한 소유자, 관리자, 사용자, 신청자를 확인하고 지속적인 관리 및 통제에 대한 책임소재가 명시되어 있는가? 개인정보 및 개인정보 관리 자산의 유형, 가치, 소유자, 관리자, 사용자 등이 명시된 목록이 유지관리될 수 있는 절차가 존재하여 지속적으로 관리되어야 한다.	개인정보 및 개인정보 관리 자산에 대한 책임소재가 분자 명하게 식별되지 않으면 자리에 대한 관리가 이루어질 수 없다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
3.2	신청기관 의 현황에 맞는 개인정보의 분류방식을 선택하여 개인정보 흐름도를 작성하고, 주기적인 검토를 통해 최신본으로 유지하여야 한다.	개인정보 흐름 분석	분류 및 식별된 개인정보의 수집, 이용 및 제공, 저장 및 관리, 파기 등 취급상의 개인정보 흐름을 파악하여야 한다. 또한, 개인정보 흐름도는 주기적으로 검토되어 취급상의 변화를 반영하여 작성성 하여야 한다.	분류 및 식별된 개인정보에 대하여 수집, 이용 및 제공, 저장 및 관리, 파기 등 취급상의 개인정보 흐름을 분석하였는가?	분류 및 식별된 개인정보의 수집 경로, 관련 시스템 및 연결된 인터페이스 등을 파악하고, 이를 통한 수집, 이용 및 제공, 저장 및 관리, 파기의 흐름을 분석하여 흐름도를 작성하여야 한다. 이를 통해 개인정보의 취급 단계별 위험요인 및 취약성이 분석되고, 관리될 수 있도록 하여야 한다.	필수	
		3.2.1	개인정보 흐름 분석	개인정보 취급 상의 흐름을 분석하여 개인정보 및 관련자에 의해 주기적으로 검토되어야 하며, 검토 결과 관련 업무 및 환경, 개인정보를 재작성 되어야 한다.	개인정보 취급 상의 흐름을 분석하여 개인정보 및 관련자에 의해 주기적으로 검토되어야 하며, 검토 결과 관련 업무 및 환경, 개인정보를 재작성 되어야 한다. 반영해 재작성하고 있는가?	개인정보 흐름도는 담당자 및 관련자에 의해 주기적으로 검토되어야 하며, 검토 결과 관련 업무 및 환경, 개인정보를 재작성 되어야 한다.	필수
		3.2.2	개인정보 및 개인정보 관리에 대하여 보안등급을 부여하고, 보안등급 표시를 부착하여 관리하여야 한다.	분류 및 식별된 개인정보 및 개인정보 관리 자산에 보안등급이 부여되어 있는가? 보안등급 표시하고 있는가? 보안등급 표시를 부착하여 관리하여야 한다.	분류 및 식별된 개인정보 및 개인정보 관리 자산에 대한 보안등급 선정기준에 근거하여 부여하고, 인지도록 보안등급 표시를 부착하여야 한다.	선택	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
4. 교육 및 훈련	4.1			보안등급의 부여에 따른 취급절차가 정의되어 이행하고 있는가? 다. 또한 보안등급의 부여에 따라 취급절차를 정의하여 이행하여야 한다.	보안등급에 따라 취급절차와 요령이 정의되어야 하며, 이를 준수할 수 있도록 접근통제 기능이 수립되어야 한다.	선택	
	4.1.1	교육 및 훈련 대상에 대한 신원확인, 개인정보취급자, 개인정보처리담당자 모두를 포함하여야 한다.	교육 및 훈련 대상은 개인 정보관리책임자(CPO), 개인 정보취급자 및 관리 담당자 등을 포함하고 있는가?	교육 및 훈련 대상은 개인 정보관리책임자(CPO), 개인 정보취급자, 개인정보취급부서 책임자 및 관리 담당자 등을 대상으로 한다. 따라서, 개인정보책임자(CPO)와 개인정보관리자에 대한 차별화된 교육이 별도로 존재하는지 확인하여야 한다.	필수	필수	○
				조직이 보유한 개인정보를 공유, 제공 받거나 접근 권한을 부여받은 외부 직원에 대한 교육훈련을 제공 하는가?	수탁자나 제3자 등 개인정보를 공유, 제공, 접근할 수 있는 모든 인력이 개인정보보호에 대한 의무사항을 인식할 수 있도록 보장하여야 한다.	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		교육 및 훈련내용	교육내용은 개인정보 보호 관련 법률 및 제도, 관리적 기술적 조치 및 이를 수행하기 위한 방법, 사내 규정 등 개인정보취급자가 필수적으로 알아야 하는 사항을 포함하여야 한다.	교육내용은 개인정보보호 교육내용은 관련 법률,규제,사내규정, 보호 조치 방법 등을 포함해야 하며, 특히 개인정보취급자가 이용자의 개인정보를 유출할 경우에는 증벌에 처해진다 사실을 주지시키는 것은 개인정보보호책임자의 의무이므로 이러한 사항을 교육 내용에 포함해야 한다	개인정보보호 교육내용은 개인정보보호 교육내용은 관련 법률,규제,사내규정, 보호 조치 방법 등을 포함해야 하며, 특히 개인정보취급자가 이용자의 개인정보를 유출할 경우에는 증벌에 처해진다 사실을 주지시키는 것은 개인정보보호책임자의 의무이므로 이러한 사항을 교육 내용에 포함해야 한다	필수	○
		4.1.2	교육 및 훈련내용	개인정보보호 교육시 교육 대상자의 직위 및 담당하는 업무의 특성에 따라 교육 내용을 차별화하여 적합한 교육을 실시하고 있는가?	관련자는 전반적인 개인정보 보호 요구사항 및 중요성, 관련 법규 및 개인의 보안책임에 관한 교육을 받아야 한다. -임원 및 관리자는 일반 직원과 별도로 관리책임에 관한 교육을 받아야 한다. -IT 부서원은 일반 직원과 별도로 업무 수행에 필요한 보안 기술 교육 훈련을 받아야 한다. -개인정보취급자는 업무수행에 필요한 개인정보보호 교육 훈련을 받아야 한다.	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	범위 근거 여부
4.2	교육 및 훈련은 정기적으로 실시하여야 하며, 교육 및 훈련 종료 후 검토를 통하여 차기 교육에 반영하여야 한다.	교육 및 훈련 수행	교육 및 훈련은 정기적으로 실시하여야 하며, 개인정보보호정책의 절차 및 역할 변경이 있는 경우에는 정기적인 교육에 내용을 포함하고 이에 대한 기록을 유지한다.	교육 및 훈련이 계획에 따라 년2회 이상 시행되고, 이 시행되어야 하고, 이를 기록하여 유지하며, 실제 시행 내역은 계획과 일치하여야 한다. - 교육계획에는 다음사항을 포함하여야 한다. 1. 교육목적 및 대상 2. 교육 내용 3. 교육 일정 및 방법	수립된 개인정보보호 교육 및 훈련 계획이 년 2회 이상 시행되어야 하고, 이를 기록하여 유지하며, 실제 시행 내역은 계획과 일치하여야 한다. - 교육계획에는 다음사항을 포함하여야 한다. 1. 교육목적 및 대상 2. 교육 내용 3. 교육 일정 및 방법	필수	0
		교육 및 훈련 종료 후 평가	교육 및 훈련 종료 후 평가 결과를 통하여 차기 교육에 반영하여야 한다.	교육 및 훈련은 개인정보보호정책이나 절차, 새로운 대책 수립, 역할 변경 등 경이 있는 경우에 실시하고, 이에 대한 기록을 유지하는가? 교육 및 훈련의 효과를 측정, 개선하기 위한 평가기준에 따라 결과를 측정하고, 측정된 결과를 분석하여 개선사항을 차기 계획에 반영하여야 한다.	정정보호정책이나 절차, 새로운 대책 수립, 역할 변경 등 경이 있는 경우 변경된 사항에 대해 관련자들이 변경된 결과를 숙지할 수 있도록 변경이 있을 경우 교육을 시행하고, 기록하여 유지하여야 한다.	필수	
		4.2.2	교육 및 훈련 종료 후 평가	교육 및 훈련의 효과를 측정, 개선하기 위한 평가기준에 따라 결과를 측정하고, 측정된 결과를 분석하여 개선사항을 차기 계획에 반영하여야 한다.	교육 및 훈련은 개인정보보호정책이나 절차, 새로운 대책 수립, 역할 변경 등 경이 있는 경우에 실시하고, 이에 대한 기록을 유지하는가? 교육 및 훈련의 효과를 측정, 개선하기 위한 평가기준에 따라 결과를 측정하고, 측정된 결과를 분석하여 개선사항을 차기 계획에 반영하여야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
5. 인적보안	5.1 개인정보취급자는 최소한으로 제한하고 개인정보 취급자 명단 관리 및 책임 명시, 처벌규정을 마련하여야 한다.	5.1.1 개인정보 취급자 감독	업무상 개인정보를 취급해야 하는 개인정보 취급자는 최소한으로 제한하고 개인정보 취급자 명단 관리 및 통제방안을 마련하여야 한다.	업무상 개인정보를 취급해야 하는 사람들을 최소한으로 제한하고 있는가? 개인정보 취급자 명단을 관리하고 있는가? 개인정보취급자의 업무 수행 시 적격심사를 진행하고 있는가?	개인정보처리시스템에 대한 접근권한은 개인정보관리책임자, 개인정보취급자를 대상으로 최소한으로 부여하여야 한다. 개인정보를 취급해야 하는 사람들을 개인정보 취급자로 정의하고 명단을 관리하여야 한다. 계약직 및 임시직원은 물론 정직원도 개인정보 취급 관련 업무를 수행 시 신분, 업무능력, 교육정도, 경력 등에 대한 적격심사가 이루어져야 한다.	필수	0
				개인정보취급자가 다수일 경우, 개인정보를 관리할 수 있는 부서별 책임자 및 담당자 및 담당자를 지정하고 감독, 일일 작업 기록 검토, 적절한 관리·감독 방안을 마련하는가?	개인정보취급자가 다수일 경우, 개인정보취급자 및 담당자를 지정하고 작업장 내 업무 감독, 일일 작업 기록 검토, 작업 시간 작업 기록 검토, 작업 사전 승인 등의 적절한 관리·감독 방안을 마련하여야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		5.1.2	인사규정 등에 임직원 및 개인정보취급자에 대한 회사내규상 책임 및 관련 법규상의 책임을 명시하여야 한다. 또한 책임을 이행하지 않는 경우를 대비한 적절한 처벌규정을 포함하여야 한다.	인사규정 또는 채용계약서 등에 개인정보취급자가 무상 취득한 개인정보를 훼손·침해 또는 누설하는 경우 관계법령상의 책임 및 처벌 규정에 대해 명시하고 있는가? 개인정보취급자의 퇴직 및 직무변동으로 인해 직무변동 시, 인사부서와 개인정보 관련부서 간에 상호 공지가 이루어지는가?	인사규정 또는 채용계약서 등에는 개인정보취급자가 개인정보를 유출한 경우에 대한 법적책임 등 개인정보에 대한 임직원 및 개인정보취급자에 대한 책임 및 처벌 규정이 포함되어야 한다.	필수	○
5.2	개인정보취급자에게 이용자의 개인정보에 대한 보호에 대한 모안서 약속을 징구하여야 한다. 임시직원이거나 제3자에게 개인정보에 대한 접근	개인정보 보호서약	개인정보취급자에게 이용자의 개인정보에 대한 보안서약을 징구하여야 한다. 임시직원이나 제3자에게 개인정보에 대한 접근 권한을 부여할 경우에도 그들로부터 개인정보 보호서약서에 서명을 받아야 하며, 직원	내부직원(정규직/계약직/임시직)의 개인정보 취급 업무 시작 시 개인정보보호에 관한 책임 및 의무를 고지한 개인정보보호서약을 징구하는가?	개인정보 취급자는 최초 개인정보 취급업무를 할당받을 때 개인정보보호서약서의 내용을 숙지하고 서명하여야 한다. 만약, 보안서약서에 개인정보 보호에 대한 책임 및 법적 처벌규정이 명시되었을 경우 보안서약서로 대체 가능하다.	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
	근권한을 부여할 경우에도 그들로부터 개인정보 보호 서약서에 서명을 받아야 하며, 직원의 고용계약에 변경이 있을 경우, 특히 퇴사 또는 계약기간 만료 시 개인정보 보호 서약서를 환기시켜야 한다.		의 고용계약에 변경이 있을 경우, 특히 퇴사 또는 계약기간 만료 시 개인정보 보호 서약서를 환기시켜야 한다.	제3자 등 외부 인원에게 접근권한을 부여하는 경우 개인정보 보호에 관련된 사항이 계약서에 포함되어 있으며, 개인 정보를 취급하는 인원에 대해서는 개인정보 보호 서약을 받는가?	제3자 등 외부 인원이 조직 내부의 개인정보처리시스템을 접근하는 일을 수행할 경우, 개인정보 보호에 관련된 사항을 계약서에 반영하여야 하며, 접근자에 대해 개인정보 보호 서약서에 서명을 받아야 한다.	필수	○
	근권한을 부여할 경우에도 그들로부터 개인정보 보호 서약서에 서명을 받아야 하며, 직원의 고용계약에 변경이 있을 경우, 특히 퇴사 또는 계약기간 만료 시 개인정보 보호 서약서를 환기시켜야 한다.		의 고용계약에 변경이 있을 경우, 특히 퇴사 또는 계약기간 만료 시 개인정보 보호 서약서를 환기시켜야 한다.	제3자 등 외부 인원에게 접근권한을 부여하는 경우 개인정보 보호에 관련된 사항이 계약서에 포함되어 있으며, 개인 정보를 취급하는 인원에 대해서는 개인정보 보호 서약을 받는가?	제3자 등 외부 인원이 조직 내부의 개인정보처리시스템을 접근하는 일을 수행할 경우, 개인정보 보호에 관련된 사항을 계약서에 반영하여야 하며, 접근자에 대해 개인정보 보호 서약서에 서명을 받아야 한다.	필수	
	근권한을 부여할 경우에도 그들로부터 개인정보 보호 서약서에 서명을 받아야 하며, 직원의 고용계약에 변경이 있을 경우, 특히 퇴사 또는 계약기간 만료 시 개인정보 보호 서약서를 환기시켜야 한다.		의 고용계약에 변경이 있을 경우, 특히 퇴사 또는 계약기간 만료 시 개인정보 보호 서약서를 환기시켜야 한다.	제3자 등 외부 인원에게 접근권한을 부여하는 경우 개인정보 보호에 관련된 사항이 계약서에 포함되어 있으며, 개인 정보를 취급하는 인원에 대해서는 개인정보 보호 서약을 받는가?	제3자 등 외부 인원이 조직 내부의 개인정보처리시스템을 접근하는 일을 수행할 경우, 개인정보 보호에 관련된 사항을 계약서에 반영하여야 하며, 접근자에 대해 개인정보 보호 서약서에 서명을 받아야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
6. 침해사고 대 처리 및 대 응절차	6.1 신청사업자는 실효성 있는 개인정보 사고 대응 계획을 수립·시행하 여야 한다.	6.1.1 침해사고 대응 계획 수립	개인정보의 노출, 변 경, 삭제에 대응하기 위한 긴급 연락체계, 개인정보보호 사고 발 생 시 보고 및 대응 조 절차, 사고 대응 조 의 구성, 교육 계획 등을 포함한 개인정 사고 대응 계획을 수 립·시행하여야 한다.	개인정보사고대응계획이 립되어 있고 대응계획은 관련 활동이 명확히 기 술되어 있는 등 필요한 용이 충분히 반영되어 개인정보 사고의 유형 중요도에 따라 분류되 고 이에 따른 보고라인 이 정의되어 있는가?	개인정보사고의 정의 및 범위, 긴급연락체계 구축, 개인정보사 고 발생 시 보고 및 대응 절차, 사고 대응조직의 구성, 교육계 획 등을 포함한 개인정보사 고 대응 계획을 수립하여야 한다. 개인정보 사고는 사고의 유형 또 는 중요도를 분류하여 개인정 보 관리자 또는 개인정보책임 자의 의사결정 절차를 보고라인으로 간주할 수 있다. 보고라인이 정 의된 문서가 존재하지 않을 경우 개인정보책임자 및 관리자의 역 할과 책임을 확인할 수 있다.	필수	
		6.1.2 침해사고 대응 체계 구축	개인정보사고의 대 응 신속하게 이루어질 수 있도록 중앙 집중 적인 대응체계를 구 축하고, 대응체계에는 내부직원뿐 아니라 외 부기관 및 전문가들과 의 협조체계를 반영하 여야 한다.	개인정보 침해사고를 모 니터링 하고 대응할 수 있는 대응체계를 구축 하고 대응체계를 모 니터링 및 대응 방법 은 모니터링 및 대응 절차, 보고 및 승인 필요 내용을 모두 포 함하고 있는가?	개인정보사고를 효과적으로 모니터링하고 대응하기 위해 서는 중앙집중적인 대응체 계가 구축되어야 한다. - 모니터링 및 대응 방법 - 대응 조직 및 인력 - 모니터링 및 대응 절차 - 모니터링 및 대응 보고 및 승인 방법	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				외부관계 시스템 등 외부 개인정보 관리 활용을 통해서 개인정보 사고를 모니터링하고 대응하는 체계를 구축 운영하는 경우, 이에 대한 세부 사항이 계약서 및 계획서에 반영되어 있는가?	대응체계를 외부 전문 업체와 협력하여 수립하고 구축하는 경우, 대응체계와 관련된 세부 항목들이 계약서 및 계획서에 반영되어야 한다.	필수	
				개인정보 사고 대응 절차는 개인정보 훼손 및 법률관련 부서와의 협력을 포함하고 있는가?	개인정보 사고는 이용자의 손상, 기업의 이미지 손상 및 법적 문제가 발생할 수 있으므로, 홍보 및 법률 담당 부서와의 협력이 반드시 필요하다.	필수	
				개인정보 사고의 모니터링, 대응 및 처리와 관련하여 전문가, 전문기관(KISA) 등과의 협조체계를 구축하고 있는가?	개인정보 사고의 모니터링, 대응 및 처리와 관련하여 전문가, 전문기관, 전문정부기관(KISA) 등과의 연락 및 협조를 구축해야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
6.2	개인정보사고 대응 계획, 절차 및 방법에 대하여 정기적으로 교육을 실시하여야 하며 개인 정보사고 대응 시 보고체계, 처리 및 복구 절차에 따라 신속히 수행하여야 한다.	6.2.1	침해사고 대응 계획, 절차 및 방법에 대하여 정기적으로 교육을 실시하여야 하며 사고 처리 후 재발 방지를 위하여 필요한 교육·훈련을 실시하여야 한다.	개인정보 사고 대응방법 및 절차에 관한 적절한 교육계획이 존재하고, 이에 따라 정기적으로 교육을 실시하고 있는가? 개인정보 사고발생 시 재발 방지를 위하여 필요한 교육·훈련을 진행하고 있는가?	개인정보 사고 대응 계획, 절차 및 방법에 대하여 정기적으로 교육을 실시하여야 한다. 사고 처리 후 재발 방지를 위하여 필요한 교육·훈련을 실시하여야 한다 - 향후 발생 가능 한 사고내용 대응방안 - 향후 재발방지 방안	선택	
		6.2.2	침해사고 보고 시 신속히 보고 가능한 한 신속히 보고하여야 한다. 시스템이나 네트워크의 보안추약점과 소프트웨어 기능장애에 또한 신속히 보고하여야 한다.보고자에 대해서는 적절한 보상이 주어질 수 있도록 하며 보고로 인해 불이익이 발생하지 않도록 해야 한다.	개인정보 사고의 징후 또는 개인 정보사고 발생을 인지한 때에는 보고체계에 따라 한 경우, 정의된 개인정보 사고보고절차에 의해 신속하게 보고가 이루어지고 있는가? 개인정보 사고의 징후 또는 개인정보 사고 발생을 인지한 경우, 신속히 개인정보 사고보고가 이루어져야 한다. 개인정보 사고의 징후로 개인 정보 문서나 파일이 부적절하게 다루어지고 있거나, 사고의 우려가 있는 보안취약점의 발견, 오남용 가능성 등을 인지하면 보고하도록 하여야 한다.	필수		

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				개인정보 사고 보고서에는 개인정보 사고 날짜, 사고 보고서가 작성되어야 하고 내용 등 필요 내용을 모두 포함하고 있는가? - 개인정보 사고날짜 - 보고자와 보고일시 - 사고내용 - 사고 대응내용 - 개인정보사고 통계 - 사고대응까지의 소요시간 등	개인정보 사고가 조직에서 규정된 중요사안에 해당 될 경우 최고경영층에 신속히 보고되고 있는가? 개인정보 사고보고시 법률이나 규정 등에 의해 관련 기관에 보고해야 할 경우 이를 준수하여야 한다.	필수	
				개인정보 사고를 보고한 자에 대해 보상이 주어져서 사고사실로 인해 불이익이 발생하지 않도록 보호하는가?	보고자에게는 포상이나 가산 점 등 적절한 보상이 주어지지 않고, 사고를 장려하도록 하여야 하며, 보고자가 이로 인해 불이익이 발생하지 않도록	필수	0

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
					보고자 신분을 알리지 않는 등 필요한 보호조치를 취해야 한다.		
		6.2.3 침해사고 처리 및 복구	개인정보사고 대응 시 절차에 따라 처리와 복구를 신속히 수행하여야 한다.	개인정보사고처리 및 복구 절차가 존재하며 복구 절차 및 방법, 책임 등 필요한 내용들을 모두 포함하고 있는가?	개인정보사고 처리 및 복구 절차는 아래와 같은 내용을 포함하고 있어야 하며, 이에 따라 사고 처리 및 복구를 신속히 수행하여야 한다. - 복구절차 및 방법 - 복구 범위 및 담당자 - 원인분석을 위한 증거자료의 수집 - 취약성의 제거 등 사후관리 - 재발방지를 위한 기타사항	필수	
				개인정보사고 발생할 경우 이루어지며 복구일시, 복구 방법 등 필요한 내용이 모두 포함되어있는가? 개인정보사고가 발생할 경우 발생부터 해결될때까지 처리 내역을 파악할 수 있도록 정리되어 있는가?	개인정보사고의 처리, 복구기여 및 복구절차 경우 처리결과는 문서화되어야 하고, 문서에는 복구일시, 복구자, 복구방법이 명시되어야 한다. 개인정보사고는 사고발생 후 처리되기까지의 각 단계를 파악할 수 있어야 하고, 해당 사고가 최종 종료되기까지 진행 경과를 추적 가능하여야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
6.3	개인정보사고 종결 후 이에 대한 분석결과 보고 및 과가 보고 및 공유되고, 재발방지 대책을 수립하여 보안 체계에 반영하여야 한다.	침해사고 분석 및 정보공유	개인정보사고가 처리되고 종결된 후 이에 대한 분석이 수행되어야 하며, 그 결과가 보고되어야 한다. 또한 사고에 대한 정보와 발견된 취약성들이 관련조직과 인력에 공유되어야 한다.	개인정보사고가 종결된 후 개인정보사고의 원인을 분석하고 있는가?	개인정보사고가 처리되고 종결된 후 이에 대한 분석이 수행되어야 하며, 그 결과가 보고되어야 한다.	필수	○
			개인정보사고로부터 얻은 정보를 활용하여, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하여야 한다. 이를 위해 필요한 경우 정책, 절차, 조직 등의 보안체계에 대한 변경도 이루어져야 한다.	개인정보사고 발생된 정보와 발견된 취약성들이 관련조직과 인력에 공유되고 있는가?	개인정보사고에 대한 정보와 발견된 취약성들이 관련조직과 인력에 공유되어야 한다.	필수	
6.3.2	침해사고 재발방지	개인정보사고로부터 얻은 정보를 활용하여, 유사 사고가 반복되지 않도록 재발방지 대책을 수립하여야 한다. 이를 위해 필요한 경우 정책, 절차, 조직 등의 보안체계에 대한 변경도 이루어져야 한다.	개인정보사고 분석을 통해 개인정보사고 발생된 정보와 발견된 취약성들이 관련조직과 인력에 공유되고 있는가?	개인정보사고 분석을 통해 얻어진 정보를 활용하여 유사 사고가 반복되지 않도록 재발방지 대책이 수립되는가?	개인정보사고 분석을 통해 얻어진 정보가 반복되지 않도록 재발방지 대책이 수립되어야 한다.	필수	
		개인정보사고에 의해 개인정보사고 대응절차, 보안대책, 절차, 조직 등의 보안체계에 대한 변경도 이루어져야 한다.	개인정보사고 발생된 정보와 발견된 취약성들이 관련조직과 인력에 공유되고 있는가?	개인정보사고 발생된 결과에 따라 필요한 조사대응절차, 보안대책, 절차, 조직 등의 보안체계에 대해 변경을 검토하는 절차가 존재하며, 필요시 이에 따라 변경이 이루어지는가?	개인정보사고 발생된 결과에 따라 필요한 조사대응절차, 보안대책, 절차, 조직 등의 보안체계에 대해 변경을 검토하는 절차가 존재하며, 필요시 이에 따라 변경이 이루어지는가?	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
7. 기술적 보호조치	7.1 접근통제 정책을 수립하고, 개인정보 취급자의 접근통제 및 모니터링을 이행하여야 한다.	7.1.1 접근통제 정책 수립	개인정보보호 요구사항에 기초하여 통합적인 접근통제 권한 부여, 개인정보 취급자에 대한 접근통제 정책을 수립하고 문서화하여야 한다.	개인정보보호 요구사항에 기초하여 개인정보처리시스템에 대한 접근통제 정책이 존재하는가?	업무 요구사항에 기초하여 논리적, 물리적, 네트워크 접근을 관리하기 위한 통합적인 접근통제 정책이 문서화 되어야 한다.	필수	
		7.1.2 접근통제 정책 수립	개인정보 및 개인정보처리시스템에 대한 접근통제 권한 부여, 개인정보 취급자에 대한 접근통제 정책을 수립하고 문서화하여야 한다.	개인정보 취급자 등록 및 해지 관리 절차를 마련하고 수행하고 있는가? 개인정보취급자 계정은 유익한 식별자를 가지고 식별자는 적절한 명명규칙을 따르고 있는가?	개인정보 취급자의 계정 발급 및 삭제에 관한 공적 절차가 문서화되어야 한다.	필수	
			개인정보 취급자 계정은 유익한 식별자를 가지고 식별자는 적절한 명명규칙을 따르고 있는가? 개인정보 취급자 계정 생성 및 권한부여 절차가 적절히 직무분장 되어 있으며 사용자 권한 변경의 기록을 별도로 검토하고 있는가?	개인정보 취급자 계정 생성 및 권한부여 절차가 적절히 직무분장 되어 있으며 사용자 권한 변경의 기록을 별도로 검토하고 있는가?	개인정보 취급자 계정 생성/삭제 및 권한부여가 한 사람에 의해 모두 수행되어서는 안되며 모든 사용자 권한변경이 감사기록되어 주기적으로 별도 인력에 의해 검토되어야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		7.1.3	개인정보취급자의 접근 권한이 서비스 제공을 위하여 필요한 최소한의 인원에게만 부여하고 그 내역을 기록 관리하여야 한다.	개인정보처리시스템에 접근 권한을 서비스 제공을 위하여 필요한 최소한의 인원에게 부여하고 있는가? 개인정보취급자의 업무 내용에 따라 접근 권한을 제한하고 있는가?	개인정보취급자 외에는 개인 정보처리시스템에 접근 권한을 부여하지 않아야 한다.	필수	○
		7.1.4	이용자 패스워드의 관리 절차를 수립하고 이행하여야 한다.	개인정보처리시스템에 접근한 부여 현황, 변경 또는 말소 내역 등을 기록하고 최소 5년 이상 보관하는가?	개인정보처리시스템에 대한 권한 부여, 변경 또는 말소 내역 등을 기록하고, 그 기록을 최소 5년간 보관하여야 한다.	필수	○
		7.1.4	이용자 패스워드의 관리 절차를 수립하고 이행하여야 한다.	다음 사항을 포함하는 이용자 패스워드 관리절차가 존재하고, 이에 따라 이행되고 있는가? - 안전한 패스워드 사용기준 - 초기 패스워드 할당 후의 변경 - 패스워드의 암호화 - 패스워드의 재발급 등	다음 사항을 포함하는 이용자 패스워드 관리절차를 이행하여야 한다. 1. 이용자가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자를 패스워드로 사용하지 않도록 패스워드 작성규칙을 수립, 적용하고 주기적으로 변경되어야 한다.	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	범위 근거 여부
					2. 관리자가 활동한 사용자의 초기 패스워드는 사용자 로 그인 즉시 변경하도록 하여 야 한다. 3. 패스워드는 적절히 암호화 되도록 한다. 4. 패스워드 재발급시 안전한 채널을 통한 신원확인 절차 가 있어야 한다.		
		개인 정보 취급자의 접근 권한 검토	개인정보 및 개인정보 처리시스템에 대한 접근 권한을 관리하기 위해서 정기적으로 접근 권한에 대하여서 점검을 하여야 한다.	개인정보 취급자 접근 권한에 대해 정기적으로 검토가 이루어지고 있는가? 정보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하는가? 개인정보 취급자 접근 권한에 대한 정기적 점검 시, 담당자 다음사항이 포함되어 있는가?	개인정보담당자는 개인정보 취급자의 접근 권한을 주기적으로 검토하여 재승인하여야 한다. 정보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.	필수	
		7.1.5				필수	0

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				<ul style="list-style-type: none"> - 문서상으로 인가된 자만 접근 허용 - 장기간 비사용 계정의 처리 - 임직원의 퇴직 및 부서이동 등의 인사처리 시 접근 권한 변경 등 	<p>에 대한 확인 및 삭제 등의 조치 여부, 퇴직 및 부서이동 등의 인사처리 시 계정관리 담당자에게 문서를 통지하고, 계정의 삭제 또는 권한 변경이 이루어지는지의 여부 등을 확인하여야 한다.</p>		
		7.1.6 개인정보 취급자의 책임	개인정보처리시스템 및 패스워드 관리 책임은 개인정보 취급자 자신에게 있음을 주시시키고 관리지침을 제공하여야 한다.	<p>개인정보처리시스템 및 패스워드 관리 책임은 개인정보 취급자 자신에게 있음을 주시시키고 있는가?</p> <p>개인정보처리시스템 및 패스워드 관리지침을 제공하고 있는가?</p>	<p>개인정보 취급자는 자신의 개인정보처리시스템과 패스워드 관리 책임이 자신에게 있음을 주시하여야 한다.</p> <p>개인정보취급자가 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자를 패스워드로 사용하지 않도록 개인정보 취급자 계정 및 패스워드의 안전한 관리 방법을 공지하여 숙지하도록 하여야 하며, 비밀번호 작성규칙은 다음을 포함하여야 한다</p> <ol style="list-style-type: none"> 1. 다음 각 항목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종 	필수	0

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부	
					<p>류 이상을 조합하여 최소 8 자리 이상의 길이로 구성 가. 영문 대문자(26개) 나. 영문 소문자(26개) 다. 숫자(10개) 라. 특수문자(32개) 2. 연속적인 숫자나 생일, 전화 번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고 3. 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경</p>			
		7.1.7	<p>비인가된 접근을 막기 위해 네트워크의 내부 연결통제, 사용자 터미널과 컴퓨터 서버가 공간에 물리적 및 논리적 경로의 통제, 사용자 인증, 고장 진단 등에 대한 접근 제 등을 포함한 네트워크 접근정책을 수립하고 이행하여야 한다.</p>	<p>다음은 포함하는 네트워크 접근정책이 수립되어 있고, 이에 따라 운영되고 있는가? - 접근통제 정책에 따라 사용자만이 네트워크에 연결할 수 있도록 함 - 사용자 터미널과 컴퓨터 서버간의 물리적 및 논리적 경로의 통제 - 접근통제 정책에 따라 인가된 사용자만이 네트워크에 연결할 수 있도록 함 - 사용자 터미널과 컴퓨터 서버간의 물리적 및 논리적 경로의 통제</p>	<p>다음은 포함하는 네트워크 접근정책이 수립되어야 한다. 1. 접근통제 정책에 따라 인가된 사용자만이 네트워크에 연결할 수 있어야 한다. 2. 사용자 단말에서 컴퓨터 서비스까지의 논리적, 물리적 접근 경로가 문서화되고 각 단계에 적절한 통제가 수립되어야 한다.</p>	필수		

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				<ul style="list-style-type: none"> - 접근통제 정책에 따른 네트워킹 라우팅 통제 - 원격 사용자의 적절한 인증 - 중요한 정보 서비스, 사용자 그룹, 시스템 그룹의 별도 분리 및 비인가자의 접근 통제 대책 마련 등 	<p>3. 접근통제 정책에 따라 네트워킹에 대한 라우팅을 제한하여야 한다.</p> <p>4. 전화 접속시에는 다이얼백 등의 별도 인증을 사용하여 비인가자의 접속을 제한하여야 한다.</p> <p>5. 사용자가 원격으로 서비스에 접근할 때는 적절한 인증을 거쳐야 한다.</p> <p>6. 고장진단 포트는 시스템 관리자 및 운영요원만이 접근할 수 있어야 한다.</p> <p>7. 중요한 정보서비스, 사용자, 시스템 그룹을 분리하여, 비인가자의 접근통제 대책을 마련하여야 한다.</p>		
				<p>외부업체에 의한 유지보수 작업 시 불법적인 네트워크 접근을 통해 개인정보가 노출되지 않도록 조치하는가?</p>	<p>외부업체에 의한 유지보수 작업 시 개인정보가 노출되지 않도록 보안조치를 취하여야 한다.</p> <p>1. 시스템 담당자 감독</p> <p>2. 작업 내역 기록 및 확인</p> <p>3. 신원보증 및 허가된 특정 인원만으로 출입통제</p>	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		7.1.8 운영체제 접근	<p>안전한 로그인 절차, 식별 및 인증관리, 필요 시 터미널 자동확인 등을 포함하여 시스템의 운영체제 접근을 통제하여야 한다.</p>	<p>다음은 포함하는 개인정보 처리시스템 운영체제 접근 통제기 존재하며, 이에 따라 이행되고 있는가?</p> <ul style="list-style-type: none"> - 개인정보처리시스템 대한 안전한 로그인 절차 - 식별 및 인증관리 	<p>개인정보처리시스템 운영체제 접근통제 정책은 다음 내용을 포함하여야 한다.</p> <ol style="list-style-type: none"> 1. 정보시스템 접근에 대한 불법접근 경고, 이전 로그인 및 시도 이력 등의 안전한 로그온 절차가 지원되어야 한다. 2. 패스워드를 사용한 기본적인 식별 인증관리가 필수적으로 지원되어야 한다. 	필수	
				<p>개인정보처리시스템의 운영체제 접근통제가 다음의 사항을 포함하며 이에 따라 운영되고 있는가?</p> <ul style="list-style-type: none"> - 터미널 자동확인 및 주요 터미널 통제 - 시스템 유틸리티 프로그램의 사용제한 - 중요 서비스의 연결시간을 업무시간 내로 제한 등 	<p>개인정보처리시스템 운영체제 접근통제 정책은 다음 내용을 포함하여야 한다.</p> <ol style="list-style-type: none"> 1. 중요 시스템 또는 중요 계정의 경우 추가적인 인증방법을 채택하여야 한다. 2. 중요한 기능을 수행하는 시스템, 사용자 권한으로의 로그인 시에는 자동 단말기 확인 기능을 통해 특정 위치의 단말기에서만 수행하도록 제한하여야 한다. 	선택	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
					3. 노출된 지역 및 주요 서비스와 연결되는 터미널은 일정 시간 사용이 없으면 연결이 종료되고 화면이 삭제되는 등의 통제가 있어야 한다. 4. 중요한 서비스에 대한 접근은 가능 시간대나 사용자별 시간 제한을 두어야 한다. 5. 설치된 시스템 유틸리티에 대한 접근의 인가 및 통제가 있어야 한다.		
		응용프로그램 접근	개인정보 취급자 접근이 허가되지 않은 응용 프로그램의 기능들에 대한 정보 제공을 제한하여야 한다. 또한 중요 정보를 처리하는 개인정보 응용 프로그램의 출력물은 허가된 위치에서만 출력되어야 한다.	정보 및 응용 프로그램 기능의 접근이 개인정보 응용 프로그램 접근통제 정책에 따라 제한되는가?	응용 프로그램 접근통제 정책에 따라 지정된 횟수의 패스워드 오류 시 아이디 차단 등 개인정보 응용 프로그램의 각 기능과 대상 정보에 대한 접근이 제한되어야 한다. 개인정보를 처리하는 응용 프로그램에서 불필요한 기능을 제거하여 권한을 우회할 수 없도록 조치하여야 하고, 우회 방법이 존재할 경우 이를 방지할 대책이 수립되어야 한다.	필수	
		7.1.9		개인정보를 처리하는 응용 프로그램에서 권한에 따른 기능 및 메뉴만 제공하고 불필요한 기능을 통제하고 있는가?		필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				중요 정보 및 응용 프로그램 출력이 등급 및 전달자를 포함하여 출력되는가?	중요 정보의 출력물에는 표지에 등급과 지정 배포처, 경고문 등이 표시되어야 하며 각 장마다 등급 및 문서번호가 표시되어야 한다.	선택	
				개인정보를 처리하는 시스템은 분리된 환경에서 수행되는가? 컴퓨팅 환경에서 수행되는가?	시스템은 전용 컴퓨터 환경에서 수행함으로써 다른 프로세스가 가용성, 기밀성, 무결성에 영향을 미치는 일이 없도록 하여야 한다.	선택	
				일정시간동안 입력이 없는 세션은 자동 차단되는가?	일정시간 동안 입력이 없는 세션은 Time-out 설정을 통해 연결차단되어야 한다.	필수	
				동일 사용자의 동시 세션 수를 제한하고 있는가?	중요한 응용 프로그램은 동일 사용자의 동시 세션 수를 제한하여 비인가된 접근을 검출할 수 있어야 한다.	필수	
		7.1.10 데이터베이스 접근	데이터베이스 레벨에서 데이터에 대한 접근 통제, 데이터사전 및 데이터베이스 유틸리티에 대한 접근 통제, 중요 정보의 암호화 등을 통해 데이터	다음의 사항을 포함하는 데이터베이스 내 개인정보보호를 위한 운영 절차가 있는가? 1. 데이터베이스 관리자 및 사용자 활동이 추적될 수 있도록 유일한 식별을 보장하여야 한다.	데이터베이스 내 개인정보 보호를 위한 다음의 운영 절차가 있어야 한다. 1. 데이터베이스 관리자 및 사용자 활동이 추적될 수 있도록 유일한 식별을 보장하여야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
	7.2 개인정보 암호화 정책 및 암호키 관리 방안을 수립하고, 이에 따라 개인정보 암호화를 시행하여야 한다.	암호정책	개인정보의 암호화를 위한 문서화된 정책을 수립하여야 한다.	<ul style="list-style-type: none"> - 데이터사전 및 유틸리티에 대한 접근통제 명시 	<ul style="list-style-type: none"> 2. 데이터베이스 접근권한은 가능한 한 상세한 수준에서 통제되어야 한다. 3. 데이터사전 및 유틸리티는 그 업무를 수행할 필요가 있는 자만이 사용할 수 있도록 제한되어야 한다. 		
	7.2.1 암호정책은 암호화 대상 및 암호화 방법은 명확하게 정의하고 있는가? 암호정책은 법적 요건을 만족하고 있는가?				<ul style="list-style-type: none"> 문서화된 암호정책이 있는가? 암호정책은 암호화 대상 및 암호화 방법은 명확하게 정의하고 있는가? 암호정책은 법적 요건을 만족하고 있는가? 	필수	
					<ul style="list-style-type: none"> 암호정책에는 암호화대상과, 암호화 방법 등을 명시하여야 한다. 암호정책은 아래와 같은 법적 요건을 만족하여야 한다. <ul style="list-style-type: none"> - 비밀번호 및 바이오정보의 일방향 암호화 저장 - 주민등록번호, 신용카드번호 및 계좌번호에 대한 안전한 알고리즘 적용을 통한 암호화 저장 - 정보통신망을 통한 이용자 개인정보 및 인증정보 송·수 	필수	0

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
			암호정책에 따라 암호 대상 개인정보의 암호화를 시행하여야 한다.	암호정책에 따라 암호화가 필요한 경우, 적절한 알고리즘과 키 길이를 결정하여 사용하고 있는가?	신시 안전한 보안서버 구축 등의 조치를 통한 암호화 - 이용자 개인정보의 개인용 컴퓨터 저장 시 암호화		
		7.2.2	암호정책에 따라 암호 대상 개인정보의 암호화를 시행하여야 한다.	암호정책에 따라 암호화가 필요한 경우, 적절한 알고리즘과 키 길이를 결정하여 사용하고 있는가? 개인정보취급자가 이용자의 개인용컴퓨터(PC)에 저장할 때 암호화하여 저장하고 있는가?	암호정책에 따라 암호화를 시행하고, 알고리즘과 적절한 키 길이로 암호화하여야 한다. 개인정보취급자가 이용자의 개인용컴퓨터(PC)에 저장할 때에는 이를 암호화하여야 한다.	필수	0
		7.2.3	암호키에 대한 관리지침, 절차 및 방법을 마련하고 필요시 복구 방안을 마련하여야 한다.	암호키에 대한 관리지침과 절차 및 방법이 마련되어 있는가? 암호키 복구 방안을 마련하여 이에 따라 복구되는가?	암호키에 대한 관리지침과 절차를 마련하여 지침, 절차, 방법을 마련하고 필요시 복구 방안을 마련하여야 한다.	필수	
				암호키 복구 방안을 마련하여 이에 따라 복구되는가?	사용자 및 관리자들이 키 관리 지침 및 절차에 따라 키를 사용, 관리, 복구하여야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
7.3	개인정보처리시스템 관련 자산 변경관리 절차를 수립하고, 네트워크 운영 보안 유지를 위해 직무 분리, 접근권한 통제, 원격접속 설비 관리, 네트워크 분리 등을 위한 책임 및 절차 등을 포함한 대책을 수립하여야 한다.	정보 관련 자산 관리	개인정보처리시스템 관련 자산을 조사하고, 모든 변경사항을 반영할 수 있는 공식적인 관리책임 및 절차를 수립하여야 한다.	개인정보처리시스템 관련 자산들(장비, 소프트웨어, 드웨어 및 문서)에 대한 변경 관리절차가 존재하는가?	새로운 소프트웨어의 설치, 업무프로세스, 운영환경, 새로운 연결 등의 변경들은 업무에 상당한 영향을 미칠수 있으므로 변경사항들은 정적인 승인절차에 따라 이루어져야 한다.	필수	
		7.3.1		개인정보처리시스템과 관련된 자산에 대하여 보안시스템의 변경이 이루어지기 전에 이에 미치는 영향을 파악하기 위한 분석이 수행되고 있는가?	변경을 수행하기 전 변경사항이 보안, 성능, 업무 등에 미치는 영향을 분석하여야 한다.	필수	
				성공적이지 않은 변경에 대해 복구하는 절차가 정의되어 있고 이에 의해 복구가가 정의 되어야 하고 이에 이루어져 있는가?	성공적이지 않은 변경에 대해 복구하는 절차를 정의하여 이를 복구하는 절차가 정의 되어야 하고 이에 따라 복구가 수행 되어야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		7.3.2 직무분리	부주의에 의한 또는 고의적인 시스템 오용의 위험을 감소시키기 위해 직무를 분리하고, 직무 분리가 어려운 특수한 경우 별도의 관리감독 대책을 수립하여야 한다.	개발자와 운영인력에 대한 책임과 직무분리가 이루어 있으며, 어려운 경우에는 보완대책이 존재하는가?	주요 업무에 대해서 한 사람에게 과도한 권한이 부여되어서는 안되며 특히, 운영과 개발 업무는 가능한 분리해야 한다. 또한, 운영인력의 책임과 직무 분리의 원칙이 정의되고 직무 기술서에 반영 되어야 한다. 직무분리 여건이 안 될 경우 모니터링을 강화하는 등의 추가적인 보완 대책이 필요하다.	필수	
		7.3.3 개발 과 운영 환경의 분리	완전히 분리된 개발, 테스트, 운영 환경을 분리하여야 한다. 또한 개인정보 응용프로그램을 개발환경으로 이진하는 절차를 정의하고 문서화하여야 한다.	개발 및 테스트 시스템이 운영시스템과 분리되어 있는가? 개발 및 운영 환경이 충분히 분리되어 있는가? 개인정보 응용프로그램을 개발환경으로 이진하는 절차를 정의하고 문서화하여야 한다.	개발 및 테스트 시스템이 운영시스템과 분리가 이루어지지 않으면 무결성과 가용성이 깨질 위험이 증대한다. 테스트가 완료된 내용들만이 변경관리 절차에 의해 운영 계로 이전되어야 한다. 운영시스템에 대한 로그온 절차와 테스트/개발 시스템에 대한 로그온 절차가 동일하다면 테스트/개발시스템의 접근자가 쉽게 운영시스템을 접근할 수 있으므로 테스트/	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
			네트워크 운영 보안 조치를 위해 직무 분리, 접근권한 통제, 원격접속 대비, 접근권한 관리, 네트워크 분리 등을 위한 책임 및 절차 등을 포함한 대책을 수립하여야 한다.	다음과 같은 내용을 포함한 네트워크 운영절차 및 보안 정책이 수립되고 이행되는가? - 네트워크 분리 - 접근권한 통제 - 책임 및 직무분리 - 원격접속설비 관리	개발시스템의 로그온절차와 운영시스템의 로그온 절차는 달라야 한다. 네트워크 운영과 보안 유지를 위해 직무 분리, 접근 권한 통제, 원격접속 설비관리, 네트워크 분리 등이 필요하며 이러한 사항들에 대한 책임 및 절차 등을 포함한 대책이 수립되어야 한다.	필수	
		7.3.4 네트워크 운영대책		네트워크를 구성하는 주요 자산에 대한 목록 및 구성도를 유지하고 있는가? 개인정보 침해위험 권리를 통해 접근통제가 이루어지도록 네트워크가 물리적 또는 논리적인 영역으로 분리되어 있는가? 외부 사용자에게 서비스를 제공하는 네트워크는 내부 업무용 네트워크와 분리되는가?	네트워크를 구성하는 자산들에 대한 목록 및 구성도가 유지되어야 한다. 핵심 업무영역의 네트워크는 개인정보 침해위험 관리를 통해 물리적 또는 논리적인 영역으로 분리되어야 한다. 외부사용자에게 서비스를 제공하는 네트워크와 내부 업무용 네트워크를 분리함으로써 상호 침투로 발생할 수 있는 위험에 대응한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				외주개발업무에 사용되는 네트워크는 내부 운영 네트워크와 분리되는가? 내부망에서 사용하는 주소는 사실 IP주소를 사용하며 내부 IP주소체계는 외부로 유출되지 않도록 하고 있는가? 내부망에서 사용하는 주소는 사실 IP주소를 사용하며 내부 IP주소체계는 외부로 유출되지 않도록 하고 있는가? 합법적인 승인 없이 네트워크 모니터링을 수행할 수 있는가? 크 모니터링을 수행할 수 있도록 되어 있는가?	외주개발 업무시 사용 네트워크를 내부 운영 네트워크와 분리함으로써 외부인력이 내부 네트워크에 불법적으로 접근하는 것을 제한한다. 내부망에서의 주소 체계는 사실 IP주소 체계를 사용하므로 외부 주소체계를 외부에 유출되지 않도록 해야 한다. 내부 조직 내 합법적인 승인 없이 네트워크 패킷 모니터링이 금지되어야 한다.	필수	
		인터넷 접속 리	개인정보취급자의 PC 및 개인정보처리시스템을 보호하기 위하여 인터넷과의 접속에 대한 통제 정책을 수립하고, 침입차단시스템 및 침입탐지시스템 등을 설치하여 보호한다.	취급 중인 개인정보 권한 없는자에게 공개되지 않도록 개인정보취급자의 PC 및 개인정보처리시스템의 설정에 대한 정책이 수립되어 있는가? 인터넷 연결시 네트워크 구성 정책 이메일, 인터넷 사이트의 접속, 메신저, P2P 등을 통한 파일 전송 제한 공유 설정 제한	취급 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되지 않도록 개인 정보처리시스템 및 개인 정보처리시스템의 PC를 설정하여야 한다.	필수	O

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				개인정보처리시스템은 침입 차단시스템에 의해 보호되는가? 침입차단시스템의 규칙은 범법 • 규정 및 기업의 개인정보 보호 정책과 지침을 준수하여야 설정 되었는가? 침입차단시스템의 보안정책을 임의로 변경하는 것을 금지하고, 침입차단시스템 정책의 변경에 대해서는 공식적인 절차를 거치는가?	개인정보처리시스템은 침입 차단시스템에 의해 보호되어야 한다. 침입차단시스템의 규칙은 범법 • 규정 및 기업의 개인정보 보호 정책과 지침을 준수하여야 한다. 침입차단시스템의 보안정책을 임의로 변경하는 것을 금지하고, 침입차단시스템 승인에 의해서 이루어져야 한다. 변경에 따른 변경요청서 및 승인결과가 문서화되어야 한다.	필수	○
				침입차단시스템을 우회한 인터넷 접속을 금지하고 있는가?	침입차단시스템을 우회하는 모뎀접속등의 우회 인터넷 접속은 금지되어야 하고 이러한 정책이 사용자들에게 공지되어야 한다.	필수	○
				침입차단시스템의 패치가 적용되고 최신으로 트되는가?	침입차단시스템에는 최신의 패치가 설치 됨으로써 과거의 버전에서 보고된 보안위험이 대응되어야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				<p>접입을 확인하기 위해 침입 차단시스템의 로그가 수집되고, 정기적으로 점검되는가?</p> <p>침입차단시스템 관리기능에 대한 접근이 강력하게 통제되고 보호되는가?</p>	<p>로그파일은 불법적인 접근 시도 여부를 확인하는 유용한 정보로 사용될 수 있으므로 침입차단시스템의 로그는 일 정기간 동안 저장되어야 하 고 정기적으로 점검 되어야 한다.</p>	필수	○
				<p>침입차단시스템 관리기능에 대한 접근이 강력하게 통제되고 보호되는가?</p>	<p>침입차단시스템의 관리기능에 권한이 없는자가 접근하 지 못하도록 접근권한과 접근방법은 강력하게 통제되고 보호 되어야 한다.</p>	필수	
				<p>개인정보처리시스템 접속 시 외부망에서의 직접접속은 차단되고, 가상사설망(VPN) 등을 통해 접근하도록 통제되는가?</p>	<p>개인정보처리시스템 외 시 외부망에서 VPN을 활용하여 외부와 은 차단되고, 가상사설망(VPN) 등을 통해 접근하도록 통제되는가?</p>	필수	○
				<p>침입기록의 자동기록, 비인가자 접속 시 자동차단, 자 동경보기능 및 분석정보제 공 기능을 보유하고 있는 침입탐지시스템을 설치 운영하고 있는가?</p>	<p>개인정보처리시스템 및 개인 정보 취급자의 PC를 보호하 기 위하여 외부의 침입을 모 니터링하고 탐지하는 침입탐 지시스템 또는 침입방지시스 템을 설치 운용해야 한다.</p>	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부	
				<p>침입탐지 기록은 수시 또는 주기적으로 검토되고 이에 따른 의심스런 사건이 처리되는가?</p> <p>네트워크를 통해서 시스템을 운영하는 경우 시스템을 관리하는 특정터미널을 통해서만 내부의 특정 터미널에서만 할 수 있도록 제한되는가?</p> <p>원격운영 관리를 위해 시스템 관리를 수행하는 경우 시스템 운영하는 경우 시스템을 관리하는 특정 터미널을 통해서만 할 수 있도록 제한하는가?</p> <p>7.3.6 원격운영 관리</p>	<p>침입탐지 기록은 수시 또는 주기적으로 검토되고 이에 따른 의심스런 사건이 처리되는가?</p> <p>네트워크를 통해서 시스템을 운영하는 경우 시스템을 관리하는 특정 터미널을 통해서만 내부의 특정 터미널에서만 할 수 있도록 제한하는가?</p> <p>원격운영 관리를 위해 시스템 관리를 수행하는 경우 시스템 운영하는 경우 시스템을 관리하는 특정 터미널을 통해서만 할 수 있도록 제한하는가?</p>	<p>침입탐지 기록은 수시 또는 주기적으로 검토 됨으로써 의심스런 침입사건을 대응해야 한다.</p> <p>네트워크를 통해 시스템을 운영하는 경우 시스템관리는 특정 터미널을 통해서만 할 수 있도록 제한한다.</p>	필수	
			<p>7.3.7 매체 취급 및 보관</p>	<p>개인정보가 유출되거나 오용으로부터 개인 정보를 보호하기 위해, 매체의 취급 및 보관에 대한 절차를 수립하고 운영하여야 하는가?</p> <p>개인정보의 중요도에 따라 테이프, 디스크, 출력물, 이동식 저장 장치 등 개인 정보 저장 매체에 대한 분류/취급/사용/보관/배출/폐기에 관한 사항이 정의되어 있는가?</p>	<p>개인정보가 유출되거나 오용으로부터 개인 정보를 보호하기 위해, 매체의 취급, 배분, 폐기 등에 대한 절차를 수립하고 운영하여야 한다.</p> <p>개인정보의 중요도에 따라 테이프, 디스크, 출력물, 이동식 저장 장치 등 개인 정보 저장 매체에 대한 분류/취급/사용/보관/배출/폐기에 관한 사항이 정의되어 있는가?</p>	필수		

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				매체에 대한 관리책임이 명 확하게 정의되어 있는가? 개인정보 저장 매체의 목록 이 작성되고 유지관리 되고 있는가? 개인정보 저장매체에 대한 라벨링이 이루어지고 있는 가? 개인정보 저장 매체의 사용 내역이 기록되어 있는가?	각 매체에 대한 관리 책임이 명확하게 정의되어 있어야 한다. 개인정보 저장 매체에 대해 매체명, 관리자, 위치 등을 포함한 목록이 작성되어야 하며 이에 대한 변경이 유지 관리되어야 한다. 개인정보 저장매체에 대해서 는 적절한 라벨링 규칙에 의 거하여 라벨링 되어야 한다. 개인정보 저장 매체에 대해 서는 복사, 대어 등의 사용기 록이 관리되어야 한다.	필수	
		매 체 의 폐 기	매체 폐기를 부주의하 게 이행하여 외부자에 게 개인정보가 누출되 지 않도록 폐기시점을 수립하고 운영하여야 한다.	개인정보 저장 매체의 폐기 시 관련 정보(일자,내용 등) 및 폐기자는 감사증적을 위 해 기록되는가? 외부계약자에 의해 매체가 폐기될 경우 폐기의 확인이 계약서에 정의되어 있고, 완 전한 폐기에 대한 확인이 이루어 지는가?	개인정보 저장 매체의 폐기 시 관련 정보(일자,내용 등) 및 폐기자는 감사증적을 위 해 기록되어야 한다. 외부계약자에 의해 매체가 폐기될 경우 폐기의 확인이 계약서에 정의되어 있고, 완 전한 폐기에 대해 사진, 실사 등의 방법을 통해 확인이 되 어야 한다.	필수	
		7.3.8				필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부	
				<p>폐기가 즉시 이루어지지 않을 경우, 안전한 방법으로 폐기 시까지 보관 되는가?</p> <p>바이러스 등의 악성 프로그램으로부터 개인정보처리시스템 및 개인정보취급자의 PC를 보호하기 위해 악성 프로그램을 예방하고 탐지, 대응하는 대책을 수립하여야 한다.</p>	<p>바이러스 등의 악성소프트웨어로부터 시스템을 보호하기 위한 정책이 존재하는가? 허가되지 않거나 불분명한 소스, 네트워크 등으로 부터의 다운로드를 금지하고, 부특이 하게 다운로드 받을 경우 다운로드 받은 소프트웨어를 검사하는가?</p> <p>전자우편의 첨부파일에 대해 전자우편서버 등에서 바이러스 검사를 수행하는가? 사용자에서의 부주의를 최소화 한다.</p>	<p>폐기가 즉시 이루어지지 않을 경우, 폐기 시까지 개인정보가 노출되지 않도록 안전한 보관이 이루어져야 한다.</p> <p>악성 프로그램 통제 지침 및 절차가 존재하고, 이에 따른 책임할당이 명확해야 한다.</p> <p>허가되지 않거나 불분명한 소스, 네트워크 등으로 부터의 다운로드를 금지하는 정책이 존재하여야 한다. 부특이 하게 다운로드 받을 경우 다운로드 받은 소프트웨어는 바이러스를 검사할 필요적으로 받게 하는 등의 대책이 적용되어야 한다.</p> <p>전자우편의 첨부파일에 대해 전자우편서버 등에서 바이러스 검사를 수행함으로써 사용자에서의 부주의를 최소화 한다.</p>	필수	
	7.3.9	악성 프로그램 통제		<p>주기적으로 바이러스 스캐닝이 이루어지고 있는가?</p>	<p>시스템, Client등에 주기적으로 바이러스 스캐닝을 최소 월 1회 이상 수행함으로써 바이러스를 발견하여 대응한다.</p>	필수	○	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				<p>바이러스 프로그램은 최신 버전으로 업데이트 되는가?</p>	<p>바이러스 프로그램은 최소 월 1회 이상 업데이트를 통해 항상 최신의 것으로 보유될 수 있도록 한다. 또한 바이러스 경보가 발령된 경우 백신소프트웨어 제작업체에서 업데이트 공지가 있는 경우에는 즉시 갱신한다.</p>	필수	0
				<p>바이러스 감염이 발견되었을 경우에 바이러스 확산 및 피해 최소화를 위한 절차가 있는가?</p> <p>사용자는 바이러스 등의 악성 프로그램과 관련된 교육을 받는가?</p> <ul style="list-style-type: none"> - 소프트웨어의 설치 - 소프트웨어의 다운로드 금지 - 불법소프트웨어 설치 금지 - 이메일 주의 	<p>바이러스 발건 시 확산과 피해를 최소화하기 위한 보고, 대응 절차가 존재하며 이에 따라 대응이 이루어져야 한다. 사용자들은 바이러스 등의 악성 프로그램에 대한 예방 및 대응에 대한 교육을 주기적으로 받아야 한다.</p>	필수	0
				<p>악성 프로그램의 내역, 탐지, 대응방법 등에 대한 정보를 사용자에게 지속적으로 공지하는가?</p>	<p>기법은 사용자들에게 악성 프로그램의 탐지 등에 대한 정보를 지속적으로 제공함으로써 사용자들로 하여금 즉각적으로 대응할 수 있도록 해야 한다.</p>	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		7.3.10 이동컴퓨팅	휴대용 정보통신기기의 사용 시에 개인정보 보호를 보호하기 위한 보안 정책을 수립하고, 내부 네트워크의 연결 및 공공 장소에서의 사용에 대한 정책을 수립하여야 한다.	이동컴퓨터 보안에 대한 다 음과 같은 정책이 수립되어 있는가? - 이동컴퓨터의 사용 - 물리적보호, 접근제어, 암호화, 백업, 바이러스 정책 - 내부네트워크와의 연결	이동컴퓨터 보안에 대해서 다음과 같은 정책이 수립 되어야 한다. - 이동컴퓨터의 사용 - 물리적보호, 접근제어, 암호화, 백업, 바이러스 정책 - 내부네트워크와의 연결	필수	
				이동컴퓨터의 분실 시 개인 정보의 유출 방지를 위한 암호화, 장비보호를 위한 물리적 로깅장치, 분실 컴퓨터의 추적 등의 대책이 수립 되어 있는가?	이동컴퓨터의 분실시 정보의 유출 방지를 위한 암호화, 장비보호를 위한 물리적 로깅장치, 분실 컴퓨터의 추적 등의 대책을 수립해야 하고, 주요 이동컴퓨터에 대해서는 강화된 보안대책을 수립한다.	필수	
				이동컴퓨터 사용자는 관련 보안위험과 대응방안을 교 육받고 있는가?	이동컴퓨터 사용자는 관련 보안위험 및 대응방안에 대해 교육받아야 한다.	필수	
				이동컴퓨터로 부터 공공망을 통해 내부 네트워크 접속시 속도의 적절한 인식, 인증, 접근 통제 대책(VPN 등 포함)이 수립되어 있는가?	이동컴퓨터로 부터 공공망을 통해 내부 네트워크 접속시 속도의 적절한 식별, 인증, 접근 통제 대책(VPN 등 포함)이 수립되어야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		7.3.11 원격작업	재택 근무와 같은 원격 작업 수행시 이에 대한 물리적, 논리적인 보호를 위한 정책과 절차를 마련하여야 한다.	다음의 내용을 포함한 재택 근무와 같은 원격작업에 대한 정책, 절차가 존재하는가? - 허가된 원격작업의 내용 - 작업시간 - 접근허가된 내부 시스템 및 서비스 원격작업을 통해 내부 시스템 접근 시, 접근통제, 암호화 대책이 수립되어 있는가? (ID/Password외 추가인증, 접근통제, 암호화 대책, VPN 은 타 점검항목 참조)	재택 근무와 같은 원격 작업 수행시 이에 대한 물리적, 논리적 보호를 위한 정책 및 절차를 마련하여야 한다.	필수	
				재택 근무의 물리적 보안 환경이 마련되어 있는가?	재택근무에 대한 물리적 보안 환경에 대한 지침이 정의되어 있고, 재택근무자가 이 지침을 숙지하며 이에 따른 근무환경을 구성하여야 한다.	선택	
				원격작업의 기간이 완료되었을 경우 접근권한, 장비 등이 회수되고 있는가?	원격작업의 기간이 완료되었을 경우 접근권한, 장비 등이 회수되어야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		7.3.12 공개 서버 보안관리	웹서버 등을 통해 이용자의 개인정보를 처리할 경우 이를 통해 개인정보 노출이 발생하지 않도록 공개 서버에 대한 기술적, 물리적 보안대책을 수립하고 운영하여야 한다.	다음과 같은 사항들을 포함하는 웹서버 등의 공개서버에 대한 관리 및 보안 지침이 존재하는가? - 접근제한관리 - 네트웍상의 위치 설정 - 설정 관리 - 로깅관리 - 주기적 점검 관리 등	웹서버 등 공개서버에 대한 관리 및 보안지침이 수립되어 있다. - 접근제한관리 - 네트웍상의 위치 설정 - 설정 관리 - 로깅관리 - 주기적 점검 관리 등	필수	
				웹서버에 개인정보를 게시할 경우 승인과 책임 등의 권한 할당과 게시절차가 정되어 있는가? 공개 서버는 내부망과 분리하여 설치되며, 침입차단 시스템 등에 의해 보호되는 네트워크 보호 대책이 수립되고 운영되고 있는가?	웹서버 등을 통해 개인정보를 공개할 경우 정보에 대한 수정, 저장 및 공개에 따른 허가 및 게시절차가 수립되어야 한다. 공개 서버에 대한 네트워크 보호 대책이 수립되고 운영되어 있다.	필수	○
				공개 서버 내에 보호되어야 할 주요 개인정보를 정의하며, 주요 개인정보 전송시 비밀성과 무결성을 보장하는 보안서버 구축 등의 조치를 적용하고 있는가?	공개 서버에 보호되어야 할 주요 개인정보를 정의하며, 주요 개인정보 전송시 비밀성과 무결성을 보장하는 보안서버 구축 등의 조치를 적용하여야 한다.	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				<p>공개 서버에 접근할 수 있는 사용자 계정을 제한하고 불필요한 계정, 웹서비스 계정에 불필요한 모든 서비스, 개발도구 등의 사용을 제한하는가?</p> <p>계약성진단도구 등을 이용하여 서버의 취약성 및 서버상의 중요 응용 프로그램에 대한 무결성을 수시로 점검하고 이에 따라 발견된 문제점을 해결하고 있는가?</p> <p>개인정보 노출을 방지하기 위하여 공개서버의 모니터링을 실시하고 있는가?</p>	<p>공개 서버에 접근할 수 있는 사용자 계정을 제한하고 불필요한 계정, 웹서비스 계정에 불필요한 모든 서비스, 개발도구 등의 사용을 제한하는가?</p> <p>계약성진단도구 등을 이용하여 공개서버는 다양한 위험에 노출되어 있으므로 수시로 취약성 진단프로그램을 이용한 무결성 점검하여 서버의 취약성을 점검하고 이에 따라 발견된 문제점을 해결해야 한다.</p>	필수	
				<p>개인정보 노출 및 접근 영역에 대해 로깅지침이 수립되어야 하며, 해당 로그는 안전하게 저장되고 접근이 통제되고 있는가?</p>	<p>공개서버에 대한 로깅 및 로그관리지침이 수립되어야 하며, 이에 따라 로깅 및 보관이 이루어져야 한다.</p>	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
7.4	개인정보 처리시스템 개발 시 개인정보 영향평가를 수행하여야 하며, 보안 요구 사항에 따라 구현 및 테스트 등에 대한 공식적인 변경관리 절차를 수립하고 이행하여야 한다.	분석 및 설계 보안 관리	개인정보 처리시스템을 새로 개발 또는 구매 및 개선 시 개인정보 영향평가를 수행하여야 하며 평가 결과에 따른 보안 요구 사항을 포함하여 개발하여야 한다.	개인정보처리시스템 개발, 구매 및 개선 시 개인정보 영향평가를 수행하였는가?	개인정보처리시스템 개발 및 개선 시 개인정보 영향 평가를 수행하여야 한다. 영향 평가 결과에 따라 보안 요구 사항을 도출하고 이러한 보안 요구 사항은 법적 요건을 만족하여야 한다.	필수	
		7.4.1			보안요구사항을 만족하기 위한 보안대책이 설계에 포함되어 있는가?	필수	
		7.4.2	개인정보처리시스템에 대한 보안요구사항을 만족하는 대책을 구현하고 보안요구사항에 대한 시험을 수행하여야 한다.	웹 등 응용시스템 안전 구현을 위한 코딩표준이 마련되어 있는가?	응용시스템의 안전한 구현을 위한 코딩규약 및 표준이 있어야 한다	필수	
				응용시스템이 코딩 표준에 따라 구현되고 있는가?	응용시스템은 코딩 표준에 따라 구현되어야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				구현된 기능이 본래의 개인정보 보호 요구사항을 충족하는지 확인하기 위한 시험 계획 및 기준이 존재하고 이에 따라 시험을 수행하는가?	개인정보 보호 요구사항을 충족하는지를 확인하기 위한 시험이 수행되고 충족하는 것으로 확인되어야 한다. · 시험의 성공/실패, 시험의 종료에 관한 정의된 기준이 존재하고 이에 따라 시험이 시행되어야 한다.	필수	
		7.4.3 운영 환경 이행보안	개인정보 운영 프로그램의 수정 권한이 적절한 범위 내에 제한되어 있고, 개인정보 운영시스템은 실행코드만 보유하여야 한다. 실행코드는 성공적인 시험과 사용자 인수 후에 실행하여야 한다.	개인정보 운영 프로그램의 수정 권한이 적절하게 통제되고 있는가? 개인정보 운영 시스템에는 실행코드만 존재하는가?	인가된 개발자 또는 관리자만이 인가된 방법으로 운영 프로그램을 수정할 수 있어야 한다. 개인정보 운영시스템에는 가능한 한 실행코드만이 존재하여야 하며, 소스 프로그램이나 컴파일러 등이 존재해서는 안된다.	필수	
				시험이 성공적으로 완료되고 사용자가 최종 인수를 승인한 후에만 실행코드가 수행되는가?	개인정보 응용시스템의 운영 시작 전에 필요한 시험과 사용자 인수의 인수가 이루어져야 한다.	선택	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부	
		7.4.4	<p>데이터의 보호</p> <p>운영데이터를 시험용으로 사용하고자 할 경우 개인정보를 변경 또는 삭제하고 개인정보관리책임자의 승인 후에 시행하여야 한다. 또한 테스트 환경에 대하여 운영환경에 준하는 보안을 시행하고 테스트 완료 후 운영데이터는 테스트 시스템에서 삭제하여야 한다.</p>	<p>운영데이터가 복사될 경우 보호를 테스트 하는 경우를 최소화하여야 하며, 중요 개인정보를 변경 또는 삭제하고 승인을 받은 후 복사하는 절차를 수립하여 이 테스트 환경에 따라 수행하고 있는가?</p>	<p>운영데이터를 시험용으로 사용하기 위하여 복사할 경우 중요한 개인정보를 변경 또는 삭제하고 승인을 받은 후 복사하는 절차를 거치며 감시기록을 생성하여야 한다.</p>	필수		
		7.4.5	<p>프로그램의 접근보안</p> <p>소스 프로그램은 실제 운영 환경에 보관하지 않는 것을 원칙으로 하며, 소스 프로그램 관리자는 각 운영시스템 별로 지정하여야 한다. 또한 소스 프로그램 접근에 대한 통제절차를 수립하고 이행하여야 한다.</p>	<p>소스 프로그램은 실제 운영 환경에 보관하지 않는 것을 원칙으로 하고 있는가?</p>	<p>소스 프로그램과 목적 프로그램 간의 버전관리가 성립하고 있는가?</p>	<p>소스 프로그램은 원칙적으로 운영 환경에 보관해서는 안된다. 단 웹은 스크립트 파일의 경우 엄격한 변경관리 대책이 필요하다.</p> <p>소스 프로그램과 목적 프로그램은 일대일 대응되는 방식으로 버전관리가 이루어져야 한다.</p>	선택	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				이전 소프트웨어 버전이 비상대책을 위해 보관되고 있는가?	이전 버전의 소프트웨어, 운영 일시, 지원 소프트웨어, 작업통제, 데이터 정의, 절차 등의 정보와 함께 보관되어야 한다.	선택	
				시스템에 대한 접근 통제 절차를 수립하고 이행하는가?	운영자나 사용자 등 인가되지 않은 사람이 시스템에 접근할 수 없도록 접근 통제 하여야 한다.	필수	
		7.4.6. 변경 관리 절차	개인정보처리시스템의 변경에 따른 개인정보 노출, 손상, 파괴를 최소화하기 위하여 공식적인 변경관리 절차를 수립하고 이행하여야 한다.	개인정보처리시스템의 공식 존재 관리 하에 따라 변경이 이루어지는가?	문서화된 변경관리절차가 존재하여 이에 따른 변경관리 절차가 수행되어야 한다. 변경관리 절차는 변경 요청, 변경 계획 및 인가, 최종 확인절차 등이 포함되어야 한다. 또한 일반적 변경절차와 달리 시급한 조치를 요하는 경우를 대비한 비상 변경 절차가 마련되어야 하며 이는 사후 검토와 인가를 필요로 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				개인정보처리시스템의 변경이 승인되기 전에 변경에 따라 개인정보에 발생할 수 있는 영향을 평가하는가?	변경에 따른 개인정보에 대한 새로운 위험 발생 여부와 보호 요건을 확인하기 위하여 변경의 규모에 적합한 영향평가를 시행하고 필요한 경우 대책을 개발하여야 한다.	필수	
				개인정보처리시스템의 변경 수행 전에 상세한 변경내역을 문서로 승인하는가?	변경 요청서에 따른 상세 변경 계획서가 IT 부서 또는 개발 부서에서 마련되고 확인되어야 한다면 변경계획서에는 변경 내역, 기간, 인력, 영향 등을 포함하여야 한다.	필수	
				개인정보처리시스템에 대한 실제 이루어진 변경이 문서화된 내용과 일치하는가?	변경에 대한 문서화가 정확하게 이루어져야 한다. 변경 사항에 관련된 프로그램 및 매뉴얼은 해당 변경을 반영하여 변경되어야 한다.	필수	
				개인정보처리시스템 변경 후 사용상의 문제를 확인하는 절차가 있는가?	변경 완료 후 일정 기간이 지나 사용자의 반응을 확인하고 문제가 발생된 것이 없는지 확인하는 절차가 있어야 한다.	선택	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				개인정보처리시스템 변경에 대한 관리자 교육이 수행되는가?	변경 및 사용방법의 변동사항은 관리자 및 운영자에게 적시에 교육되어야 한다.	필수	
		운영체제 변경 시의 변동 검토	운영체제 변경이 필요한 경우 개인정보처리시스템의 운영이나 보안에 미치는 영향을 분석, 검토하여야 한다.	운영체제의 변경이 개인 정보처리시스템의 전반적인 보안 및 성능 향상을 평가하는 공시적인 영향 분석서가 있는가?	운영체제 및 인프라의 변경 시에는 공식적인 영향분석이 이루어지고 문서화되어야 한다.	필수	
		7.4.7		운영환경에 도입되기 전에 개인정보보호에 대한 기능현업에 포함하여 철저한 시험이 이루어지는가?	별도의 시험환경에서 가장 가까운 형태로 응용시스템의 시험운용을 거쳐야 하며 이때 보안 관련 요구들을 함께 테스트해야 한다.	선택	
				운영체제 설치시 파라미터, 패스워드 등이 적절하게 변경되고 있는가?	운영체제 설치 시 필요한 파라미터들은 설치 안내서 또는 기 사용되던 값으로 적절히 변경되어야 하며, 디폴트 패스워드는 반드시 변경되어야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		7.4.8 소프트웨어 패키지 변경	개인정보처리를 위한 소프트웨어 패키지는 개인정보보호 정책 및 법적요건을 만족하여야 하며 패키지 변경 시에는 공급자의 동의 를 얻으며, 수정이 가 능한지 확인하여야 한 다. 모든 변경사항은 시험하고 문서화하여 야 한다.	개인정보처리를 위해 소프트웨어 패키지를 도입할 경 우 조직의 개인정보보호 정책 및 법적 요건을 만족하 는지 검토하는가? 소프트웨어 패키지의 변경 으로 인한 개인정보보호 에 대한 영향이 분석되는가?	개인정보처리 시스템은 조직 의 개인정보보호 정책 및 법 적 요건을 만족하여야 한다. 정책 및 법적 요건상 반드시 소프트웨어 패키지 변경이 필요한 경우 이러한 변경에 따른 공식적인 영향 분석이 수행되고 문서화되어야 한다.	선택	
				소프트웨어 패키지 변경시 다음을 포함하여 변경에 대한 공급자의 동의를 받는 가? - 표준적인 패키지 업데이트 가능 - 유지보수에 대한 책임과 영향	소프트웨어 패키지 변경시에 는 반드시 변경에 대한 공급 자 동의를 받고 수행하여야 한다. 공급자의 동의 시에는 - 추후의 업데이트에 대한 지 원 보증 - 필요한 고려사항 명시 - 예상되는 문제 및 그 해결 방안 - 변경 사항에 대한 유지보수 책임 및 수행 방안을 확인한 다.	선택	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				소프트웨어 패키지에 대한 변경이 개인정보 처리에 미치는 영향을 고려하여 모든 개인정보 관련 기능을 포함하여 시험을 수행하고 관련된 모든 문서를 업데이트하여야 한다.	변경 계획서에 따라 변경을 수행하고 개인정보 보호 관련 기능을 포함하여 시험을 수행하고 관련된 모든 문서를 업데이트하여야 한다.	선택	
7.5	개인정보처리시스템에서 개인정보의 출력시 용도, 용도에 따라 출력할 정보를 복사할 경우 필요한 사항을 기록하고 사생활을 보호하여야 한다.	출력, 복사 시 용도 특정	개인정보처리시스템에서 개인정보의 출력시 용도를 특정하여야 하며, 용도에 따라 출력할 정보를 최소화하여야 한다.	개인정보처리시스템에서 개인정보의 출력시 용도에 따른 출력 항목을 최소화하는가?	개인정보를 인쇄하거나, 파일로 출력할 경우에는 어떤 업무용인지 용도를 정하여야 한다. 업무상 용도에 따라 필요하지 않은 항목을 출력해서는 안된다. 특히 인쇄 및 파일 출력은 더 많은 개인정보를 담게 되므로 강력하게 제한하여야 한다.	필수	0
				개인정보처리시스템에서 화면에 개인정보를 출력할 때 기능을 메뉴화하여 업무내용에 따라 필요한 정보만을 표시할 수 있도록 하고, 본사, 이용자와 필요한 최소한의 정보만을 표시하는가?	개인정보처리시스템에서 화면에 개인정보를 출력할 때 필요한 정보만을 표시하도록 하고, 본사, 이용자 등 접근 위치에 따라, 부서 별, 업무 별, 직급 별로 권한을 달리하여 볼 수 있는 정보를 제한하여야 한다.	필수	0

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		출력, 사시 및 인	개인정보를 테이프, 디스크, 출력물, 이동식 저장 장치 등에 복사할 경우 필요한 사항을 기록하고 사진을 받아야 한다.	개인정보취급자가 테이프, 디스크, 출력물, 이동식 저장 장치 등에 복사할 경우 필요한 사항을 기록하는가?	기록하여야 할 사항은 다음과 같다. 1. 출력·복사물 일련번호 2. 출력·복사물의 형태 3. 출력·복사 일시 4. 출력·복사의 목적 5. 출력·복사물 한자의 소수 및 생명 6. 출력·복사물을 전달 받을 자 7. 출력·복사물의 파기일자 8. 출력·복사물의 파기 책임자	필수	0
		7.5.2	출력, 사시 및 인	개인정보를 출력하거나 등 가능한 저장매체에 복사할 경우 사전에 개인정보관리책임자의 승인을 받는가?	개인정보관리책임자는 해당 출력, 복사행위가 법 규정에 위배되지 않는지를 검토하여 적합한 경우에만 승인하여야 한다. 조직의 규모에 따라 개인정보책임자가 수행하기 어려운 경우, 초기에는 개인정보관리책임자의 승인을 받고 반복되는 경우 부서별 책임자 또는 관리자의 사전 승인을 받되 그 적절성에 대한 주기적 검토가 필요하다.	필수	0

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부			
				<p>인쇄 및 파일 출력시 출력자, 출력 일시 등을 포함하는 로고는 로고가 기록되는가?</p> <p>출력물, 복사물에는 조직의 명칭 및 기록된 출력, 복사물의 일련번호를 표시하는가?</p> <p>출력물, 복사물로부터 다시 출력 또는 복사하는 경우에도 조직의 명칭 및 새로운 일련번호를 표시하며 대한 로고가 기록되는가?</p> <p>개인정보의 출력, 복사에 대한 승인 시 승인받고자 하는 개인정보취급자에게 범 유출 시 법적 책임을 지게 됨을 주지시키는가?</p>	<p>인쇄 및 파일 출력시 출력자, 출력 일시 등을 포함하는 로고가 남아야 한다. 이 로고는 위변조되지 않도록 보관되어야 한다.</p> <p>우편발송, 고지서 발급 등을 위해 개인단위로 증이에 인쇄하는 경우 일련번호를 표시하지 않아도 된다</p> <p>출력, 복사물로부터 다시 출력 또는 복사하는 경우에도 적용되어야 한다.</p> <p>이용자의 개인정보를 취급하거나 취급하였던 자가 직무 상 알게 된 개인정보를 훼손, 침해 또는 누설할 경우 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 규정하고 있는 관련 법규를 주시시켜야 한다.</p>	필수	필수	필수	필수	○
						필수	○			
						필수	○			

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				보호구역에 대하여 정책에 명시한 물리적 접근 제가 수행되고 출입기록이 남겨지고 있는가?	정책에서 명시한 보안 대책 이 존재하고 이용되며 접근 통제 실시되어야 한다. 허가 된 개인정보취급자만이 보호 구역에 출입하여야 하며 일반 출입 기록을 남겨야 한다. 그 외의 출입자는 신원확인 및 출입 사유와 함께 기록을 남겨야 한다.	필수	
		물리 접근통제	개인정보를 취급,처리 하는 보호구역에 대한 출입통제기록을 남기고, 주기적으로 타당성을 검토해야 한다.	보호구역의 출입 내역을 주기적으로 검토하고 있는가? 출입허가의 타당성을 주기적으로 검토하고 있는가?	정책에서 명시한 보안 대책 이 존재하고 이용되며 접근 통제가 실시되어야 한다. 허가된 개인정보취급자만이 보호 구역에 출입하여야 하며 일반 출입 기록을 남겨야 한다. 그 외의 출입자는 신원확인 및 출입 사유와 함께 기록을 남겨야 한다.	필수	
		8.1.2			출입허가지 명단 또는 출입 증 배부 명단을 관리자가 주 기적으로 검토하여 현재의 출입 필요에 따르고 있는지 확인하여야 한다.	선택	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
8.2	전력 및 통신 케이블 등의 장비를 보호하고, 개인정보를 담고 있는 장비의 폐기 및 재사용 시에는 기록된 완전히 삭제되어 복구 불가능한지 확인하여야 한다.	이러한 정보 보호	개인정보를 송·수신하거나 정보서비스를 지원하는 전력 및 통신 케이블은 방화벽이나 손상을 입지 않도록 보호하여야 한다.	통신 회선이 도청이나 손상으로부터 보호되고 있는가?	전력 및 통신 회선은 상호 교란이 일어나지 않도록 분리하여 쉽게 접근하지 못하도록 매설이나 보호조치를 취하여야 한다.	필수	
	8.2.1	장비 안전 및 폐기 재사용	개인정보를 담고 있는 장비의 폐기 및 재사용 시에는 이를 물리적으로 파괴하거나 폐기 전에 저장 매체에 기록된 내용이 완전히 삭제되어 복구가 불가능한지 확인하여야 한다.	개인정보 장비의 폐기 시에 개인정보 장비의 폐기 시에 저장 매체를 물리적으로 파괴하거나, 저장된 정보가 완전히 삭제되어 복구가 불가능한지 확인하여야 한다.	개인정보 장비의 폐기 시에 저장 매체를 물리적으로 파괴하거나, 저장된 정보가 완전히 삭제되어 복구가 불가능한지 확인하고 있는가?	필수	0
8.3	개인정보취급자에 대하여 계약서에 개인정보 문서나 저장 매체를 남겨놓지 않도록 하고, 통상 근무시간 동안이나 그 외의 시간에는 비인가된 자에 의한 정보 접근, 손상	사무실 보호	개인정보취급자에 대하여 계약서에 개인정보 문서나 저장 매체를 남겨놓지 않도록 하고, 통상 근무시간 동안이나 그 외의 시간에는 비인가된 자에 의한 정보 접근, 손상	개인정보 자료를 업무시간 이후에는 이석시 자책상위에 개인 정보 문서나 자료를 보관하는 개인 정보 저장 매체를 비우지 않도록 하는 정책을 수립하고 있는지 확인하고 있는가?	업무시간 이후에는 이석시 자책상위에 개인정보 문서나 자료를 보관하는 개인 정보 저장 매체를 비우지 않도록 하는 개인정보저장 매체를 방치하지 않도록 하고, 통상 근무시간 동안이나 그 외의 시간에는 비인가된 자에 의한 정보 접근, 손상	필수	
8.3.1	8.3.1	사무실 보호	개인정보취급자에 대하여 계약서에 개인정보 문서나 저장 매체를 남겨놓지 않도록 하고, 통상 근무시간 동안이나 그 외의 시간에는 비인가된 자에 의한 정보 접근, 손상	개인정보 자료를 업무시간 이후에는 이석시 자책상위에 개인 정보 문서나 자료를 보관하는 개인 정보 저장 매체를 비우지 않도록 하는 정책을 수립하고 있는지 확인하고 있는가?	업무시간 이후에는 이석시 자책상위에 개인정보 문서나 자료를 보관하는 개인 정보 저장 매체를 방치하지 않도록 하고, 통상 근무시간 동안이나 그 외의 시간에는 비인가된 자에 의한 정보 접근, 손상	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
	간 동안이나 그 외의 시간에 비인가된 자에 의한 정보 접근, 손상 등을 방지하기 위하여 컴퓨터 모니터에 정보 처리에 관한 사항을 남기지 않도록 하여야 한다.		을 방지하기 위하여 컴퓨터 화면에 정보 처리에 관한 사항을 남기지 않도록 하여야 한다.	컴퓨터에 중요한 화면을 띄워놓고 이석하지 않도록 하는 정책이 있으며 준수되고 있는가? 팩스, 복사기, 공개 단말기, 하드디스크가 있는 프린터 등 사용자가 지정되어 있지 않은 사무 장비에 대한 보호대책이 있는가?	개인정보처리 응용이나 데이터를 띄워놓고 자리를 이석하여서는 안된다. 장시간 자리를 비울 경우 전원을 꺼야 하고 열쇠, 패스워드 등의 보호수단을 사용하여야 한다. 사용자가 지정되지 않은 응용 장비에 대해서는 책임자가 지정되어야 한다. 이러한 장비에서 개인정보가 처리되는 경우 위험 및 대책을 직원들이 알고 있어야 하며 적절한 점검을 수행하여야 한다.	필수	
9. 내부감사 및 감사	개인정보에 대해 적용되는 모든 법, 규제, 계약상의 요구사항을 문서화하고, 이에 대한 내용을 개인	법적 요구사항 명시	기관의 개인정보에 대해 적용되는 모든 법, 규제, 계약상의 요구사항을 정의하고 문서화하여야 하며, 이들 요구사항을 개인정보 보호관리체계에 포함시켜 문서화 한다.	개인정보에 관련된 법, 제, 계약상의 요구사항을 문서화하여 정의하는가?	개인정보보호와 관련하여 기관에 적용되는 법률 및 관련 기준, 계약 요구사항을 식별하고 문서화하여야 한다. * 정보통신망이용촉진 및 정보보호 등에 관한 법률, 신용정보 이용 및 보호에 관한 법률, 금융실명거래 및 비밀보	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
	<p>정보보호관리 체계에 포함 시켜 준수 여부를 검토해야 한다.</p>		<p>개인정보 관련 법규에 서 요구하는 사항의 준수 여부를 검토해야 한다.</p>	<p>법, 규제, 계약상의 요구사항이 준수되고 있는지 검토하였는가?</p>	<p>장에 관한 법률, 공공기관의 개인정보보호에 관한 법률, 위치정보의 보호 및 이용 등에 관한 법률, 통신비밀보호법, 정보통신기반보호법, 전자거래등에서의 소비자보호에 관한 법률, 방문판매등에 관한 법률, 보험법 및 의료법 등이 있으며 이러한 법률에 관련된 시행령, 시행 규칙, 각종 기준 및 가이드라인 등이 존재한다.</p>	필수	
			<p>개인정보 관련 법규에 서 요구하는 사항의 준수 여부를 검토해야 한다.</p>	<p>법, 규제, 계약상의 요구사항이 준수되고 있는지 검토하였는가?</p>	<p>문서화된 법, 규제, 계약상의 요구사항이 준수되고 있는지 검토하여야 한다. 이는 개인정보관리체계 준수 검토 결과 중 법, 규제, 계약상의 요구사항에 매핑된 것만을 뽑아내 확인하는 것으로 가능하다.</p>	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
9.2	개인정보보호 정책 및 대책 준수 여부를 검토하고, 정기적인 점검 실시를 통해 문제점을 고장정하여야 한다.	9.2.1 정책 준수 검토	개인정보 관련 법규에서 요구하는 사항의 준수여부를 검토해야 한다.	개인정보를 취급하는 부서에서 준수해야 하는 개인정보 보호정책을 검토하고, 검토 및 점검시 필요 정보를 문서화하여 제공하며, 발견 사항에 대해 교정하고 있는가?	개인정보를 취급하는 부서의 개인정보보호정책, 절차 준수 여부를 검토하여야 한다. 개인정보를 취급하는 부서는 검토에 필요한 정보를 수집하는 것에 검토해야 한다.	필수	
		9.2.2 기술 점검	개인정보처리시스템이 절차에 따라 운영 관리되고 있는지 정기적으로 점검을 실시한다. 이에 따라 문제점들을 발견한 후 필요한 조치를 취한다.	개인정보처리시스템이 절차에 따라 운영되고 있는지를 점검하기 위한 점검이 정기적으로 수행되는가?	개인정보처리시스템에 대한 기술적인 보안점검이 정기적으로 수행되어야 한다. - 라우터나 스위치 등 네트워크 장비분석 - 방화벽 등의 보안시스템 분석 - 웹서비스 취약점 진단 - 도의침투 테스트 등	필수	
				기술적인 점검은 자격이 있고 숙련된 인력에 의해 점검하며, 허가된 인력의 감독 하에 수행되는가?	기술적인 보안점검은 자격 있고 허가된 인력에 의해서만 수행되어야 한다. * 내부 인력이 기술적 보안점검을 수행할 경우 입사 시 자격심사가 완료 되었다고 볼 수 있고, 용역을 통해 보안점검을 수행할 경우 외부 인력에 대한 자격 적절성 검토가 수행되어야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
9.3	개인정보처리 활동 모니터링 수 있고, 개인 정보 열람 기록 및 처리 기록을 주기적으로 검토하여야 한다.	개인정보 처리 활동 모니터링 등 모니터링 열람을 수 있고 시행하여야 한다. 모니터링 결과는 정기적으로 점검하여야 하고 위험의 정도에 따라 점검 주기를 결정하여야 한다.	9.3.1	기술적 점검시 점검도구의 오용을 방지하기 위한 대책이 수립되어 있는가?	기술적 점검결과 발견된 취약성에 대한 대응방안 및 조치가 이행되며, 적절한 관리층에 보고되어야 한다.	필수	
				기술적 점검결과 발견된 취약성에 대한 대응방안 및 조치가 이행되며, 적절한 관리층에 보고되어야 한다.	필수		
			개인정보처리시스템 사용 및 접근에 대한 모니터링 절차와 책임이 정의되고 있는가?	개인정보처리시스템의 모니터링 절차를 수립하고 시행하여야 한다. - 비인가된 접근 시도	필수		
					- 특권 계정의 사용, 시스템 시작 종료, IO 장비 장착 및 탈착 등 특권적 활동 - 시스템 경고 및 실패 - 시스템 보안설정, 통제에 대한 변경 및 변경 시도	필수	
				모니터링 결과를 점검하는 주기가 정의되어 있으며, 이 결과에 따라 모니터링 결과가 검토되며 보고되는가?	모니터링 결과는 정기적으로 점검하여야 하고 위험의 정도에 따라 점검 주기를 결정하여야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		9.3.2	개인정보 처리 시스템 운영을 방지하기 위하여 개인정보 열람 및 오남용 방지를 위하여 개인정보 열람에 대한 기록을 남기고 주기적으로 검토하여야 한다.	개인정보취급자의 오남용을 방지하기 위하여 개인정보 열람 및 권한 없는 열람시도에 대한 기록을 남기는가? 개인정보 열람 기록을 주기적으로 검토하여 권한없는 열람 및 과도한 접근시도 등의 사용내역을 분석하여, 개인정보 오남용, 이상징후를 추적하여 보고하고 필요한 조치를 취하는가?	열람이 허가된 개인정보취급자라 하더라도 오남용을 방지하기 위하여 개인정보 열람에 대한 취급자, 일시, 대상 등의 기록을 남겨야 한다.	필수	
		9.3.3	개인정보 처리 시스템에 대한 접근을 검토하고 정기적으로 하며, 위변조를 막기 위한 조치를 취해야 한다	개인정보 취급자 등의 의무자 외 위탁업체 및 제3자의 개인정보처리시스템에 대한 접속기록을 일시 및 내역 등 접속기록을 최소 6개월 이상 저장하는가? 응용프로그램을 통하지 않고 DB에 직접 접속하여 개인정보를 조회/변경/삭제/출력시 로그 기록이 남는가?	위탁업체 및 제3자의 개인정보처리시스템에 접속에 대한 일시, 내역 등 접속기록을 최소 6개월 이상 저장하여야 한다.	필수	0

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				개인정보처리시스템 접속 기록을 월1회 이상 정기적으로 확인 및 감독 하는가? 개인정보처리시스템의 접속 기록이 위·변조되지 않도록 별도 저장장치 등의 별도 저장장치에 백업 보관하고, 보관하는가?	개인정보처리시스템 접속 기록을 월1회 이상 정기적으로 확인 및 감독 하여야 한다. 개인정보처리시스템의 접속 기록은 위·변조되지 않도록 별도 저장장치 등의 별도 저장장치에 백업 보관하고, 보관하는가?	필수	0
		9.3.4	이행점검 기록의 명확성을 보장하고 법적인 처리내역과 관련한 정보의 정확성을 보장하고 해당 자료가 정확성을 갖기 위해서는 법적 증거나 징계 자료로서 시스템을 정확히 설정하여야 한다.	개인정보처리시스템의 접근 및 처리내역과 관련한 정보의 정확성을 보장하고 해당 자료가 정확성을 갖기 위해서는 법적 증거나 징계 자료로서 시스템을 정확히 설정하는가?	이행점검 기록의 명확성을 보장하기 위해, 주기적으로 정확한 시각의 설정 및 동기화를 점검한다.	필수	
	9.4	9.4.1	보안감사 계획 및 결과를 수립하고, 감사결과 보고 후 지적사항이 조치되도록 사후관리 하여야 한다.	보안감사 대상, 범위, 주기, 방법, 절차, 감사도구를 포함하고 시행하여야 한다.	개인정보보호 감사 또는 점검을 위한 개인정보 인력이 구성되어 있는가?	필수	0

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				개인정보보호 감사인력에 대한 자격요건이 정의되어 있으며, 감사인력이 독립성 및 전문성을 보유하고 있는가?	개인정보보호 감사 또는 점검 자격요건에 대한 자격요건이 정의를 지무기술서 또는 이행점검 지침에 반영되어야 하고, 이에 따라 선별되어야 한다.	필수	
				개인정보보호감사는 정기적으로 수행되는가?	개인정보보호감사는 정기감사와 별도로 수행되어야 한다.	필수	○
				9.4.2 감사결과와 감사의 결과에 따라 감사보고서를 작성하고 적절한 책임자에게 보고하며, 감시지적 내용이 이행 되도록 사후관리 하여야 한다.	감사결과에 따라 감사 보고서가 작성되어 있으며, 감사결론을 위한 증거가 충분히 뒷받침되고 있는가? 감사결과를 경영진에게 하는 보고 프로세스가 존재하며 이에 따라 적절한 책임자에게 보고가 이루어지는가? 감사결과 검토를 위한 위원회 구성되어 있는가? 정기적으로 회의를 개최하는가?	필수	
					감사결과에 따른 지적사항이 이행 되도록 사후관리가 이루어지는가?	필수	○

생명주기 요구사항

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	범위 근거 여부
1. 개인정보 수집에 따른 조치	1.1 최소한의 정보만을 수집하고, 추가 정보, 민감정보, 간접 수집한 개인정보 등에 대하여 이용자 등의 및 적절한 보호를 취해야 한다.	서비스 제공을 위해 필요한 최소한의 정보만을 수집하고, 수집 시 주민등록번호 대의 수단을 제공하여야 하며, 추가적 정보의 수집을 원할 경우, 정보주체가 선택 제공할 수 있도록 필수와 선택 사항으로 구분하여 기재할 수 있도록 하여야 하며, 선택 사항의 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하여서는 아니된다.	서비스 제공을 위해 필요한 최소한의 정보만을 수집하고, 수집 시 주민등록번호 대의 수단을 제공하여야 하며, 추가적 정보의 수집을 원할 경우, 정보주체가 선택 제공할 수 있도록 필수와 선택 사항으로 구분하여 기재할 수 있도록 하여야 하며, 선택 사항의 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하여서는 아니된다.	서비스 제공을 위해 필요한 최소한의 정보만을 수집하고, 수집 시 주민등록번호 대의 수단을 제공하여야 하며, 추가적 정보의 수집을 원할 경우, 정보주체가 선택 제공할 수 있도록 필수와 선택 사항으로 구분하여 기재할 수 있도록 하여야 하며, 선택 사항의 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하여서는 아니된다.	서비스 제공자는 이용자의 개인정보를 수집하는 경우에는 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 한다. 필수 서비스 외의 부가서비스, 제휴 등의 서비스 및 개인정보 제공을 거부한다는 이유로 필수 서비스의 제공을 거부하여서는 안된다.	필수	○
		1.1.1	서비스 제공을 위해 필요한 최소한의 정보만을 수집하고, 수집 시 주민등록번호 대의 수단을 제공하여야 하며, 추가적 정보의 수집을 원할 경우, 정보주체가 선택 제공할 수 있도록 필수와 선택 사항으로 구분하여 기재할 수 있도록 하여야 하며, 선택 사항의 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하여서는 아니된다.	서비스 제공을 위해 필요한 최소한의 정보만을 수집하고, 수집 시 주민등록번호 대의 수단을 제공하여야 하며, 추가적 정보의 수집을 원할 경우, 정보주체가 선택 제공할 수 있도록 필수와 선택 사항으로 구분하여 기재할 수 있도록 하여야 하며, 선택 사항의 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하여서는 아니된다.	서비스 제공자는 이용자의 개인정보를 수집하는 경우에는 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 한다. 필수 서비스 외의 부가서비스, 제휴 등의 서비스 및 개인정보 제공을 거부한다는 이유로 필수 서비스의 제공을 거부하여서는 안된다.	필수	○
			서비스 제공을 위해 필요한 최소한의 정보만을 수집하고, 수집 시 주민등록번호 대의 수단을 제공하여야 하며, 추가적 정보의 수집을 원할 경우, 정보주체가 선택 제공할 수 있도록 필수와 선택 사항으로 구분하여 기재할 수 있도록 하여야 하며, 선택 사항의 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하여서는 아니된다.	서비스 제공을 위해 필요한 최소한의 정보만을 수집하고, 수집 시 주민등록번호 대의 수단을 제공하여야 하며, 추가적 정보의 수집을 원할 경우, 정보주체가 선택 제공할 수 있도록 필수와 선택 사항으로 구분하여 기재할 수 있도록 하여야 하며, 선택 사항의 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하여서는 아니된다.	서비스 제공자는 이용자의 개인정보를 수집하는 경우에는 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 한다. 필수 서비스 외의 부가서비스, 제휴 등의 서비스 및 개인정보 제공을 거부한다는 이유로 필수 서비스의 제공을 거부하여서는 안된다.	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				개인정보 수집 시 아이핀 등 주민등록번호를 대체하는 수단을 제공 하는가?	정보통신서비스 제공자는 개인정보 수집 시 아이핀 등 주민등록번호의 수집을 최소화 또는 대체할 수 있는 수단을 제공하여야 한다.	필수	○
		1.1.2 중요 정보 제한	개인의 권리·이익이나 생활을 뚜렷하게 침해할 우려가 있는 중대한 개인정보를 수집하지 않아야 하며, 필요한 경우 이용자의 동의를 받아야 한다.	중요한 개인정보를 수집하는 경우, 법적 근거가 있거나, 본인의 동의를 받는가?	서비스 제공자는 사상, 신념, 과거의 병력(病歷) 등 개인의 권리·이익이나 생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 그 개인정보를 수집할 수 있다.	필수	○
		1.1.3 간접 수집 시 조치	수집 시스템에 의한 수집 또는 개인정보 처리를 통해 생성한 간접 수집한 개인정보에 대해 적절한 보호를 취하여 적절히 보호를 취해야 한다.	간접 수집하는 개인정보들에 대해 미리 이용자에게 고지하거나 이를 고지하거나 취급방침 등에 명시하고 동의를 받는가?	이용자로부터 직접 수집하는 정보가 아닌 시스템(예:쿠키) 또는 개인정보 처리를 통해 생성되어 간접 수집된 정보들은, 미리 이용자에게 고지하거나 이용약관에 명시하여야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법규 근거
	1.2 개인정보는 정보주체 또는 법정대리인의 동의를 얻은 후에 수집하여야 하고, 이에 대한 기록을 보관하여야 한다.	1.2.1 정보주체의 동의	개인정보는 정보주체의 동의를 얻은 후에 수집하여야 한다.	간접 수집된 정보를 제공받는 경우, 개인정보 수집에 대한 동의 획득 책임이 개인 정보 제공업체에 있음을 통해 명시하고 있는가?	수집된 정보를 제공받는 경우, 수집 시 동의 획득의 책임이 수집 기관에게 있음을 명시하여야 한다. 또한 위탁관계의 경우 개인정보보호 규정을 위반하지 않도록 감독하여야 한다.	필수	
				개인정보 수집 시 이용자가 쉽고 명확하게 이해할 수 있는 방법으로 이용자의 동의를 받고 있는가?	수집하는 개인정보를 이용하는 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음 사항을 반드시 이용자에게 알리고 동의를 받아야 한다. 1. 개인정보의 수집·이용 목적 2. 수집하는 개인정보의 항목 3. 개인정보의 보유·이용 기간	필수	○
				개인정보 수집 시 이용자가 쉽고 명확하게 이해할 수 있는 방법으로 이용자의 동의를 받고 있는가?	개인정보 수집 시 정보주체로부터 개인정보 수집에 대한 동의를 획득하여야 하며, 동의는 다음 중 하나의 방법으로 동의를 얻어야 한다.	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수여부	법규여부	
					1. 인터넷 사이트에 동의 내용을 게재하고 이용자가 동의 여부를 표시하도록 하는 방법 2. 동의 내용이 기재된 서면을 이용자에게 직접 교부하거나, 우편 또는 모사전송을 통하여 전달하고 이용자가 동의 내용에 대하여 서명날인 후 제출하도록 하는 방법 3. 동의 내용이 기재된 전자우편을 발송하여 이용자로부터 동의의 의사표시가 기재된 전자우편을 전송받는 방법 4. 진화를 통하여 동의 내용을 이용자에게 알리고 동의를 얻거나 인터넷주소 등 동의 내용을 확인할 수 있는 방법을 안내하고 재차 진화통화를 통하여 동의를 얻는 방법			

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수여부	법규거부
					<p>(동의 받지않는 예외사항)</p> <ol style="list-style-type: none"> 1. 서비스 이용계약의 이행을 위하여 필요한 경우 2. 서비스 제공에 따른 요금 정산을 위하여 필요한 경우 3. 정보통신망이용촉진및정보보호등에 관한법률 또는 다른 법률에 특별한 규정이 있는 경우 		
				<p>동의를 얻어야 할 내용을 이용자가 명확히 인지하고 확인할 수 있도록 표시하는가?</p>	<p>동의를 얻어야 할 사항을 이용자가 명확히 인지하고 확인할 수 있도록 표시하여야 하나, 개인정보 수집 매체의 특성상 동의 내용을 전부 표시하기 어려운 경우 이용자에게 동의 내용을 확인할 수 있는 방법(인터넷주소·사업장 전화번호 등)을 안내하고 동의를 얻을 수 있다.</p>	필수	0

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		1.2.2	만14세 미만의 아동의 개인정보를 수집 및 활용 시 동의를 획득하고 고지하여야 한다.	만14세 미만 아동의 개인정보를 수집하는 경우 법정대리인에게 필요한 사항을 고지하여야 하는가?	만14세 미만의 아동으로부터 개인정보를 수집 시 이에 대한 동의를 얻어야 한다.	필수	○
		1.2.3	이용자에게서 동의를 받은 기록은 보관하여야 한다.	만14세 미만 아동의 동의를 받은 기록을 보관하는가?	만14세 미만의 아동으로부터 개인정보를 수집 시 이에 대한 동의를 얻어야 한다.	필수	○
				만14세 미만 아동의 동의를 받은 기록을 보관하는가?	만14세 미만의 아동으로부터 개인정보를 수집 시 이에 대한 동의를 얻어야 한다.	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
1.3	개인정보취급 방침을 마련하여 이용자가 언제든지 접근할 수 있도록 적절한 방법을 따라 공개하여야 한다.	개인정보취급 방침 1.3.1	개인정보취급 방침을 마련하여 이용자가 언제든지 쉽게 확인할 수 있도록 적절한 방법에 따라 공개하여야 한다.	개인정보취급방침이 법적인 요구사항 및 운영에 필요한 사항에 포함되어 정의되었는가? 는가?	이용자의 개인정보를 취급하는 경우, 법적 요건에 따라 아래의 내용을 포함한 개인정보취급방침을 마련하여야 한다. 1. 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집방법 2. 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법적인 경우에는 법인의 명칭을 말한다), 제공받는 자의 이용 목적과 제공하는 개인정보의 항목 3. 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 파기방법(방법 제29조 각 호 외의 부분 단서에 따라 개인정보를 보존하여야 하는 경우, 그 보존근거와 보존하는 개인정보 항목을 포함) 4. 개인정보 취급위탁을 하는	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수여부	법률근거여부
				개인정보취급방침을 이용자가 언제든지 쉽게 확인할 수 있도록 적절한 방법으로 공개하였는가?	업무의 내용 및 수탁자(해당되는 경우에만 취급방침에 포함) 5. 이용자 및 법정대리인의 권리와 그 행사방법 6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항 7. 개인정보 관리책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처 개인정보의 수집 장소와 매체 등을 고려하여 하기 내용 중 어느 하나 이상의 방법으로 개인정보취급방침을 공개하되, 그 명칭을 '개인정보취급방침'이라고 표시하여야 한다.	필수	O

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수여부	관련규약	
					<p>1. 인터넷 홈페이지의 첫 화면 또는 첫 화면과의 연결화면을 통하여 법 제27조의2제2항 각 호의 사항을 이용자가 볼 수 있도록 하는 방법. 이 경우 정보통신서비스 제공자들은 글자 크기, 색상 등을 활용하여 이용자가 개인 정보취급방침을 쉽게 확인할 수 있도록 표시하여야 한다.</p> <p>2. 점포·사무소 안의 보기 쉬운 장소에 새 붙이거나 비치하여 열람하도록 하는 방법</p> <p>3. 동일한 제호로 연 2회 이상 계속적으로 발행하여 이용자에게 배포하는 간행물·소식지·홍보지·청구서 등에 지속적으로 게재하는 방법</p>			

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				<p>개인정보취급방침을 변경하는 경우에는 그 이유 및 변경 내용을 지정된 방법에 따라 지체 없이 공지하고, 이용자가 언제든지 변경된 사항을 쉽게 알아 볼 수 있도록 조치하는가?</p>	<p>개인정보취급방침을 변경하는 경우에는 그 이유 및 변경 내용을 지정된 방법에 따라 지체 없이 공지하고, 이용자가 언제든지 변경된 사항을 쉽게 알아 볼 수 있도록 조치하여야 한다. 개인정보취급방침의 변경 이유 및 내용은 다음 각 호의 방법 중 어느 하나 이상의 방법으로 공지한다.</p> <ol style="list-style-type: none"> 1. 정보통신서비스 제공자등이 운영하는 인터넷 홈페이지의 첫 화면의 공지사항란 또는 별도의 창을 통하여 공지하는 방법 2. 서면·모사전송·전자우편 또는 이와 비슷한 방법으로 이용자에게 공지하는 방법 3. 점포·사무소 안의 보기 쉬운 장소에 써 붙이거나 비치하는 방법 	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
2. 개인정보 제 이용 및 제 공에 따른 조치	2.1 개인정보는 이 용자에게 고지 하고 동의 받은 범위를 벗어나 이용하지 않아 야 하고, 만약 동의 범위를 벗 어나 이용할 경 우, 정보주체로 부터 추가적인 동의를 받아야 한다.	2.1.1 목적 내 개인정보 이용	개인정보는 이용자에 게 고지하고 동의 받 은 범위를 벗어나 이 용하지 않아야 하고, 만약 동의 범위를 벗 어나 이용할 경우, 정 보주체로부터 추가적 으로 동의를 받아야 한다.	이용자 및 이용자의 범 위로 동의한 범위를 벗 어나 이용하거나 정보 를 제공하지 않는가? 개인정보 수집 시 고지 하는 범위나 이용목적 에 맞는 정보 수집을 하는가?	개인정보 수집 시 고지하 거나 이용약관에 명시 한 목적을 벗어난 개인 정보 수집이 없는지 확인한다.	필수	○
	2.2 신청사업자는 이용자의 불 만 처리를 위 한 상담창구 를 운영하고, 이용자의 요 청을 지체없 이 처리하고 기록을 남겨 야 한다.	2.2.1 이용자의 불 만 처리 관련	개인정보와 관련한 이 용자의 의견 및 불만 을 접수·처리하기 위 하여 상담창구를 운영 하여야 한다.	이용자로부터의 개인 정보에 관한 의견과 불 만 사항을 접수하고 처 리하는 상담창구 운영 영향을 받고 있는가? 개인정보에 대한 불 만 사항을 접수하고 처 리하는 상담창구 운영 영향을 받고 있는가?	이용자로부터의 개인 정보에 관한 의견과 불 만 사항을 접수하고 처 리하는 상담창구 운영 영향을 받고 있는가? 개인정보에 대한 불 만 사항을 접수하고 처 리하는 상담창구 운영 영향을 받고 있는가?	개인정보 수집 시 고지하 거나 이용약관에 명시 한 목적을 벗어난 개인 정보 수집이 없는지 확인한다.	필수

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				이용자의 열람, 이용, 정정 및 제공내역 요청을 받은 경우 본인여부를 확인하는 절차가 있는가?	정보주체가 개인정보에 대한 열람·정정 또는 개인정보의 이용 및 제3자 제공내역을 요청하는 경우 본인여부를 확인할 수 있는 절차가 마련 되어 있어야 한다.	필수	○
				이용자 및 이용자의 법정대리인인 사용자 개인정보에 대한 오류 정정을 요구할 경우 오류를 정정할 때까지 해당 이용자의 개인정보 이용 제공을 중단하고 있는가? 외부위탁 또는 제3자에게 제공한 개인정보에 대한 정정 요구 시 이에 대해서도 정정 및 동의철회시에는 수 동의철회에 대한 조치를 취하고 결과를 확인하는가?	이용자 및 법정대리인의 개인정보에 대한 오류 정정을 요구하는 경우 이를 확인하고 당해정보를 정정하기 전까지 개인정보가 이용 이용되지 않도록 하는 절차가 마련되어 있어야 한다.	필수	○
				이용자가 개인정보 수집·이용·제공 등의 동의 철회를 요청할 경우 지체없이 조치하여야 하는가?	이용자 및 법정대리인이 언제든지 개인정보 사용에 대한 동의를 철회할 수 있는 방법 및 절차가 있는가?	필수	○
		동의철회	2.2.3				

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				이용자 및 이용자의 법정대리인이 이용자의 개인정보 등의 수집·이용·제공 등의 동의 철회를 요청할 경우 지체 없이 수집된 개인정보를 파기하는 등 필요한 조치를 취하는가?	이용자 및 이용자의 법정대리인은 이용자의 동의 철회 (또는 탈퇴) 요청을 받은 경우 지체없이 수집된 개인정보를 파기하는 등 필요한 조치를 취한후 그 사실을 이용자에게 지체 없이 통지 해야 한다. 다만, 정통방법을 제외한다면 법령의 규정에 의하여 보존할 필요성이 있는 경우에는 파기하지 않아도 된다.	필수	○
				이용자 및 이용자의 법정대리인이 개인정보 수집·이용·제공 등의 동의철회를 요청할 경우 본인 및 법정대리인의 본인 여부를 확인하는 절차가 존재하는가?	이용자 및 이용자의 법정대리인이 개인정보 수집·이용·제공 등의 동의철회를 요청할 경우 본인 및 법정대리인의 본인 여부를 확인하는 절차가 존재하여야 한다.	필수	
				법적근거에 따라 동의철회 후에도 개인정보를 보관하는 경우 적절한 보호조치를 취하고 있는가?	법적근거에 따라 동의철회 후에도 개인정보를 보관하는 경우 적절한 보호조치를 취하여야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		2.2.4 이 용 자 의 오 청 의 처 리	이용자의 요청을 지체 없이 처리하고 기록을 남겨야 한다	이용자가 동의의 철회, 개인정보의 열람·제공 또는 오류 정정을 요구하는 방법은 개인정보의 수집 방법보다 쉬운가? 이용자가 개인정보 수집·이용·제공 등의 동의철회 또는 개인정보의 열람·제공, 오류의 정정 등을 요구할 경우 지연 또는 거절 시 타당한 사유에 근거하고 있는가?	이용자가 개인정보 수집·이용·제공 등의 동의철회 또는 개인정보의 열람·제공, 오류의 정정을 요구하는 방법은 개인정보의 수집 방법보다 더 쉬워야 한다. 이용자의 요청을 거절할 경우에는 합법적이고 타당한 사유가 있어야 한다. - CCTV 기록 열람시 타인 정보 침해 - 금융계약 안전성 유지를 위한 일정기간 내 동의 철회 제한 - 기타 법적 불가 사유	필수	○
				이용자가 개인정보 수집·이용·제공 등의 동의철회 또는 개인정보의 열람·제공, 오류의 정정 등을 요구할 경우 요청내역 및 처리에 대한 모든 기록이 남는가?	이용자의 개인정보에 대한 모든 요청에 대하여 요청 내역, 처리 결과와 거절 시 사유를 기록 관리하여야 한다.	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
2.3	<p>신청사업자는 제3자에게 개인정보를 처리할 시 이용자 동의를 취득하고, 계약서 및 서비스 수 준 협약에 수탁사 책임을 명시하여 수탁사를 관리 감독 하 여 야 한다.</p>	<p>이용자 및 고지 동의</p>	<p>제3자에게 개인정보를 처리할 수 있도록 업무를 위탁하는 경우에는 관련 사항을 이용자에게 알려야 한다.</p>	<p>제3자에게 이용자의 개인정보를 위탁하는 경우 관련 사항을 이용자에게 알리는가?</p>	<p>제3자에게 이용자의 개인정보를 수집·보관·처리·이용·제공·관리·파기 등을 할 수 있도록 업무를 위탁하는 경우에는 다음 각 호의 사항을 이용자에게 알려야 한다.</p> <ol style="list-style-type: none"> 개인정보취급위탁을 받는 자(이하 수탁자) 개인정보취급위탁을 하는 업무의 내용 	필수	○
		2.3.1		<p>개인정보 취급위탁에 대한 동의 획득시, 개인정보 수집 시와 동일한 방법으로 동의를 받는가?</p>	<p>개인정보의 수집 시 동의 방법과 동일한 방법으로 동의를 받아야 한다. 단, 정보통신서비스의 제공에 관한 계약의 이행을 위하여 필요한 경우 상기 통지 또는 개인정보취급방침의 규정에 따라 이용자에게 필요한 사항을 공개한 경우는 동의 절차를 거치지 않을 수 있다.</p>	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				개인정보 취급 위탁 시 수탁업체 변동 또는 위탁업무 범위 및 계약상의 변동사항이 발생할 경우 이용자로부터 별도의 동의절차를 거치고 있는가?	개인정보 취급 위탁 시 위탁업체 변동 또는 위탁업무 범위 및 계약상의 변동사항이 발생할 경우 이용자로부터 별도의 동의절차를 거치고 있는가?	필수	○
		2.3.2 위탁자 책임	개인정보의 위탁 시 위탁사는 수탁사가 안전하게 개인정보를 취급하도록 관리 감독하여야 하며, 수탁자가 법령 규정을 위반한 경우 처리절차가 있어야 한다.	위탁사는 개인정보 취급 목적을 미리 정하고, 수탁사가 취급목적 외의 개인정보를 취급하지 않도록 관리하는가? 수탁사가 개인정보취급 시 개인정보를 위반하였을 경우 처리 및 배상에 관한 절차가 있는가?	위탁사는 개인정보 취급 목적을 미리 정하여야 하며, 수탁사는 이 목적을 벗어나서 이용자의 개인정보를 취급하지 않아야 한다. 위탁사는 수탁사가 개인정보를 위반하였을 경우 수탁사를 소속직원 등으로 보아 배상책임을 져야 한다.	필수	○
		2.3.3 외부위탁 관리 특	외부위탁 업체가 계약서 및 서비스 수준 협약에 명시된 사항을 충분히 이행하는지 상시 관리 감독하고 주 기적으로 점검 또는 감사하여야 한다.	수탁업체로부터 개인정보 보호와 관리상황을 정기적으로 보고 받고, 정기 또는 시점검을 통해 관리감독하고 있는가?	외부위탁 업체의 요구사항 준수여부를 정기적으로 보고 받고 관리 감독하며, 정기 및 수시점검 또는 감사를 수행하여야 한다.	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				개인정보 취급 위탁 시 수탁사 직원에 대한 보안교육을 하고 있는가?	개인정보시스템 구축 및 운영, 관리업무, 개인정보 취급업무 등을 위탁하는 경우 수탁사 직원에 대한 보안교육 사항이 마련되어 있어야 한다.	필수	
				수탁사 및 외부로부터의 개인정보처리시스템 접근내역을 기록하고 남기고 있는가?	수탁사 및 외부로부터의 개인정보처리시스템 접근내역을 기록하고 남기고 있는가?	필수	
				개인정보 위탁계약 종료 시 개인정보를 회수·파기하고 있는가?	개인정보 위탁계약 종료 시 개인정보를 회수·파기하고 있는가?	필수	
		위부위탁 계약 관련 연사항	신청기관의 개인정보 업무를 외부 위탁하는 경우에는 개인정보보호에 관한 요구사항 및 관리감독에 관한 사항을 계약서 및 서비스 수준 협약서 상에 명시하여야 한다.	외부위탁 계약 시 개인정보 보호에 관한 요구사항을 사전에 분석하였는가?	개인정보 처리의 위탁 종료 시 수탁업체로부터 개인정보를 회수·파기하는 절차를 수립하여 이행하여야 한다. 외부위탁 계약 시 아래와 같은 개인정보보호에 관한 요구사항을 사전에 분석하여야 한다. - 기술적·관리적 보호의무 - 이용자정보에 관한 비밀유지 - 이용자정보의 제 3자 제공 금지	필수	
		2.3.4				필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	관련 근거 여부	
					<ul style="list-style-type: none"> - 처리 종료 후의 이용자정보의 반환 또는 파기 등의 규정 - 이용자정보 취급 현황 및 이용자정보 보호 활동에 대한 주기적인 보고 - 위탁자의 점검·이행점검에 대한 적극적인 대응 및 관련 근거자료 제출 의무 - 사고시의 책임부담 - 위탁처리 기간 등 			
				외부위탁 계약시 개인정보 보호와 관련한 법적 요건 및 조직의 개인정보보호정책을 만족하기 위한 요구사항을 계약서상에 명시하였는가?	법적으로 위탁자는 수탁자가 개인정보보호 규정을 위반하지 않도록 관리 감독하여야 하며 수탁자가 업무와 관련된 하여 손해를 발생시킨 경우 위탁자가 배상하도록 하고 있으므로 이에 대한 조치가 필요하다.	필수	○	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
	2.4 제3자 제공시 동의를 득하고, 제3자에게 제공한 개인정보에 대한 보안관리 방안을 마련하여야 한다.	제3자 등 공시의	이용자의 개인정보를 제3자에게 제공하는 경우 모든 사항에 대하여 이용자에게 알리고 동의를 얻어야 한다.	외부위탁 계약서는 수탁사의 의무 및 책임에 대하여 아래의 내용을 포함하고 있는가? - 개인정보보호책임자 지정 - 정기적인 관리현황 보고 - 위탁사에 의한 이행점검 - 개인정보 침해 발생 시 대책 및 책임관계 관련 조항	외부위탁 계약서는 책임자의 지정, 정기 및 사안 발생 시 수시로 보고 또는 이행점검, 교육 시행 등의 관리 감독 조치, 침해사고 발생 시 책임 소재 및 손해배상 등의 항목을 포함하여야 한다.	필수	
	2.4 제3자 제공시 동의를 득하고, 제3자에게 제공한 개인정보에 대한 보안관리 방안을 마련하여야 한다.	제3자 등 공시의	이용자의 개인정보를 제3자에게 제공하는 경우 모든 사항에 대하여 이용자에게 알리고 동의를 얻어야 한다.	이용자의 개인정보를 제3자에게 제공하는 경우 다음 사항에 대하여 이용자의 알리고 동의를 얻는가? 1. 개인정보를 제공하는 자 2. 개인정보를 제공받는 자의 개인정보 이용 목적 3. 제공하는 개인정보의 항목 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용기간	이용자의 개인정보를 제3자에게 제공하는 경우에는 법에서 규정한 경우가 아니면 반드시 이용자에게 알리고 동의를 받아야 한다.	필수	0

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				동의받지 않은 개인정보를 제3자에게 제공하는 경우는 법적으로 허용된 경우이며, 제공내역을 기록하고 개인정보관리책임자 또는 의사결정자의 승인을 얻는가?	동의받지 않은 개인정보를 제3자에 제공할 수 있는 경우는 다음과 같다. - 서비스의 제공에 따른 요금 정산을 위하여 필요한 경우 - 법률에 특별한 규정이 있는 경우	필수	
				개인정보의 제3자 제공과 관련하여 사전에 이용자에게 고지한 사항 중 변경이 발생한 경우 이용자에게 알리고 동의를 얻는가? 제3자 개인정보 제공에 대한 동의방법은 개인정보 수집 시 동의방법과 동일한 방법을 사용하고 있는가?	개인정보의 제3자 제공과 관련하여 사전에 이용자에게 고지한 사항 중 변경이 발생한 경우 이용자에게 알리고 동의를 얻어야 한다. 제3자 개인정보 제공에 대한 동의방법은 개인정보 수집 시 동의방법을 준수하여야 한다. 1. 인터넷 사이트에 동의 내용을 게재하고 이용자가 동의 여부를 표시 2. 동의 내용이 기재된 서면을 이용자에게 직접 교부하	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수여부	법규거부	
					<p>거나, 우편 또는 모사전송을 통하여 전달하고 이용자가 동의 내용에 대하여 서명날인 후 제출</p> <p>3. 동의 내용이 기재된 전자우편을 발송하여 이용자가 기재된 동의의 의사표시가 기재된 전자우편을 전송받음</p> <p>4. 전화를 통하여 동의 내용을 이용자에게 알리고 동의를 얻거나 인터넷주소 등 동의 내용을 확인할 수 있는 방법을 안내하고 재차 전화통화를 통하여 동의를 얻는 방법(개인정보 수집 매체의 특성상 동의 내용을 전부 표시하기 어려운 경우 이용자에게 동의 내용을 확인할 수 있는 방법(인터넷주소·사업장 전화번호 등)을 안내하고 동의를 얻을 수 있다.</p>			

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		2.4.2 제공받은 개인정보를 타 기관의 정보로부터 제공받은 경우 관리 정보의 관련 제공받은 목적으로 사용하지 않아야 하며, 제3자에게 제공하지 않아야 한다.	개인정보를 제공받은 경우 목적 외의 용도로 사용하지 않아야 하며, 제3자에게 제공하지 않아야 한다.	개인정보를 제공받은 경우 제공받은 목적 외의 용도로 사용하지 않는가?	제공받은 개인정보는 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우를 제외하고는 제공받은 목적 외의 용도로 사용하지 않아야 한다.	필수	○
		2.4.3 제3자 보	제3자에게 개인정보에 대한 접근을 제공하는 경우 절차에 따라 통제하여야 한다.	개인정보에 대한 제3자의 접근을 통제하고 기록하며 정기적으로 기록을 검토하고 있는가?	제공받은 개인정보는 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우를 제외하고는 다시 제3자에게 제공해서는 안된다.	필수	○
		2.4.3 제3자 보 인관리	제3자에게 개인정보에 대한 접근을 제공하는 경우 절차에 따라 통제하여야 한다.	개인정보에 대한 제3자의 접근을 통제하고 기록하며 정기적으로 기록을 검토하고 있는가?	제공받은 개인정보는 이용자의 동의에 따라 개인정보를 제공할 경우 사안 별 적법성을 확인하고 승인 및 기록을 남기는 등의 절차가 마련되어야 한다.	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				제3자에게 개인정보 제공 시 안전한 절차에 따르도록 하며, 제공 내역을 기록하여 남기고 있는가?	이용자 본인 또는 법정 대리인 이 요청할 경우 이용자의 개인 정보에 대한 제3자 제공 내역을 제공할 수 있어야 한다.	필수	
		제3자 제 공 시 관련 계약 사항	제3자에게 개인정보 제공 또는 개인정보에 대한 접근을 경 우, 제3자가 제공하는 개인정보의 개인정보보호정책 준수 및 법적 요건을 만족하기 위한 방안을 마련하여야 한다.	제3자에게 개인정보 또는 개인정보에 대한 접근을 제 공할 경우, 제공하는 사업자의 개인정보보호정책 준수 및 법적 요건을 포함하여 체결되었는가?	공식계약 시 신청사업자와 제3자간의 계약종료 또는 제 공 기관과 이용자와의 계약 종료 또는 이용자 요청 시 이용자의 개인정보 이용 중지 및 삭제 등 제3자가 준수 해야 할 정책 및 보안요건의 준수 의무와 위반 시 손해배 상 등의 조항이 포함되어야 만 추후 문제 발생 시 책임 소재 규명 및 명확한 처리가 가능하다.	필수	
		2.4.4					

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
	2.5	양도, 양수, 합병 등 개인정보 이전 시 적절한 조치를 취하여야 한다.		제3자에 개인정보를 제공 후에도 보안요구사항이 준수될 수 있도록 이 와 관련된 항목을 계약서 상에 명시하고 있는가?	제3자의 요구사항 준수 여부를 정기보고, 감독 등을 통하여 지속적으로 점검하고 필요시 감사 등 적절한 조치를 수행하여야 한다. 단, 계약관계 상의 사유로 위 활동에 어려움이 있는 경우 계약서 상에 관련 조항을 명시하여야 한다.	필수	○
	2.5.1	개인정보를 이전하는 경우 보호 조치를 취하여야 한다.	영업의 양도, 합병 등으로 개인정보를 이전할 경우에는 필요한 사항을 이용자에게 미리 통지하는가?	영업의 양도, 합병 등으로 개인정보를 이전하려는 경우 전자우편, 서면, 팩스, 전화 또는 이와 유사한 방법으로 통지하는가?	영업의 양도, 합병 등으로 개인정보를 이전하려는 경우 전자우편, 서면, 팩스, 전화 또는 이와 유사한 방법으로 통지하여야 한다. 단, 정보통신서비스제공자 또는 영업양수자	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부	
					등이 과실 없이 이용자의 연락처를 알 수 없는 경우에 해당되어 위의 방법에 따라 통지할 수 없는 경우에는 인터넷 홈페이지에 최소 30일 이상 게시하여야 한다. 천재·지변 그 밖에 정당한 사유로 홈페이지 게시가 곤란한 경우에는 「신문 등의 자유와 기능보장에 관한 법률」에 따른 전국을 보급지역으로 하는 둘 이상의 일반일간신문(이용자의 대부분이 특정 지역에 거주하는 경우에는 그 지역을 보급구역으로 하는 일간신문)에 1회 이상 공고하는 것으로 갈음할 수 있다.			
		2.5.2 개인정보 영업을 이행을 위한 경우 적절한 조치	영업의 양도, 합병 등으로 개인정보를 이전하는 경우 적절히 조치하여야 한다.	양도자가 이전한 사실을 통지하지 않고 영업을 양도, 합병 등으로 개인정보를 이전했다면, 지체없이 그 사실을 이용자에게 통지하였는가?	영업의 양도, 합병 등으로 개인정보를 이전하는 경우 지체없이 그 사실을 이용자에게 통지하며, 양도자가 미리 이전 사실을 통지한 경우에는 하지 않아도 된다.	필수	0	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
2.6	개인정보를 해외로 이전하는 경우 적절한 보호조치를 취해야 한다.	해외 이전 시 보호조치	개인정보를 해외로 이전하는 경우 적절한 보호조치를 취해야 한다.	영업의 양도, 합병 등으로 개인정보를 이전받은 경우 양도자가 이용자의 개인정보를 이용하는 목적을 명시한 개인정보처리방침을 수립하고, 영업의 양도, 합병 등으로 개인정보를 이전받은 자가 이용자의 개인정보를 제공하는 목적 범위 안에서만 개인정보를 이용하거나 제공하는가?	양수자는 양도자가 이용자의 개인정보를 이용할 수 있는 당초의 목적 범위를 초과하여 개인정보를 이용하거나 제공하여야 한다.	필수	○
				개인정보의 해외 이전 시 국외로 이전하는 경우 국내법 및 해당 국가의 법적 요건을 만족하는 공식적인 계약을 체결하여야 하는가?	이용자의 별도의 동의는 얻지 않은 경우에는 동의받은 목적 범위를 초과하여 제공하거나 제공할 수 있다.	필수	○
2.6.1	개인정보를 해외로 이전하는 경우 적절한 보호조치를 취해야 한다.	해외 이전 시 보호조치	개인정보를 해외로 이전하는 경우 국내법 및 해당 국가의 법적 요건을 만족하는 공식적인 계약을 체결하여야 하는가?	개인정보의 해외 이전 시 수집된 개인정보를 국외(본사 등)로 이전할 계획이 있다면 이에 대한 사항을 정보주체에게 미리 고지하고 동의를 얻어야 하는가?	개인정보를 해외로 이전하는 경우 국내법 및 해당 국가의 법적 요건을 만족하는 공식적인 계약을 체결하여야 한다.	필수	○
				개인정보의 해외 이전 시 수집된 개인정보를 국외(본사 등)로 이전할 계획이 있다면 이에 대한 사항을 정보주체에게 미리 고지하고 동의를 얻어야 하는가?	개인정보를 해외로 이전하는 경우 국내법 및 해당 국가의 법적 요건을 만족하는 공식적인 계약을 체결하여야 한다.	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
3. 개인정보 파기 조치	3.1	신청사업자는 개인정보 파기 내부규정을 마련하고 이에 따라 개인정보의 수집 목적이 달성된 경우 개인정보를 안전하게 방법으로 지체없이 파기하여야 한다.	개인정보 수집된 개인정보는 안전하게 저장 및 관리 하여야 하며 정확성을 유지 하여야 한다.	개인정보의 해외 이전 시 분실, 도난, 누출, 변조, 훼손을 막을 수 있는 안전한 방법으로 이전하고 있는가? 해외 이전된 개인정보에 대해 기술적, 관리적 보호조치를 취하고 있는가?	전송 또는 이전 중 개인정보의 분실, 도난, 누출, 변조, 훼손을 막을 수 있는 암호화 등의 조치를 취하여야 한다. 해외에서 저장, 처리되는 개인정보에 대하여 해당 국가의 법적 요건 뿐만 아니라 국내법의 법적 요건을 만족하여야 한다.	필수	
	3.1.1	개인정보 및 관리	개인정보 수집된 개인정보는 안전하게 저장 및 관리 하여야 하며 정확성을 유지 하여야 한다.	수집된 개인정보는 정확하고 최신의 상태로 유지되는가? 수집된 개인정보는 정확하고 최신의 상태로 유지되어야 한다. 단, 개인정보 수집 항목이 최소 (이름, 주민번호, 이메일)일 경우 정기적인 프로세스가 없더라도 최신의 상태를 유지하는 것으로 본다.	수집된 개인정보는 정확하고 최신의 상태로 유지되어야 한다. 단, 개인정보 수집 항목이 최소 (이름, 주민번호, 이메일)일 경우 정기적인 프로세스가 없더라도 최신의 상태를 유지하는 것으로 본다.	필수	○

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		3.1.2	개인정보의 보유기간 및 파기 관련 내부 규정이 마련되어야 한다.	수집 및 취급하는 개인정보의 보유기간 및 파기 관련 내부 규정이 존재하는가?	수집한 개인정보 및 개인정보가 기입된 서류 등의 저장 및 보유기간, 파기 및 파기책임자 지정 등에 관한 내부 규정이 마련되어 있어야 한다.	필수	
		3.1.3	개인정보가 저장된 매체, 문서 등은 서비스 이용계약 해지 등 개인정보의 수집 목적에 달성된 경우 이를 지체없이 파기해야 한다.	개인정보의 수집 및 이용목적에 개인정보가 저장된 매체가, 문서 등은 서비스 이용계약 해지 등 개인정보의 수집 목적에 달성된 경우 이를 지체없이 파기하는가?	이용자의 동의를 얻은 개인정보의 보유 및 이용기간이 종료한 경우 지체없이 개인정보를 파기하여야 한다. 1. 정보통신서비스의 제공에 관한 계약의 이행을 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상의 동의를 받는 것이 현저히 곤란한 경우 2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우에는 동의없이 수집할 수 있다. 이 경우에도 각각의 목적을 달성한 경우 지체없이 파기하여야 한다.	필수	0

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
				<p>사업을 폐지하는 경우 지체 없이 개인정보를 파기하는가?</p> <p>개인정보를 파기하여야 하 는 경우, 위탁 또는 제3자에 게 제공한 개인정보도 함께 지체없이 파기하는가?</p>	<p>사업을 폐지하는 경우 지체 없이 개인정보를 파기하여야 한다.</p> <p>위탁업체 또는 제3자에게 제3자의 파기이행여부를 직 접 확인하기 어려운 경우 계 약서 상에 파기 관련 조항을 명시하여야 한다.</p>	필수	○
		3.1.4 파기방법	<p>개인정보는 안전한 방법으로 파기하여야 한다.</p>	<p>저장 매체에 저장된 개인정보 복구할 수 없는 방법으로 파기하였는가?</p> <p>종이문 종이문 용이문서의 경우 쇄절, 소각 등을 통해 파기하였는가?</p>	<p>개인정보를 파기할 경우 복 구할 수 없는 방법으로 파기 하여야 한다.</p> <p>종이문서의 경우 쇄절, 소각 등 재생활 수 없는 방법을 이용하여 파기하여야 한다.</p>	필수	○
				<p>개인정보 파기일자, 파기사 실 등에 대해 정기적으로 확인하고 검토하는가?</p>	<p>파기일자 후 파기책임자가 실제로 파기하였는지를 확인 하여야 한다.</p>	필수	

도메인	통제목적	통제사항	통제내용	점검항목	설명	필수 여부	법률 근거 여부
		3.1.5 목적 후 사유	개인정보의 수집목적 달성 후에도 개인정보를 관련 법령 등에 의해 일부 또는 전부를 보유한다면 정보주체에게 보유기간, 목적, 보유기간 및 항목에 대해 고지하거나 약관에 명시하고 최소한의 항목으로 제한하여야 한다.	개인정보의 수집목적 달성 된 경우에도 개인정보의 전부 또는 일부를 보유한다면 보유기간, 보유목적, 보유기간 및 보유항목에 대해서 정보주체에게 이를 고지하거나 이용약관 등에 명시하고 있는가? 개인정보의 수집목적 달성 후에도 개인정보의 일부 또는 전부를 보유해야 할 경우, 보유하는 개인정보의 항목을 보유목적에 맞는 최소한의 항목으로 제한하고 있는가? 개인정보의 수집목적 달성 된 경우에도 개인정보의 전부 또는 일부를 보유한다면 별도의 해지고객 DB에 보관 하도록 하고 있는가? 해지고객 DB에 보유하는 개인정보에 대한 접근권을 최소한의 인원으로 제한하고 있는가?	개인정보의 수집목적이 달성 된 경우에도 개인정보의 전부 또는 일부를 보유한다면 보유기간, 보유목적, 보유기간 및 보유항목에 대해서 정보주체에게 이를 고지하거나 이용약관 등에 명시해야 한다. 서비스 이용약관 해지 등 개인 정보의 수집목적이 달성된 경우 관련 법령 등에 의해 개인 정보의 일부 또는 전부를 보유해야 할 필요가 있다면, 보유하는 개인정보의 항목을 필요 하는 개인정보의 항목을 필요 최소한으로 제한해야 한다.	필수	
						필수	
						필수	

개인정보보호 관리체계 인증준비 안내서(사업자용) - 부록편 -

2010 년 12월 인쇄

2010 년 12월 발행

- 발행인 : 서 종 렬
- 발행처 : 한국인터넷진흥원
서울시 송파구 가락동 79-3번지
대동빌딩 한국인터넷진흥원
Tel: (02) 405-5118
- 인쇄처 : 호정씨앤피
Tel: (02) 2277-4718

〈비매품〉

- 본 안내서 내용의 무단 전재를 금하며, 가공·인용할 때에는 반드시 한국인터넷진흥원 『개인정보보호 관리체계 인증준비 안내서』라고 출처를 밝혀야 합니다.

《 한국인터넷진흥원(KISA) 『118 안내서·해설서』 시리즈 》

분류	안내서·해설서	해당팀명	발간년월	대상	수준
인터넷 진흥	DNS 설정 안내서	시스템관리팀	'09.	IT시스템관리자	중급
	인터넷주소분쟁해결 안내서	도메인팀	'10.3	일반	초급
	모바일 RFID코드 및 OID기반 RFID코드 적용 안내서	무선인터넷팀	'09.8	IT기업개발자	중급
	13.56MHz대역의 OID적용을 위한 마들웨어 개발 안내서	무선인터넷팀	'09.12	IT기업개발자	중급
인터넷이용 활성화	공공기관 IPv6 적용 안내서	IP팀	'08.12	IT시스템관리자	중급
	본인확인제 안내서	인터넷윤리팀	'09.2	일반·업무관계자	중급
정보보호 시스템 관리	본인확인제 완화 안내서	인터넷윤리팀	'09	일반	초급
	정보보호 사전진단 수행안내서	인터넷서비스보호팀	'10.4	IT시스템관리자	중급
	정보보호수준평가 방법론 안내서	인터넷서비스보호팀	'07.8/'10.3	IT시스템관리자	중급
	BcN주요장비별 정보보호 안내서	인터넷서비스보호팀	'07/'10.1	IT시스템관리자	중급
	침해사고 분석절차 안내서	해킹대응팀	'10.1	IT시스템관리자	고급
	웹서버구축 보안점검 안내서	웹보안지원팀	'10.1	IT시스템관리자	고급
	웹어플리케이션 보안 안내서				
	홈페이지 개발보안 안내서	해킹대응팀	'10.1	일반	중급
	무선랜 보안 안내서				
	침해사고대응팀(CERT) 구축/운영 안내서	침해사고대응기획팀	'07.9	업무관계자	중급
	WebKnight를활용한 IIS 웹서버 보안 강화 안내서	웹보안지원팀	'09.6	IT시스템관리자	중급
	WebKnight 로그 분석 안내서				
	ModSecurity를 활용한 아파치 웹서버 보안 강화 안내서				
보안서버구축 안내서	개인정보보호기획팀	'08.7	IT시스템관리자	중급	
정보보호인증	IT보안성 평가인증 안내서	공공서비스보호팀	'09.12	일반·업무관계자	초급
기업 정보보호	정보보호 안전진단 해설서	기업보안관리팀	'08.4/'10.1	업무관계자	초급
	정보보호 안전진단 업무 안내서	기업보안관리팀	'10.1	업무관계자	초급
	정보보호관리체계 안내서	기업보안관리팀	'09.12	일반	초급
신규 서비스 정보보호	인터넷전화(VoIP) 침해사고 대응 안내서	융합보호R&D팀	'10.5	업무관계자	초급
	패스워드 선택 및 이용 안내서	융합보호R&D팀	'10.1	일반	초급
	암호이용 안내서	융합보호R&D팀	'07./'10.1	일반	중급
	IPv6운영보안 안내서	융합보호R&D팀	'06.12	IT시스템관리자	중급
	IPv6보안기술 안내서	융합보호R&D팀	'05.	일반	초급
	와이브로 보안기술 안내서	융합보호R&D팀	'06.8	IT시스템관리자	중급
	암호 알고리즘 및 키 길이 이용 안내서	융합보호R&D팀	'07	IT시스템관리자	중급
	(7업및7관리IT 정보자산 보호를 위한 암호정책 수립 기준 안내서	융합보호R&D팀	'07	IT기업개발자	중급
	(정보의 안전한 저장과 관리를 위한) 보자기억체 이용 안내서	융합보호R&D팀	'09	일반	초급
웹사이트 회원탈퇴 기능 구현 안내서	융합보호R&D팀	'06	IT시스템관리자	중급	
개인정보	개인정보의 기술적·관리적 보호조치 기준 해설서	개인정보보호기획팀	'09.9	업무관계자	중급
	위치정보의 보호 및 이용 등에 관한 법률 해설서	개인정보보호기획팀	'08.12	업무관계자	중급
	위치정보보호를 위한 관리적·기술적 보호조치 권고 해설서	개인정보보호기획팀	'08.11/'10.1	업무관계자	중급
	웹사이트 개발·운영을 위한 개인정보 안내서	개인정보보호기술팀	'09.11	IT기업 개발자 관리자	중급
	I-PIN 2.0 도입 안내서	개인정보보호기술팀	'09.7/'10.6	업무관계자	중급
	김대리, 개인정보보호 달인되기	이용자권익보호팀	'09.8	업무관계자	중급
스팸 인력양성	기업의 개인정보영향평가 수행을 위한 안내서	이용자권익보호팀	'09.1	업무관계자	중급
	사업자를 위한 불법스팸 방지 안내서	스팸대응팀	'08.9	일반, 업무관계자	초급
지식정보보안 신규일자리 창출사업 세부시행 안내서	KISA아카데미팀	'09	업무관계자	초급	

- 본 안내서·해설서는 한국인터넷진흥원 홈페이지(www.kisa.or.kr)자료실에서 내려 받으실 수 있습니다.

 이 책을 볼 수 있는 독자는?



한국인터넷진흥원

138-950 서울시 송파구 가락동 79-3번지 대동빌딩
Tel. 405-5118 Fax. 405-5119
www.kisa.or.kr