2020년 하반기 개인정보처리업무 수탁업체 교육

2020. 12

삼성화재

CONTENTS

1. 개인정보보호법률(개정)

삼성화재

개인정보보호법제 최신동향(1)-법개정

개인정보 처리 범위 확대 - 목적 중심적 해석에서 목적 합치적 해석으로 확대

[개인정보보호법 개정]

제15조 (개인정보의 수집 · 이용)

③ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다.

제17조 (개인정보의 제공)

④ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보 주체의 동의 없이 개인정보를 제공할 수 있다

개인정보 처리 범위 확대 – 목적 합치적 처리를 위해 대통령령으로 정하는 사항

[시행령]

제14조의2(개인정보의 추가적인 이용 · 제공의 기준 등) ① 개인정보처리자는 법 제15조제3항 또는 제17조제4항에 따라 정보주체의 동의 없이 개인정보를 이용 또는 제공(이하 "개인정보의 추가적인 이용 또는 제공"이라 한다)하려는 경우에는 다음 각 호의 사항을 고려해야 한다.

1. 당초 수집 목적과 관련성이 있는지 여부
2. 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부
3. 정보주체의 이익을 부당하게 침해하는지 여부
4. 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

삼성화재

사례로 살펴보는 개인정보 처리

처리단계별 주요조치

개인정보보호법령 구성

수집 이용	저장 관리	제공 위탁	파기
• 개인정보 수집이용 • 개인정보 수집의 제한 (필요 최소한의 정보수집 등) • 14세 미만자 법정대리인 동의 • 민감정보 및 고유식별정보 처리제한(주민번호 수집 법정주의 도입)	• 인터넷상 주민번호 이외의 회원가입 방법 제공 • 영상정보처리기기 설치운영, 개인정보처리방침 공개 • 개인정보보호책임자 지정 • 개인정보 안전성 확보조치	• 개인정보의 제3자 제공, 목적외 이용제공 금지 • 개인정보 처리위탁, 영업양도 등 개인정보 이전	• 개인정보 파기 - 전자적 파일 복원이 불가능한 방법 영구 삭제 - 인쇄물 등 · 파쇄 또는 소각 (기타 세부 사항 행정안전부 질의 고시)

개인정보보호법제 최신동향(1)-법개정

민감정보 범위 확대

2. 업무 위수탁 관련 법규

사례로 살펴보는 개인정보 처리

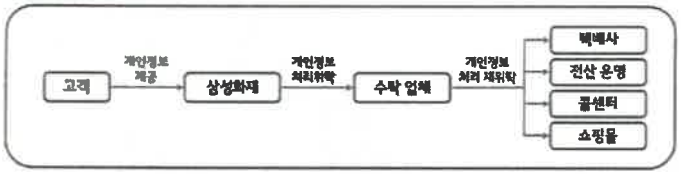
개인정보보호법률(개정)의 체계

개인정보보호법 : 본문 10장 70여개 조문 부칙

항목	세부 내용
제1장 총칙	• 목적, 정의, 개인정보보호원칙, 다른 법률과의 관계 등
제2장 개인정보 보호정책의 수립 등	• 개인정보보호위원회, 기본계획·시행계획 수립, 개인정보보호지침, 개인정보보호 관리수준 및 실태평가,자율규제촉진 등
제3장 개인정보의 처리	• 신설 : 제3절 기명정보의 처리에 관한 특례(제28조의 2~제28조의 7) • 수집·이용·제공 등 처리기준, 민감정보·고유식별정보(주민등록번호)제한, 영상정보처리기기 제한 등
제4장 개인정보의 안전한 관리	• 안전조치의무, 개인정보파일 등록·공개, 개인정보영향평가, 유출통지제도 등
제5장 정보주체의 권리 보장	• 열람요구권, 정정·삭제요구권, 처리정지요구권, 권리행사방법 및 절차, 손해배상책임 등
제6장 정보통신서비스 제공자 등의 개인정보 처리 등 특례	• 수집·이용 동의 등/유출 등의 공지·신고/보호조치/ 파기/ 이용자의 권리 등에 대한 특례
제7장 개인정보 분쟁조정위원회	• 분쟁조정위원회 설치·구성, 분쟁조정의 신청방법·절차, 효력, 집단분쟁조정제도 등
제8장 개인정보 단체소송	• 단체소송 대상, 소송허가요건, 확정판결의 효력 등
제9장 보칙	• 단체소송 대상, 소송허가요건, 확정판결의 효력 등
제10장 벌칙	• 벌칙, 몰수 추징, 과태료 및 양벌 규정 등
부칙	• 시행일, 경과조치, 다른 법률의 개정 등

개인정보처리 재위탁 등의

재위탁 개요



재위탁 사전동의 위반, 재위탁 관리감독 소홀로 인한 사고 발생 시

위탁사에서 재위탁 사전 동의 위반, 재위탁 관리감독 소홀로 인한 사고 발생 시 위탁사는 과태료, 위탁사는 과징금 처분※ 사고발생 시 민, 형사상 책임은 별도 존재 함.

개인정보보호법 제26조(업무위탁에 따른 개인정보의 처리 제한) 제1항

※ 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다

01 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항

02 개인정보의 기술적·관리적 보호조치에 관한 사항

03 위탁업무의 목적 및 범위

04 재위탁 제한에 관한 사항

05 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항

06 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항

07 법 제26조제2항에 따른 수탁자가 준수 하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

개인정보보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)제4항

※ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리 하는지를 감독하여야 한다

수탁자 선정

수탁자를 선정할 때에는 인력과 물적 시설, 재정 부담능력 등을 종합적으로 고려하여야 한다

수탁자 처리 업무 지연

개인정보처리자는 수탁자의 처리 업무의 지연, 처리 업무와 관련없는 불필요한 개인정보의 요구, 처리기준의 불공정 등의 문제점을 종합적으로 검토하여 이를 방지하기 위하여 필요한 조치를 마련해야 하여야 한다

위탁 개인정보 보호

수탁자는 위탁받은 개인정보를 보호하기위하여 「개인정보의 안전성 확보조치 기준」에 따라 관리적·기술적·물리적 조치를 하여야 한다

개인정보보호법 제26조에 따른 재위탁 제한에 관한 법률

개인정보보호법 제 9조(개인정보를 제공받은 자의 이용·제공 제한)

개인정보처리자로부터 개인정보를 제공받은 자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 개인정보를 제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공하여서는 아니 된다.

1 정보주체로부터 별도의 동의를 받은 경우

2 다른 법률에 특별한 규정이 있는 경우

개인정보보호법 제 26조 제5항(업무 위탁에 따른 개인정보의 처리 제한)

수탁자는 개인정보처리자로부터 위탁 받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니된다.

개인정보보호법 시행령 제28조 제 항 제2호(개인정보 처리 업무 위탁 시 조치)

법 제26조제1항 제3호에서 "대통령령으로 정한 사항"이란 다음 각 호의 사항을 말한다

재위탁 제한에 관한 사항

개인정보보호법 제29조(안전조치의무)

◦ 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다

01 내부관리계획의 수립·시행
02 접근권한의 관리
03 접근통제
04 개인정보의 암호화
05 접속기록의 보관 및 점검
06 악성프로그램 등 방지
07 물리적 접근 방지
08 개인정보의 파기

※ 출처 : 개인정보의 안전성 확보 조치 기준 (시행 2019.06.07) | (행정자치부고시 제2019-47호, 2019.06.07)

개인정보의 안전성 확보 조치 기준 소개

[관련 법령 참고]

[개인정보 보호법]

제24조(고유식별정보의 처리 제한)

① 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 조치를 하여야 한다

제24조의2(주민등록번호 처리의 제한)

② 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다

제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다

개인정보 유출이란?

◦ 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보 처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용한 경우

01 ◦ 개인정보가 포함된 서면, 이동식 저장장치, 휴대용컴퓨터 등을 분실 또는 도난당한 경우

02 ◦ 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우

03 ◦ 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우

04 ◦ 기타 권한이 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우

개인정보의 안전성 확보조치 기준 소개

[관련 법령 참고]

[개인정보 보호법]

제21조(고유식별정보의 안전성 확보 조치) 법 제24조제3항에 따른 고유식별정보의 안전성 확보조치에 관하여는 제30조를 준용한다.
이 경우 "법 제29조"는 "법 제24조제3항"으로, "개인정보"는 "고유식별정보"로 본다.

제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.

1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상당하는 조치
4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
5. 개인정보에 대한 보안프로그램의 설치 및 갱신
6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치

⑤ 보호위원회는 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.

⑥ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

제29조의5(가명정보에 대한 안전성 확보 조치)

① 개인정보처리자는 법 제28조의4제1항에 따라 가명정보 및 가명정보를 활용하는 과정에서 추가정보가 분리되어 별도로 보관·관리되는 등 추가정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 다음 각 호의 안전성 확보 조치를 해야 한다.

1. 제30조 또는 제40조의2에 따른 안전성 확보 조치
2. 가명정보와 추가정보의 분리 보관. 다만, 추가정보가 불필요한 경우에는 추가정보를 파기해야 한다.
3. 가명정보와 추가정보에 대한 접근 권한의 분리. 다만, 「소상공인 보호 및 지원에 관한 법률」 제2조에 따른 소상공인으로서 가명정보를 취급할 자를 추가로 둘 여력이 없는 경우 등 접근 권한의 분리가 어려운 정당한 사유가 있는 경우에는 업무 수행에 필요한 최소한의 접근 권한만 부여하고 접근 권한의 보유 현황을 기록으로 보관하는 등 접근 권한을 관리·통제해야 한다.

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

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

사회적 이슈와 개인정보보호 이슈의 연결

- N번방 사태와 공공기관 내 개인정보 오남용

경향신문

병무청, "N번방 정보유출 송구, 사회복무요원 개인정보 취급금지"

- 코로나19로 인한 감염자의 프라이버시 침해

"확진자 동선공개 '공익 · 사생활' 고려…집주소 · 직장명 비공개"

삼성화재

개인정보가 유출되면?

01 신속 통지

> 유출된 정보주체 개개인에게 지체 없이 통지

- 시 한 : 유출되었음을 알게 되었을 경우 지체 없이(5일 이내)
- 통지항목 : 1. 유출된 개인정보의 항목
  2. 유출 시점 및 그 경위
  3. 피해 최소화를 위한 정보주체의 조치방법
  4. 기관의 대응조치 및 피해구제 절차
  5. 피해 신고 접수 담당부서 및 연락처

02 긴급 조치

> 피해 최소화 위한 대책 마련 및 필요한 조치 실시

- 접속경로 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 피해를 최소화하기 위해 필요한 긴급 조치 이행
- 긴급 조치 이행 등에 어려움이 있는 경우 전문기관에 기술지원 요청

03 대량 유출

> 1만 명 이상 유출된 경우 유출 통지 결과를 신고하고 홈페이지에 공지

- 1만 명 이상 개인정보가 유출된 경우 유출 통지 및 조치 결과를 지체 없이 행정자치부 또는 전문기관(한국인터넷진흥원, www.privacy.go.kr)에 신고
- 1만 명 이상 개인정보가 유출된 경우 개별 통지와 함께 유출된 사실을 인터넷 홈페이지에 7일 이상 게재

삼성화재

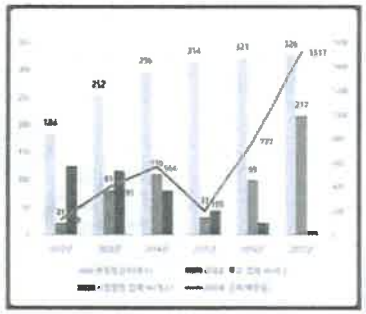
개인정보 침해 및 법 위반에 따른 처벌 수준 강화

- 법인은 물론 개인정보보호 관리 책임자에 대한 법적 책임의 강조(양벌 규정 적용)

MK

개인정보 49만여 건 유출… 본부장 벌금형

- 개인정보보호를 위한 자율 규제 유도와 지속적인 개인정보보호 법 위반 현장점검 병행



삼성화재

3. 개인정보 유출 사고 사례

삼성화재

최근 이슈

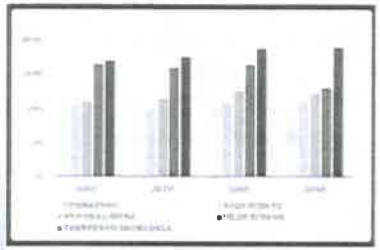
[참고] 유형별 개인정보 침해 신고 및 상담 접수 현황

접수 유형	2013년	2014년	2015년	2016년	2017년	2018년	2019년
개인정보 안전성 확보조치	4,518	7,404	4,006	2,731	1,768	2,549	2,630
개인정보 미파기	602	686	767	545	723	1,036	1,214
정보주체 권리(열람, 정정요구 등)	674	792	957	855	862	1,149	1,292
열람·정정을 수집보다 쉽게 해야 할 조치	510	352	381	286	266	364	222
이용 개인정보 수집	36	33	34	33	49	92	78
주민등록번호 등 타인정보 훼손·침해·도용	129,103	83,126	77,598	48,557	63,189	111,483	134,271
위 법 관련 개인정보 사례	35,284	57,705	60,480	38,239	30,972	37,156	8,745
계	177,736	158,908	152,151	98,210	105,122	164,497	159,255

개인정보 침해신고 유형 및 안전조치 미흡사항

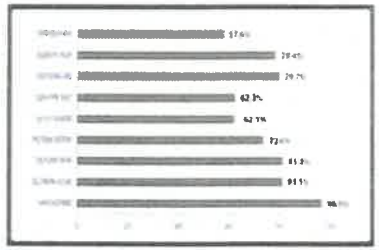
최근 4년간 개인정보 침해신고 및 상담 유형 TOP 5

- 주민등록번호 관련 피해신고와 상담이 가장 높은 비중으로 차지하고 있음
- 최근 개인정보의 목적 이용 또는 제3자 제공 관련 피해 신고와 상담이 증가하고 있음



개인정보 안전조치 분야별 미흡사항

- 개인정보보호 활동과 직접적으로 관련 안전조치 분야에서는 내부관리계획 미보유가 가장 큰 문제인 가운데 접근권한 관리, 접근통제 시스템의 미흡 등이 주요 이슈로 나타남



개인정보 유출 사례

'1억건 개인정보 유출' 금융사 3곳 벌금

1억건이 넘는 개인정보가 유출된 KB국민카드와 롯데카드, NH농협은행에 법정 최고형인 1000만원대의 벌금이 확정됐다.

대법원 2부(주심 노정희 대법관)는 개인정보보호법 위반 혐의로 기소된 이 세 금융사의 상고심에서 유죄로 판단한 원심을 확정했다고 14일 밝혔다. 이로써 KB국민카드와 농협은행은 1500만원, 롯데카드는 1000만원의 벌금을 각각 내게 됐다.

이 세 금융사는 2012~2013년 신용카드 부정사용예방시스템 개발을 위해 용역을 맡겼다. 이때 용역업체 프리아크레딧뷰로(KCB) 직원 박모씨는 개인정보가 허술하게 관리되고 있는 점을 파악하고 자신의 이동저장장치(USB)에 고객의 개인정보를 무작위로 옮겨 저장했다. 박씨는 2014년 징역 3년형을 선고받았다.

O 개인정보 암호화 미적용 및 이동저장매체(USB) 사용 통제 미흡

최근 이슈

[참고] 유형별 개인정보 침해 신고 및 상담 접수 현황

접수 유형	2013년	2014년	2015년	2016년	2017년	2018년	2019년
개인정보 수집 요건	2,634	3,923	2,442	2,568	1,876	2,764	3,237
개인정보 수집 시 고지·명시 의무	84	268	65	54	69	112	59
과도한 개인 정보 수집	1,139	1,280	868	330	681	553	605
목적외 이용 또는 제3자 제공	1,908	2,242	3,585	3,141	3,883	6,457	6,055
개인정보취급자에 의한 훼손·침해 등	1,022	1,036	857	822	484	425	383
개인정보 처리 위탁	44	40	22	25	73	141	139
영업 양도·합수	47	54	41	41	64	107	123
개인정보 보호책임자	51	39	46	123	165	169	197

4. 개인정보 유출 사고 대응 방안

개인정보 유출 사례

보험사도 뚫렸다... 손보 16만건 정보 유출

보험업계 첫 대규모 정보 유출에 금감원 중징계

(서울=연합뉴스) 심재훈 고유선 기자 = 시중은행, 카드사에 이어 보험사에서 해킹에 의해 16만여건에 달하는 대규모 고객 정보가 흘러나간 것으로 확인됐다.
금감원은 손보가 2010년 1월부터 2011년 5월까지
전산시스템에 대해 해킹 및 취약점에 대한 진단·분석, 공개용 서버에 대한 취약성, 무결점 점검을 하지 않는 등 자체 안전 대책에 소홀히 했다는 결론을 내렸다.
문제는 보험사가 은행 및 카드사와 달리 고객의 질병 내역 등 민감한 정보를 모두 갖고 있다는 점이다.
이런 정보가 흘러나가면 범죄에 악용될 소지가 커지게 된다.
IT 관련 규정 위배 시 과태료 부과, 최고경영자 문책 수위 강화, 정보책임자와 정보보안책임자 겸직 제한, 금융사 보안 수시 점검 등이 포함될 것으로 보인다.

- 업무처리시스템에 대해 취약점 진단 미수행
- 로그 기능 부재로 인한 사고원인 파악 불가

개인정보 유출 · 침해사고 예방을 위한 조치

예방 수칙

① 개인정보 최소 수집 및 파기
② 법률에서 요구하는 의무사항 이행
③ 관리자페이지는 반드시 보안설정
④ 주기적 점검(내부, 외부)은 필수

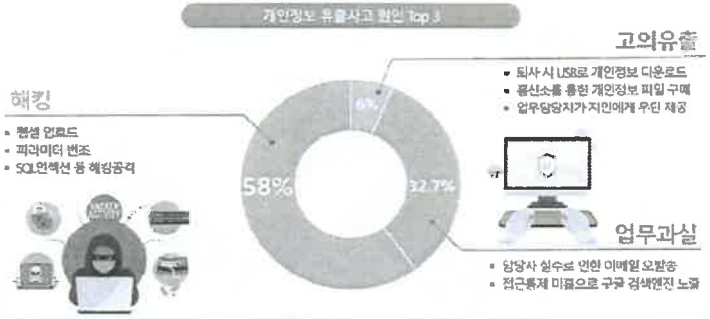
개인정보보호법 제29조(안전조치 의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

정보통신망법 제28조(개인정보의 보호조치)

정보통신서비스 제공자 등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다.

개인정보 유출 사례



- 지속적인 해킹 시도로 인한 정보 유출
- 내부 직원의 업무 목적 외 개인정보 유출
- 담당자 실수로 인한 개인정보 유출

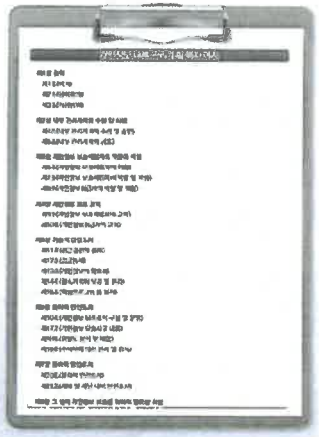
개인정보 안전성 확보 조치 기준

내부 관리 계획의 수립·시행

내부관리계획 구성

✓ **개인정보보호 조직의 구성 및 운영**

1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보취급자에 대한 교육에 관한 사항
4. 접근 권한의 관리에 관한 사항
5. 접근 통제에 관한 사항
6. 개인정보 암호화 조치에 관한 사항
7. 접속기록 보관 및 점검에 관한 사항
8. 악성프로그램 등 방지에 관한 사항
9. 물리적 안전조치에 관한 사항
10. 개인정보보호조직에 관한 구성 및 운영에 관한 사항
11. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
12. 위험도 분석 및 대응방안 마련에 관한 사항
13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항
14. 개인정보 처리 업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
15. 그 밖에 개인정보보호를 위하여 필요한 사항



개인정보 안전성 확보 조치 기준

내부 관리 계획의 수립·시행

○ 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사 결정 절차를 통하여 다음의 사항을 포함하는 내부 관리계획을 수립·시행

1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보취급자에 대한 교육에 관한 사항
4. 접근 권한의 관리에 관한 사항
5. 접근 통제에 관한 사항
6. 개인정보의 암호화 조치에 관한 사항
7. 접속기록 보관 및 점검에 관한 사항
8. 악성프로그램 등 방지에 관한 사항
9. 물리적 안전조치에 관한 사항
10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항
11. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
12. 위험도 분석 및 대응방안 마련에 관한 사항
13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항
14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
15. 그 밖에 개인정보 보호를 위하여 필요한 사항

○ 위의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리

○ 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리 계획의 이행 실태를 연1회 이상 점검·관리

개인정보 안전성 확보 조치 기준

내부 관리 계획의 수립·시행

내부관리계획 구성

✓ **개인정보보호 조직의 구성 및 운영**

1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항

[2020.8.5. 법령 개정에 따라 가명정보 처리 내부관리계획 포함 내용 예시]

- 가명정보 또는 추가 정보의 접근권한 관리책임자 지정에 관한 사항
- 추가 정보 별도 분리 보관
- 가명정보 또는 추가 정보의 안전성확보조치에 관한 사항
- 가명정보 처리 기록 작성 및 보관에 관한 사항
- 개인정보 처리방침 공개에 관한 사항
- 가명정보의 재식별 금지에 관한 사항

출처 : 개인정보보호위원회, 개인정보 가명처리 가이드라인(안) 참고, 2020.8

13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항
14. **개인정보 처리 업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항**
15. **그 밖에 개인정보보호를 위하여 필요한 사항**

개인정보 안전성 확보 조치 기준

내부 관리 계획의 수립·시행

내부관리계획 정의

✓ **"개인정보가 분실·도난·유출·위조·변조·훼손되지 않도록 안전하게 처리하기 위해 수립/시행하는 관리적 안전조치"**

✓ **전체에 통용되는 내부규정**

- 전사 차원의 개인정보보호 활동 계획
- 경영층의 주도적인 방향 제시와 지원 필수

✓ **개인정보 처리 및 보호 업무 기준**

- 최고경영층의 내부 결재 승인
- '내부규정'을 기초로 세부 지침 또는 안내서 마련/이행

제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.

1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행

개인정보 안전성 확보 조치 기준

접근 권한 관리

"접근권한이란 개인정보처리시스템에 접속, 업무처리/개인정보 생성·변경·열람·삭제 권한

- ✓ 개인정보처리시스템에 대한 접근 권한은 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여
- ✓ 전보, 퇴직 등의 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 접근 권한 변경 또는 말소
- ✓ 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 최소 3년간 보관
- ✓ 개인정보처리시스템의 사용자계정 발급 시 개인정보취급자 별로 발급하며, 다른 취급자와 공유되지 않도록 함
- ✓ 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성 규칙을 수립하여 적용
- ✓ 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근 제한 등 필요한 기술적 조치

개인정보 안전성 확보 조치 기준

내부 관리계획의 수립·시행

- ✓ **내부관리계획의 주요 변경사항 발생 시**
  - 즉시 반영 → 수정 → 시행 → 이력 관리
- ✓ **내부관리계획의 수정, 변경 사항**
  - 개인정보취급자들에게 전파 → 준수

내부관리계획의 이행 실태 점검/관리

- ✓ **역할 : 개인정보 보호책임자**
- ✓ **기간 : 연 1회 이상**
- ✓ **결과 보고**
  - 중대한 영향을 초래하거나 해를 끼칠 수 있는 사안 등 기관장(대표) 임원 보고
  - 대책 마련

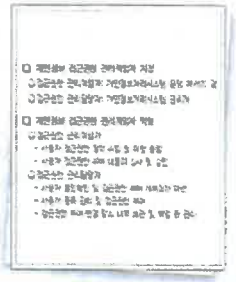
개인정보 안전성 확보 조치 기준

접근 권한 관리

접근권한 관리 체계

- ✓ **부서장이 사용자의 개인정보처리시스템 접근권한을 확인하는 절차**

- ✓ **권한 관리 절차**
  - 사용자 등록 : 사용자 ID 등록
  - 권한 부여 : 사용자별 업무범위에 맞도록 권한 부여
    - 1인1개 권한 부여 원칙 (필요시 2개 권한 부여 가능)
      ※ 개인정보 처리 내역에 대한 책임 추적성을 확보
      (예시) 사용자별 업무분장 선택 시 해당 업무만 수행하도록 제한 권한 부여
  - 권한 변경 및 중지
    - 인사이동, 조직 변경, 퇴직, 휴직, 병가 등 사용자 업무 변경·중료 시
      (예시) 권한 부여 이후 3개월간 로그인 이력이 없는 사용자는 권한 일괄 중지 및 사용자 ID 중지 처리



개인정보 안전성 확보 조치 기준(개정)

[사례] 내부 관리계획 미수립 위반

위반사항

- ✓ A병원은 30만건 이상의 개인정보를 수집·보관하고 있었으나,
- ✓ 유형에 따른 필수사항을 포함하지 않고 의무 업무와 관련된 내용만 내부관리계획으로 관리하고 있었음

조치사항

- ✓ 개인정보처리자 내부 의사 결정 절차를 통하여 내부 관리계획 수립·시행

조치 TIP • [illegible]

개인정보 안전성 확보 조치 기준

접근 권한 관리

접근권한 관리 절차 사례

∨ 접근 권한 관리

- 개인정보 접근권한 및 이용 내역 점검
- 정기점검 (반기별 1회)
  - 개인정보 접근권한 관리의 적절성 및 접근권한 오남용 여부 점검
  - 개인정보 유출 및 접근권한 부여의 적절성 등에 대해 점검
- 수시점검
  - 개인정보 유출사고 발생 시/예방 목적

개인정보 안전성 확보 조치 기준

접근 권한 관리

접근권한 관리 절차 사례

접근 권한 신청	접근 권한 부여	접근 권한 변경·점검
• 업무담당자	• 접근 권한 심사 (최초 부여시) • 접근 권한 부여 - 승인내역 기록관리	• 접근 권한 변경관리 (조직개편, 인사발령, 업무분장변경)



개인정보 안전성 확보 조치 기준

접근 권한 관리

접근권한 관리 절차 사례

접근 권한 관리 - 변경/말소

휴직자·퇴직자	업무변경자	부서 이동	장기미사용자
인사DB와 연동하여 시스템 권한 삭제	업무변경 전/후 시스템 권한 삭제/생성	매월1일 인사발령에 따라 부서코드 변경자의 시스템 권한 삭제 or 유지	30일 이상 접속 내역이 없을 경우 권한 변경 (중지 또는 삭제)

개인정보 안전성 확보 조치 기준

접근 권한 관리

접근권한 관리 절차 사례

∨ 접근 권한 신청 (공문처리)

- 개인정보의 이용·활용 목적, 근거
- 개인정보의 이용·활용 업무의 범위


개인정보 안전성 확보 조치 기준

접근 권한 관리

안전한 인증절차 및 인증방식

기술적 조치 방법

- 아이디 또는 비밀번호 일정 횟수 오입력 시 시스템 접근 제한
  ※개인정보처리시스템에 권한 없는 자에 의한 비정상적인 접근 방지 목적

- 비인가자에 대한 접근 권한 통제 방안 사례
  - (예시 1) 아이디나 비밀번호를 5회 이상 잘못 입력한 경우 사용자계정을 잠금
  - (예시 2) 아이디와 비밀번호 입력 외 추가 인증수단 (공인인증서, OTP 등)을 적용하여 정당한 접근 권한자임을 확인
  - (예시 3) 개인정보취급자에게 개인정보처리시스템에 대한 접근을 재부여하는 경우에도 반드시 개인정보취급자 이부를 확인 후 계정 잠금을 해제

개인정보 안전성 확보 조치 기준

접근 권한 관리

접근권한 점검 항목 (예시)

- ✓ root 계정은 원격 접속 제한
- ✓ 시스템 별로 접근 가능한 관리자 지정/업무 목적에 맞게 최소 권한 부여(1인 1계정)
- ✓ 시스템에 접근 가능한 중요 단말기 지정
- ✓ 시스템에 접근 시 암호화 연결(SSH, VPN 등) 적용
- ✓ 일정시간 사용이 없을 경우 세션 연결이 종료되도록 세션 타임아웃 설정
- ✓ 시스템 별로 다른 안전한 비밀번호 설정 및 갱신
  ※유추하기 어려운 비밀번호 설정(아이디, 호스트명, 연속 숫자 이용 금지 등 안전한 방법), 갱신 주기 설정, 오류 횟수 제한(5회) 등

개인정보 안전성 확보 조치 기준

접근 권한 관리

개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준

구분	구분
ID	• 접근 권한이 부여·변경·말소된 대상 ID
대상자 식별정보	• 사후에 해당 사용자를 확인할 수 있는 정보(이름, 부서명 등) ※ ID등을통해다른정보와결합하여추적이가능하다면별도로저장하지않을수있음
접근 권한 정보	• 부여·변경·말소된 접근 권한에 관한 정보(접근 권한명 등) ※ 조직별 그룹별 역할별 사용자별등 권한부여방식에따라 다양하게표현할수있지만 해당 접근 권한의상세내용(대상 메뉴/화면및 입력/조회/변경/삭제/생성/다운로드등 세부 권한을확인할수 있어야함
유형	• 접근권한 부여/변경/말소
신청사유	• 접근권한 부여·변경 또는 말소 사유(예 : 신규업사, 조직변경, 퇴사 등)
신청자 정보	• 해당 접근 권한의 신청자 ※외부자등에따라대리신청이가능한경우신청자정보를기록
신청일시	• 접근 권한의 부여·변경·말소를 신청한 일시(YYYYMMDD HH:MM:SS)
승인자 정보	• 해당 접근권한 신청에 대한 승인자 ※내부적으로접근권한승인절차가존재하는경우승인자정보를기록
승인일시 (적용일시)	• 접근 권한의 부여·변경·말소를 승인한 일시(YYYYMMDD HH:MM:SS)

개인정보 안전성 확보 조치 기준

접근 권한 관리

비밀번호 작성규칙

- ✓ **안전한 비밀번호 구성**
  - 8자리 이상 3종류 이상의 문자로 구성한다
  - 10자리 이상의 문자로 구성한다. 단, 숫자로만 구성할 경우 취약할 수 있음
- ✓ **예측이 어려운 비밀번호 설정방법**
  - 생일, 전화 번호, 잘 알려진 단어 등 예측하기 쉬운 문자열이 포함되지 않도록 한다
  - 영문자(대소문자), 숫자, 특수문자들을 혼합한 구성으로 설정하고, 알파벳 문자 앞 뒤가 아닌 위치에 특수문자 및 숫자 등을 삽입하여 설정한다.
- ✓ **비밀번호 변경**
  - 비밀번호가 제3자에게 노출되었을 경우, 새로운 비밀번호로 변경
- ✓ **동일 비밀번호 사용 제한**
  - 사이트별 비밀번호를 다르게 설정하는 등 여러 계정이나 시스템에서 동일한 비밀번호를 사용하지 않도록 한다

개인정보 안전성 확보 조치 기준

접근 권한 관리

✓ **접근 권한의 부여/변경/말소**

- 침해사고 발생 시 원인 분석 등을 위하여 접근 권한 관련 내역을 사후에 추적·검토할 수 있도록 접근권한 부여/변경/말소 내역을 저장

접근권한 내역 보관 기록 예시

번호	사용자ID	사용자명	권한명	권한ID	유형	일자	작업자	사유	...
...									
51503	Cskim	김철수	회원관리자	S0002	부여	20190220 10:22:01	Gdhong	담당업무 변경	...
51504	Yhkim	김영희	상담관리자	C0005	부여	20181210 09:50:33	Gdhong	상담팀 입사	...
51505	Yhkim	김영희	상담관리자	C0005	말소	20190423 13:55:20	Gdhong	퇴사	...

...

삼성화재 SAMSUNG

개인정보 안전성 확보 조치 기준

접근 권한 관리

✓ **계정관리 내역 기록**

- 개인정보취급자별 계정관리를 위해 계정관리 내역을 기록할 수 있음
  - 계정관리 내역으로는 개인정보취급자 정보, 계정상태(활성/비활성 여부 등), 계정 생성 삭제 비활성화 등 일시(YYYYMMDD HHMMSS) 등을 기록할 수 있음

계정 관리 내역 예시

아이디	이름	부서명	계정상태	처리일시	생성자	비활성화 일시	작업자
Gdhong	홍길동	IT팀	활성 (Y)	20190112 14:30:20	SYSTEM	-	
Cskim	김철수	IT팀	활성 (Y)	20190220 10:22:01	Gdhong	-	
Yhkim	김영희	고객팀	비활성 (N)	20190228 17:33:50	Gdhong	20190420 13:55:20	Gdhong

삼성화재 SAMSUNG

개인정보 안전성 확보 조치 기준

비정상 접근 및 장기 미접속시 계정 잠금

✓ **비정상 로그인 시도 추적**

- 실패한 인증시도에 대한 정보 기록을 통해 인증시도 실패를 추적할 수 있도록 구현
- 반복된 로그인 실패에 대한 로깅 정책을 설정하고 로그 저장을 통해 허용되지 않은 로그인 시도를 분석

✓ **장기 미접속자 계정 잠금**

- 미접속 기간 계산을 위하여 '마지막 로그인 시간'과, 계정 잠금 여부를 확인할 수 있는 '계정상태(활성/비활성 등)'등을 기록할 수 있음

✓ **비활성 계정 잠금 해제**

- 비활성화 계정에 대해 로그인 시도 시, 정상적인 사용을 위한 계정 잠금 해제 절차 및 기능을 마련
  - 예: 내부 승인 후 관리자가 계정 잠금 해제 처리

삼성화재 SAMSUNG

개인정보 안전성 확보 조치 기준

접근 권한 관리

✓ **접근 권한 설정**

- 접근 권한 설정 시, 아래의 내용을 참고하여 개인정보취급자에게 권한을 부여한다.

접근권한 설정 시 고려사

1. 개인정보처리시스템 기능(메뉴)별 개인정보 처리 내용을 식별
   ※ 조회, 쓰기, 수정, 삭제, 출력, 다운로드 등
2. 업무에 따라 최소한의 권한만 부여될 수 있도록 접근 권한 그룹 정의한다.
   (예: 최고관리자, 회원관리자, 게시판 관리자 등)
   ※ 접근 권한 형태는 사용자별, 조직별, 그룹별, 역할별 등 조직의 특성에 따라 설계 가능
3. 특히, 대량의 개인정보 유출 위험이 있는 '다운로드' 권한에 대해서는 업무상 필요한 경우로 한정하여 권한을 정의하는 것이 바람직함

삼성화재 SAMSUNG

개인정보 안전성 확보 조치 기준

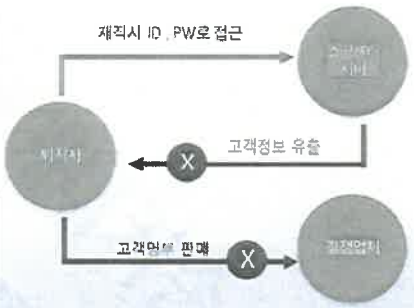
[사례] 퇴직자의 접근권한 방치

위반사항

- ✓ 퇴직한 직원의 계정이 방치되어 있는 상태에서 해당 계정으로 개인정보처리 시스템에 접근하여 개인정보 유출

조치사항

- ✓ 퇴직한 직원의 계정 접근권한 회수 사용중지 처리



개인정보 안전성 확보 조치 기준

일정시간 미입력시 자동 접속차단 기능 적용

✓ **개인정보처리시스템에 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 업무를 처리하지 않는 경우, 업무용 컴퓨터 등에서 해당 개인정보처리시스템에 대한 접속차단 조치를 해야 함**

- 단 업무용 컴퓨터의 화면잠금, 화면보호기 등은 접속차단에 해당하지 않음

✓ **개인정보를 처리하는 방법 및 환경, 업무특성 등을 고려하여 적정한 시스템 접속차단 시간을 결정**

- 시스템 접속 차단 시간은 최소한(일반적으로 10~30분 이내)으로 정하는 것을 권장

개인정보 안전성 확보 조치 기준

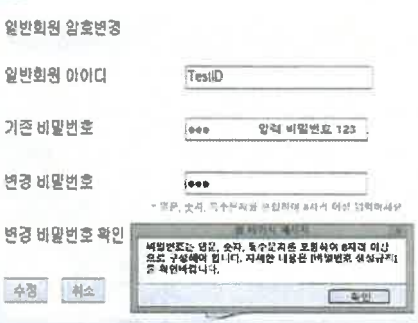
[사례] 비밀번호 작성 규칙 미수립 위반

위반사항

- ✓ B업체는 호텔·콘도·스키장·골프장 등 종합 레저 사업을 하는 업체로, 개인정보처리 시스템을 도입해 개인정보를 저장·운용하고 있다.
- ✓ 그러나 B업체는 개인정보처리 시스템 로그인 할 때 비밀번호 작성 규칙 수립 및 적용이 되어 있지 않았다.

조치사항

- 비밀번호 작성 규칙 수립 및 적용 (비밀번호는 문자, 숫자 등으로 조합·구성)



조치 TIP

- 암호 사용을 위한 클라이언트(https://kcert.kisa.or.kr)의 자동화 "패스워드 선택 및 이용규칙" 암호화방식을 기술적 강제 스크립트로 활용

개인정보 안전성 확보 조치 기준

[사례] 접근권한 부여, 변경, 말소 이력 보관 미흡

위반사항

- ✓ A사는 생활용품을 개발·제조·판매하는 온라인 쇼핑몰을 운영하고 있음
- ✓ 쇼핑몰 회원 가입시 고객들의 개인정보를 수집하였고 이를 관리하는 개인정보보호 담당자를 지정·관리하고 있었음
- ✓ 개인정보보호 담당자에게 권한을 부여·수정·삭제한 이력에 대해서 최근 1년의 내역만 보관하고 있었음

조치사항

- 개인정보처리자는 개인정보보호 담당자 권한 부여·변경·말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관

개인정보 안전성 확보 조치 기준

접근 통제

- 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등 통하여 열람권한이없는 자 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치
- 인터넷 홈페이지를 통해 고유식별정보를 처리하는 경우 연 1회 이상 취약점을 점검하고 필요한 보완 조치
- 개인정보처리시스템에 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속 차단 조치
- 업무용 모바일 기기의 분실.도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 조치

삼성화재

개인정보 안전성 확보 조치 기준

[사례] 관리자페이지 접근제어 미흡

"A공공기관의 홈페이지 관리자는 외부 출장 시 관리자페이지 접근이 가능하도록 외부망 접근 설정함. 그러나 외근 중 사고로 인해 접근제어가 방치되고 취약한 비밀번호 설정되어 결과적으로 홈페이지 개인정보가 대량 노출됨"

✓ 관리자페이지에 대한 외부 접근제어, 관리자페이지 로그인 비밀번호 설정 미흡

- 제29조 안전조치의무, 개인정보의 안전성 확보조치 기준 고시 제5조(접근 권한의 관리) 위반

삼성화재

개인정보 안전성 확보 조치 기준

접근 통제

✓ 정보통신망을 통한 불법적인 접근 및 침해사고 방지

- 인가 받지 않은 접근 제한 : 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등 제한
- 불법적 개인정보 유출 시도 탐지 및 대응 : 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등 분석
  - 개인정보처리시스템에 접속할 수 있고 인가된 사용자(개인정보취급자 고객 등)인지 구분하기 위한 대응 조치
  - 네트워크 장비의 외부 접업 차단 기능 이용
  - 접근통제 대상이 무엇인지 구분

삼성화재

개인정보 안전성 확보 조치 기준(개정)

접근 통제

○ 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음의 기능을 포함한 조치

✓ 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한

✓ 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응

* 침입차단 및 침입탐지 정책 설정, 개인정보처리시스템에 접속한 이상 행위 대응, 로그 훼손 방지 등 적절한 운영·관리가 필요

○ 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 안전한 접속 수단을 적용하거나 안전한 인증 수단을 적용

- 안전한 접속수단 : 가상사설망(VPN), 전용선 등
- 안전한 인증수단 : 인증서(PKI), 보안토큰, 일회용비밀번호(OTP) 등

삼성화재

개인정보 안전성 확보 조치 기준

접근 통제

▽ 안전한 접속 수단 적용 또는 안전한 인증수단 적용

- 원칙적으로 외부에서 내부 네트워크로 접속 차단
- 지리적으로 떨어져 있는 IDC 센터, 지사, 대리점 등과 업무
- VPN 또는 전용선을 통해 사용자의 단말기(노트북, 업무용 컴퓨터, 모바일 기기 등)로 개인정보처리시스템에 안전하게 연결

※ VPN등을 설치할 경우, 취약점(예시 : Open SSL의 HeartBleed 취약점)들을 조치 후 사용

- 안전한 인증수단 : 공인인증서(PKI), 보안토큰, 일회용 비밀번호(OTP) 등

개인정보 안전성 확보 조치 기준

접근 통제

✓ 개인정보가 포함된 문서의 유출 방지를 위해 추가적인 보안 관리 시행(법 제29조, 시행령 제30조, 고시 제6조)

개인정보취급자의 업무용 컴퓨터 및 모바일 기기, 관리용 단말기에 대한 보호조치 이행 예시

예시 1

- 개인정보가 불필요하게 보관되거나, 암호화 되지 않은 상태로 보관되는 등 업무상 수집한 개인정보가 유출될 가능성이 있는지를 정기적으로 점검

예시 2

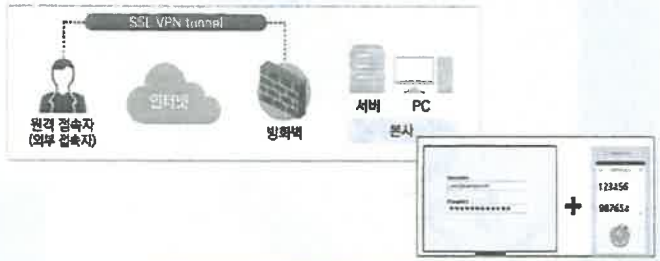
- 공유설정 기능을 사용하지 않도록 해야 하며, 만일 업무상 사용이 불가피한 경우, 이에 대한 접근통제 환경을 추가로 운영, 그 인에 개인정보가 포함되지 않도록 정기적으로 점검

개인정보 안전성 확보 조치 기준

접근 통제

✓ 외부 접속 시 안전한 인증 수단 예시

- 외부에서 개인정보처리시스템에 접근할 경우 : 2-Factor 인증으로 접속
- SSL VPN을 이용하여 아이디/비밀번호 인증(1차), 인증서/휴대폰으로 인증(2차) 후 시스템에 접근

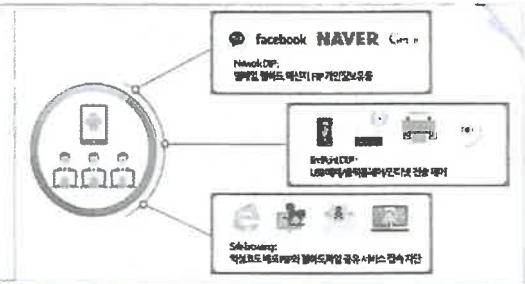


개인정보 안전성 확보 조치 기준

접근 통제

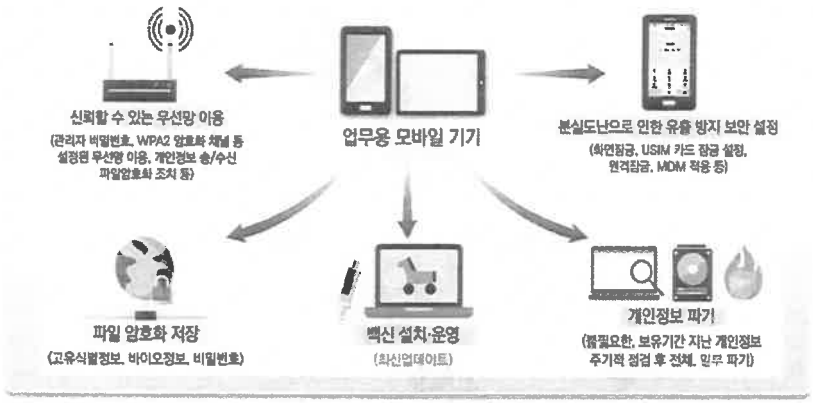
✓ 네트워크 접근
✓ 데이터베이스 접근
✓ 인터넷 접속
✓ 응용 프로그램 접근
✓ 모바일 기기 접근

- Network DLP
  - 인터넷(웹메일, 웹하드, 메신저, SNS, FTP) 등한 개인정보 전송 통제
  - HTTPS 를 통한 개인정보 유출통제
- Endpoint DLP
  - USB, DVD 미디어를 통한 파일 복사
  - 프린터를 통한 개인정보 출력
- 디바이스 반출입 통제
  - 출입통제 장치 X-ray스캐너



개인정보 안전성 확보 조치 기준

접근 통제



개인정보 안전성 확보 조치 기준

접근 통제

✓ **인터넷 홈페이지, P2P 공유설정, 공개된 무선망 이용 등을 통해 열람권한이 없는 자에게 개인정보가 공개 또는 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제**

※ 최신의 위협 동향, 대상 시스템 및 대상 기관의 특성, 위험도 등을 고려, 개인정보 유노출 방지에 적절한 조치를 취할

✓ **인터넷 홈페이지**

- 서비스 제공에 사용되지 않거나 관리되지 않는 사이트 또는 URL(Uniform Resource Locator)에 대한 삭제나 차단
- 인터넷 홈페이지의 설계개발 오류, 개인정보취급자의 업무상 부주의 등 인터넷 서비스 검색엔진(구글링 등)을 통해 관리자 페이지와 취급 중인 개인정보가 노출되지 않도록 조치
- 개인정보가 유출 위험을 줄이기 위해 정기적으로 웹 취약점 점검

✓ **개인정보처리시스템, 업무용 PC, 모바일 기기, 관리용 단말기**

- 원칙적으로 P2P 또는 공유 설정 불가
  - 만약 업무상 꼭 필요...미리 권한 설정 (열람 권한 없는 자에 공개 유출 방지)
  - 주기적 점검
    - 전체 폴더(드라이브)나 불필요한 폴더 공유 불가
    - 개인정보 파일 불포함
- 시스템 상에서 P2P 웹하드 등 사용 포트 차단

개인정보 안전성 확보 조치 기준

접근 통제

✓ **인터넷 홈페이지**

고유식별정보(주민등록번호, 운전면허번호, 외국인등록번호, 여권번호)를 처리하는 개인정보처리자는 고유식별정보가 유출·변조·훼손되지 않도록 해당 인터넷 홈페이지에 대해 연 1회 이상 취약점을 점검하여야 하며, 그 결과에 따른 개선 조치 이행

웹 취약점 점검 항목 (예시)	잘 알려진 웹 취약점 점검 항목	취약점 점검 수행
✓ 웹 취약점 점검 항목(예시) ✓ SQL_Injection 취약점 ✓ CrossSiteScript 취약점 ✓ File Upload/Download 취약점 ✓ ZeroBoard 취약점 ✓ Directory Listing 취약점 ✓ URL/Parameter 변조 등	✓ 행정안전부, 국가사이버안전센터 (NCSC) ✓ 한국인터넷진흥원 (KCERT) ✓ OWASP (오픈소스웹보안프로젝트) 등에서 발표하는 항목 참조	✓ 기관 내부의 자체 인력 ✓ 전문보안업체 취약점 점검 도구 ✓ 상용 도구 ✓ 공개용 도구 ✓ 자체 개발 도구

개인정보 안전성 확보 조치 기준

접근 통제

개인정보 안전성 확보 조치 기준

개인정보의 암호화

구 분				암호화 기준
정보통신망, 보조저장매체를 통한 송신 시	비밀번호, 바이오정보, 고유식별정보			암호화 송신
개인정보처리시스템에 저장 시	비밀번호			일방향(해쉬 함수) 암호화 저장
	바이오정보			암호화 저장
	고유식별정보	주민등록번호		암호화 저장
		여권번호, 외국인등록번호, 운전면허번호	인터넷 구간, 인터넷 구간과 내부망의 중간 지점(DMZ)	암호화 저장
			내부망에 저장	※ 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과 ※ 암호화 미적용시 위험도 분석에 따른 결과
업무용 컴퓨터, 모바일 기기에 저장 시	비밀번호, 바이오정보, 고유식별정보			※ 비밀번호는 일방향 암호화 저장 ※ 상용 암호화 소프트웨어 또는 안전한 알고리즘 암호화

- 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장
- 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장
  안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행

개인정보 안전성 확보 조치 기준

접근 통제

접근 통제 - 별도 개인정보처리시스템이 없는 경우

✓ **업무용 컴퓨터 또는 모바일 기기의 운영체제(OS: Operating System)나 보안프로그램 등에서 제공하는 접근 통제 기능 이용**

- 접근통제 시스템 설치 의무화에 관한 '안전성 확보조치 기준 고시 제6조 제1항' 미적용
  ※ 안전성 확보조치 기준 제6조 제2항, 제4항, 제5항 미적용
- (예시) 소상공인이나 영세사업자가 별도의 개인정보처리시스템 없이 업무용 컴퓨터(PC)또는 모바일 기기를 이용해 개인정보 처리

개인정보 안전성 확보 조치 기준

[사례] 관리자 계정 비밀번호 저장 미흡

해반사항

✓ A병원은 관리자 계정, 환자들 계정에 대한 비밀번호를 암호 알고리즘으로 암호화하지 않은 채 평문으로 저장하고 있었음

조치사항

- 비밀번호 저장 시 복호화 되지 않도록 일방향 암호화 적용

조치 TIP

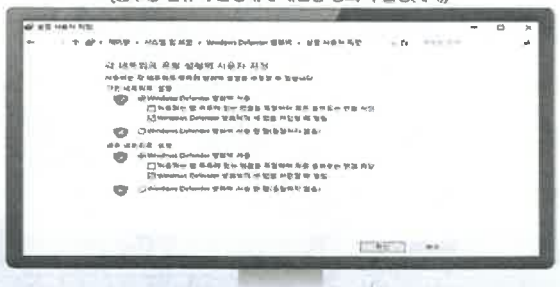
- KISA 암호기술 활용 안내 서적(https://seed.kisa.or.kr/kisa/reference/UgeGuide.do) 참고

개인정보 안전성 확보 조치 기준

접근 통제

접근 통제 - 별도 개인정보처리시스템이 없는 경우

(업무용 컴퓨터 운영체제 개인용 방화벽 설정(예시))



개인정보 안전성 확보 조치 기준

접속기록의 보관 및 점검

○ 개인정보처리시스템에 대한 개인정보 입·출력 및 수정, 피일별·담당자별 데이터 접근 내역 등을 자동으로 기록하는 로그 파일을 생성하여 최소 1년 이상 보관 및 관리

접속기록 일정기간 저장 관리할 수 있도록 개발

❖ 필수 기록 항목

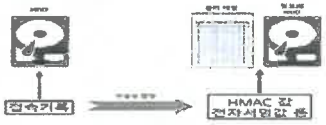
- 계정 : (개인정보취급자 식별정보) ID 등
- 접속 일시 : 날짜 및 시간
- 접속지 정보 : 접속자 정보(IP 주소 등)
- 처리한 정보주체 정보 : 고객번호, 사번 등
- 수행 업무 : 열람, 수정, 삭제, 인쇄 입력 등

접속기록 항목 (예시)				
취급자 식별정보	정보주체 식별정보	접속일시	접속지	수행업무
홍길동	성춘향	2004.04.18 15:00:00	172.168.11.11	노래교육 신청

접속기록 백업

❖ 별도 물리적인 저장 장치에 보관하고 정기적인 백업 수행

- 접속기록 위·변조 방지를 위해 CD-ROM 같은 덮어쓰기 방지 매체 사용
- 수정 가능한 매체 백업 시, 위·변조 여부를 확인할 수 있는 정보(HMAC or 전자서명 등)를 별도 장비에 보관·관리



삼성화재 SAMSUNG

개인정보 안전성 확보 조치 기준

[사례] 개인정보처리시스템 비밀번호 전송 구간 암호화 미적용

위반사항

- ✓ A학교는 소속 학생, 비소속 학생과 일반인 대상으로 교육 서비스 제공
- ✓ 해당 서비스 제공 과정은 홈페이지를 통해서만 접수 가능, 수강 종료 후 학위 자격증 확인을 위해 수강생 개인정보를 준영구적으로 보관하고 있음

조치사항

- 고유식별정보, 비밀번호, 바이오 정보를 정보통신망을 통하여 송신하는 경우 암호화 적용

삼성화재 SAMSUNG

개인정보 안전성 확보 조치 기준

접속기록의 보관 및 점검

목적

✓ **개인정보 오남용 등 침해사고 분석**

접속기록 정의

✓ **개인정보처리시스템에 접속하여 수행한 업무내역에 대해 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것**

✓ **접속 : 개인정보처리시스템과 연결되어 데이터 송신 또는 수신 가능 상태**

삼성화재 SAMSUNG

개인정보 안전성 확보 조치 기준

접속기록의 보관 및 점검

○ 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 안전하게 보관·관리 5만명 이상, 고유식별정보 또는 민감 정보 처리 시 2년 이상 보관·관리

○ 개인정보처리시스템의 접속기록 등을 월1회 이상 점검, 특히 개인정보 다운로드 발견 시 내부 관리계획으로 정하는 바에 따라 그 사유를 반드시 확인(여부 등)

삼성화재 SAMSUNG

개인정보 안전성 확보 조치 기준

접속기록의 보관 및 점검

접속기록 작성 예시

1) 계정 : 개인정보처리시스템에 접속한 자(개인정보취급자 등)의 계정정보
2) 접속일시 : 접속한 시점 또는 업무를 수행한 시점(년-월-일, 시분초)
3) 접속지 주소 : 개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버 IP
4) 처리한 정보주체의 정보 : 누구의 개인정보를 처리하였는지 알 수 있는 정보
   과도한 개인정보가 저장되지 않도록 개인의 식별정보(ID 외에 서버 등을 활용하여 기록
   대량의 개인정보를 처리하는 경우 접속로그(접속기록)으로 대체 가능
5) 수행업무 : 개인정보취급자가 개인정보처리시스템을 이용하여 개인정보를 처리한 내용
   (정보 열람, 출력, 수정, 삭제, 다운로드 등)

항목 작성 예시

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

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

개인정보 안전성 확보 조치 기준

접속기록의 보관 및 점검

항목 구체화

✓ **접속기록에 기록해야하는 항목을 구체적으로 명시**
※항목 : 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행 업무

보관기관 연장

✓ **접속기록 보관기간을 최소 1년 이상 보관하도록 차등적 연장**
※6개월 이상 → 모든 개인정보처리시스템은 1년 이상, 다만 5만명 이상 개인정보를 처리하거나 고유식별정보나 민감정보를 처리하는 시스템은 2년 이상

점검사항 개선

✓ **접속기록 점검 주기 단축 : 반기별 1회 이상 → 월 1회 이상**
✓ **개인정보를 다운로드 한 경우 내부관리계획으로 정하는 바에 따라 그 사유를 반드시 확인**

개인정보 안전성 확보 조치 기준

접속기록의 보관 및 점검

✓ **다운로드 사유 기록**

- 개인정보 다운로드 시, 다운로드 사유 확인이 필요한 기준 (내부 관리계획에 포함)을 수립하고, 수립한 기준에 따라 사유를 남기도록 개인정보처리시스템 구축 시 반영

다운로드 사유 확인 관련 내부관리계획 수립 예시

제 ○조(접속기록의 보관 및 점검)

① ○○○○○○(개인정보처리자명)는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관, 관리하여야 한다.

② ○○○○○○(개인정보처리자명)는 개인정보의 분실, 도난, 유출, 위조, 변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히, 개인정보처리시스템에서 다음 각 호중 어느 하나에 해당하는 개인정보 다운로드가 발견되었을 경우에는 그 사유를 반드시 확인하여야 한다.

1. 개인정보취급자가 100명 이상의 정보주체에 대한 개인정보를 다운로드 한 경우
2. 개인정보취급자가 1시간 내 다운로드한 횟수가 10건 이상인 경우
3. 개인정보취급자가 업무시간 외(휴무일 등) 개인정보를 다운로드한 경우

③ ○○○○○○(개인정보처리자명)는 제2항에 따라 개인정보취급자가 정당한 사유 없이 다운로드한 것이 확인된 경우 지체 없이 개인정보취급자 다운로드 한 개인정보를 회수하여 파기할 수 있다.

개인정보 안전성 확보 조치 기준

접속기록의 보관 및 점검

접속기록 필수항목

✓ **계정** : 개인정보처리시스템에서 접속자를 식별할 수 있는 ID 등 계정 정보
✓ **접속일시** : 접속한 시점 또는 업무를 수행한 시점 (년-월-일, 시분초)
✓ **접속지 정보** : 접속한 자의 PC, 모바일기기 정보 또는 서버의 IP주소 등 접속 주소
✓ **처리한 정보주체 정보** : 개인정보취급자가 누구의 개인정보를 처리했는지를 알 수 있는 (이용 ID 등)
✓ **수행업무** : 개인정보취급자가 개인정보처리시스템에서 개인정보를 처리한 내용을 알 수 있는 정보

※접속기록 (예시)

번호	접속일	접속시간	계정 (ID)	접속지정보 (IP)	수행업무 (이벤트)	정보주체 정보
1	2019-07-06	10:15:10	gdhong01	192.168.4.123	고객정보 조회	A고객카드분의
2	2019-07-06	10:16:05	gjlim02	192.168.4.17	고객정보 수정	B고객주소변경
3	2019-07-06	11:10:47	jskim01	192.168.4.34	직원 조회	부서별명통지

개인정보 안전성 확보 조치 기준

접속기록의 보관 및 점검

✓ **접속기록 보관관리기간**

→ 일반 개인정보 **최소 1년 이상**

→ 유출 시 피해가능성 높은 개인정보* **최소 2년 이상**

*5만명 이상 개인정보, 고유식별정보 또는 민감정보

✓ **보관기간의 기준 : 개인정보의 중요도, 민감도 등 고려**

※ 내부 관리계획에 보관기간 정해서 이행

✓ **보관 방법 : 별도의 물리적 저장 장치(CD-ROM 등)에 정기적 백업/보관**

※ 수정 가능한 매체에 백업 시 위변조 여부를 확인할 수 있는 정보(HMAC 또는 전자서명 값)를 별도 장비에 보관·관리

개인정보 안전성 확보 조치 기준

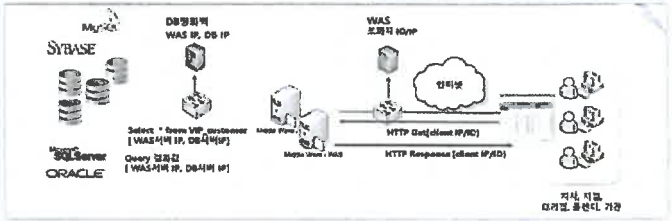
접속기록의 보관 및 점검

✓ **개인정보취급자가 조회한 고객(정보주체)의 개인 식별정보를 포함한 업무 내역 분석**

✓ **실제 사용자 IP/ID 추출 [누기했나]**

✓ **조회대상 개인정보주체 정보 식별 [누구 것을 보았나]**

✓ **사용자가 처리한 업무 내역(text/html) 저장 [왜 했나]**



개인정보 안전성 확보 조치 기준

접속기록의 보관 및 점검

✓ **월 1회 이상 정기적 점검**

✓ **비정상 행위 점검/대응조치**

▪ 비인가된 개인정보 처리 : 개인정보 대량 조회, 다운로드, 정정, 삭제

비정상 행위 (예시)

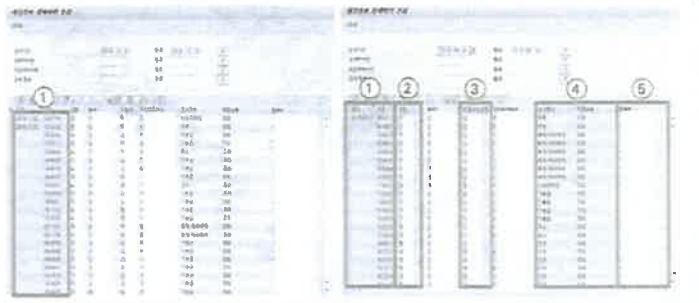
계정	접속일시	접속지 정보
접근권한이 부여되지 않은 계정으로 접속	출근시간 전, 퇴근시간 후, 새벽시간, 휴무일 등 업무시간 외 접속	인가되지 않은 단말기 또는 지역(IP)에서 접속

정보주체 정보	수행업무	기타
특정 정보주체를 과도하게 조회, 다운로드 등의 행위	대량의 개인정보에 대한 조회, 정정, 다운로드, 삭제 등의 행위	짧은 시간에 하나의 계정으로 여러 지역(IP)에서 접속

개인정보 안전성 확보 조치 기준

접속기록의 보관 및 점검

① 접속일시 ② 계정 ③ 처리한 정보주체 정보 ④ 수행업무 ⑤ 접속지정보



개인정보 안전성 확보 조치 기준(개정)

악성프로그램 등 방지

○ 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영

악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시

보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지

발견된 악성프로그램 등에 대해 삭제 등 대응 조치

개인정보 안전성 확보 조치 기준(개정)

[사례] 처리시스템 접속기록 합목 누락

위반 사항

- ✓ A기관은 주택 건설, 토지 개발 등의 공공 업무를 수행하는 기관으로 분야별 사업 특성에 따라 수집·저장하는 개인정보도 달랐고, 그것을 보관 관리하는 개인정보처리시스템 또한 여러 개로 분리 될 수밖에 없었음
- ✓ 총5개의 개인정보처리시스템은 운용하고 있었는데, 그 중 2개의 시스템의 경우 개인정보취급자 ID 및 수행 업무에 대해 기록하고 있지 않았음

조치사항

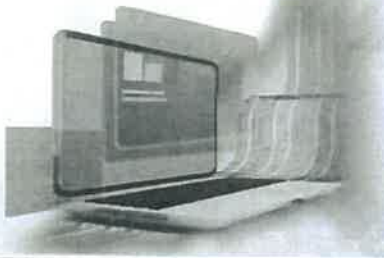
- 개인정보처리시스템에 접속한 기록을 보관할 때 필수 항목을 기록·보관

개인정보 안전성 확보 조치 기준(개정)

관리용 단말기의 안전조치

○ 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음의 안전조치를 이행

고려사항
관리용 단말기의 종류에 따른 특성, 중요도
개인정보처리시스템에 접속하는 빈도 및 수행업무
관리용 단말기를 통한 개인정보의 유출 가능성 및
개인정보처리시스템에 악성코드 전파 등



인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치

본래 목적 외로 사용되지 않도록 조치

악성프로그램 감염 방지 등 을 위한 보안조치 적용

개인정보 안전성 확보 조치 기준(개정)

[사례] 처리시스템 접속기록 보관 위반

접속기록 보관 위반 : 6개월 지난 접속기록의 삭제로 개인정보 유출 책임자 확인불가

"'12년 총선 시 서대문구 유권자 13만명 중 약 6만명의 개인정보가 특정 정당 선거캠프로 넘어갔으나 6개월이 지난 접속기록을 모두 삭제하고 있어 유출한 책임자를 확인할 수 없어요.."

"공공기관은 개인정보 유출해도, 6개월 뒤 로그기록 삭제"

접근권 관리 작성으로 접속 기록 6개월만 보관
개인정보 안전성 확보 기준에 의해 관리부실 논란

"서대문갑 지역 유권자 명부에는 이 지역 유권자 전체인 13만1천여명의 이름, 주소, 주민번호 일자리가 적혀 있고, 7만4688명의 전화번호(전체 유권자의 56%), 4만8670명의 휴대전화번호(전체의 36.6%)가 담겨 있다. <출처: 한겨레신문, 2012. 4. 23>

☞ '개인정보의 안전성 확보조치 기준(2017.07)'에 따라 6개월 이상 된 접속기록을 삭제, 해당 유출자를 찾을 수 없음...개인정보의 안전성 확보조치 기준 제8조(접속기록의 보관 및 점검)

- 개인정보보호법 제17조 개인정보의 제공 등의 위반
- 개인정보보호법 제71조 : 5년 이하의 징역 또는 5천만원 이하의 벌금

※ 정보 주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 사와 그 사정을 알고 개인정보를 제공받은 자

개인정보 안전성 확보 조치 기준

개인정보의 파기

○ 개인정보를 파기할 경우 다음 어느 하나의 조치를 하여야 함

전체 파기

완전파괴
(소각·파쇄 등)

전용 소자장비
이용하여 삭제

데이터가 복원
되지 않게 초기화
또는 덮어쓰기

○ 개인정보의 일부만을 파기하는 경우 위의 방법으로 파기하는 것이 어려울 때에는 다음의 조치를 하여야 함

일부 파기

전자적 파일 형태인 경우	제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우
개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독	해당 부분을 마스킹, 천공 등으로 삭제

개인정보 안전성 확보 조치 기준(개정)

모바일기기에 대한 안전조치

1. 의심스러운 애플리케이션 다운로드 금지
2. 신뢰할 수 없는 사이트 방문 금지
3. 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제
4. 비밀번호 설정 기능 및 관리
5. 블루투스 기능 등 무선 인터페이스 관리
6. 이상 증상이 지속될 경우 악성코드 감염 여부 확인
7. 다운로드한 파일은 바이러스 유무 검사 후 사용
8. 정기적인 바이러스 검사
9. 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트

삼성화재 수탁 업체 관리 방안

보안부서 주관

- 개인정보 관리 및 IT보안 전반에 걸친 보안 수준 점검
  1. 연 1회 점검
  2. 정보보안 관리체계(10개 항목), 네트워크(8개 항목), 고객정보처리시스템(19개 항목), PC보안(24개 항목)
  3. 점검 결과에 따른 보안 컨설팅 제공

현업부서 주관

- 개인정보파기확인서 징구(월 1회)
- 교육 점검 실시(반기 1회)
  - 19년 하반기부터 축소 운영, 기본 분기 1회 실시

개인정보 안전성 확보 조치 기준(개정)

물리적 안전조치

○ **전산실, 자료보관실 등 개인정보 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우 이에 대한 출입통제 절차를 수립·운영**

○ **개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관**

○ **개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련**

- 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있음

수탁사 보안 점검 이슈

접속기록의 보관 및 점검 - 다운로드 사유 미기록

Ⅳ 다운로드 사유 기록

- 개인정보 다운로드 시, 다운로드 사유 확인이 필요한 기준 (내부 관리계획에 포함)을 수립하고, 수립한 기준에 따라 사유를 남기도록 개인정보처리시스템 구축 시 반영

다운로드 사유 확인 관련 내부관리계획 수립 예시

제 ○조(접속기록의 보관 및 점검)

① ○○○○○○(개인정보처리자명)는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관, 관리하여야 한다.

② ○○○○○○(개인정보처리자명)는 개인정보의 분실, 도난, 유출, 위조, 변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히, 개인정보처리시스템에서 다음 각 호중 어느 하나에 해당하는 개인정보 다운로드가 발견되었을 경우에는 그 사유를 반드시 확인하여야 한다.

1. 개인정보취급자가 100명 이상의 정보주체에 대한 개인정보를 다운로드 한 경우
2. 개인정보취급자가 1시간 내 다운로드한 횟수가 10건 이상인 경우
3. 개인정보취급자가 업무시간 외(휴무일 등) 개인정보를 다운로드한 경우

③ ○○○○○○(개인정보처리자명)는 제2항에 따라 개인정보취급자가 정당한 사유 없이 다운로드한 것이 확인된 경우 지체 없이 개인정보취급자 다운로드 한 개인정보를 회수하여 파기할 수 있다.

5. 수탁업체 보안 점검 이슈

수탁사 보안 점검 이슈

접속기록 보관(예시)

① 접속일시 ② 계정 ③ 처리한 정보주체 정보 ④ 수행업무 ⑤ 접속지정보

수탁사 보안 점검 이슈

접속기록의 보관 및 점검

접속기록 보관 미흡

1) **계정** : 개인정보처리시스템에 접속한 자(개인정보취급자 등)의 계정정보
2) **접속일시** : 접속한 시점 또는 업무등 수행한 시점(년-월-일 시분초)
3) **접속지 주소** : 개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버 IP
4) **처리한 정보주체의 정보** : 누구의 개인정보를 처리하였는지 알 수 있는 정보
   - 고도한 개인정보가 지정되어 별도로 개인의 식별정보를 확인 · 처리하는 기록
   - 대량의 개인정보를 처리하는 경우 검색조건(처리내용) 기록
5) **수행업무** : 개인정보취급자가 개인정보처리시스템을 이용하여 개인정보를 처리한 내용
   - 열람, 수정, 입력, 삭제, 출력, 다운로드 등

항목 작성 예시

개인정보취급자 계정	접속일시	접속지 정보	처리한 정보주체의 정보	수행업무
A0001	2020-02-25 17:00:00	192.168.10.11	kdhong	개인정보 수정

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

신규

수탁사 보안 점검 이슈

개인정보처리시스템 첨부파일 개인정보

첨부된 이미지 파일(PDF, JPG 등)에 개인정보 포함

노출사례

- 이미지 파일 첨부를 통한 개인정보 노출

수탁사 보안 점검 이슈

접근 권한 관리

✓ 접근 권한의 부여/변경/말소

- 침해사고 발생 시 원인 분석 등을 위하여 접근 권한 관련 내역을 사후에 추적·검토할 수 있도록 접근권한 부여/변경/말소 내역을 저장

접근권한내역 보관기록 예시

번호	사용자ID	사용자명	권한명	권한ID	유형	일시	작업자	사유	...
...									
51503	Cskim	김철수	회원관리자	S0002	부여	20190220 10:22:01	Gdhong	담당업무 변경	...
51504	Yhkim	김영희	상담관리자	C0005	부여	20181210 09:50:33	Gdhong	상담팀 입사	...
51505	Yhkim	김영희	상담관리자	C0005	말소	20190423 13:55:20	Gdhong	퇴사	...
...									

...

수탁사 보안 점검 이슈

개인정보처리시스템 접근제어 미흡 등으로 인한 관리자 페이지 노출

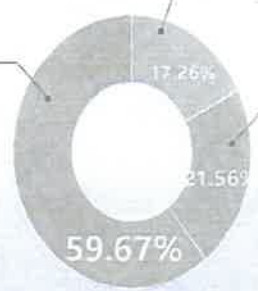
노출사례

- 접근제어 미흡으로 인한 관리자 페이지 노출

수탁사 보안 점검 이슈

개인정보처리시스템 첨부파일 개인정보

2019년도 홈페이지 첨부파일 노출 유형 Top 3



HWP, DOC

- 한글 워드파일에서 노출된 '개인정보'

PDF, JPG

- 이미지 파일에 '개인정보' 포함

XLS

- 글자색을 배경색과 같게 처리
- Sheet 숨기기 처리
- 행/열 숨기기
- Sheet 보호 처리
- 함수치환 처리
- 외부파일참조
- 메모에 "개인정보" 입력
- "개인정보"가 포함된 개체 삽입(OLE개체)

개인정보 보안 점검 이슈 사항

파기

- 개인정보처리시스템 사용 시 삼성화재 정보 파기 이슈

  개인정보처리시스템 사용 시 삼성화재 정보를 이용하여 작성된 보고서, 사고번호 등 정보 중 개인 정보만 삭제하고 삼성화재 담당자에게 파기확인서를 송부하고 있음
  수탁사 측에서 정산, 회계을 이유로 삭제하지 않고 DB에 저장하고 있음
  업무 목적이 충족된 건에 대해서 개인정보처리시스템 DB에 모두 삭제하여야 함

  ※ 단 법령(특별법)에 의해 보관기간이 정해진 경우 예외

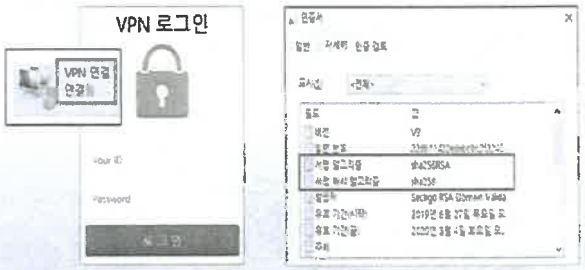
- 삼성화재에서 업무위탁으로 전송한 개인정보는 업무 목적 종료 후 파기확인서 제출과 함께 완전 파기를 원칙으로 함

수탁사 보안 점검 이슈

개인정보처리시스템 접근제어 미흡 등으로 인한 관리자 페이지 노출

조치방법

- **안전한 접속수단 마련**
- **VPN 접속 또는 SSL 적용**

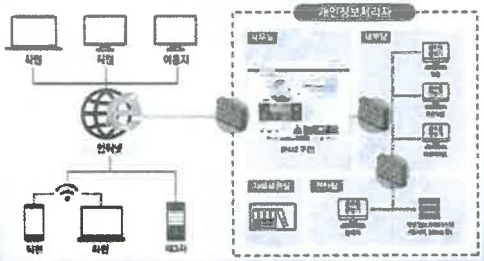


개인정보 보안 점검 이슈 사항

네트워크

- 개인정보처리시스템 사용 유무에 따른 보안 이슈

  개인정보처리시스템 미사용 수탁사는 내부망에 대한 보안조치 미적용
  개인정보처리시스템 사용 수탁사는 보안장비(UTM, WAF 등)에 대한 운영 권한이 없으며, 보안정책 현황 미관리
  보안관제 서비스 이용 중인 수탁사는 매월 탐지 로그 보고서를 통한 사후 미조치



수탁사 보안 점검 이슈

관리자 페이지 접근제어 미흡

조치방법

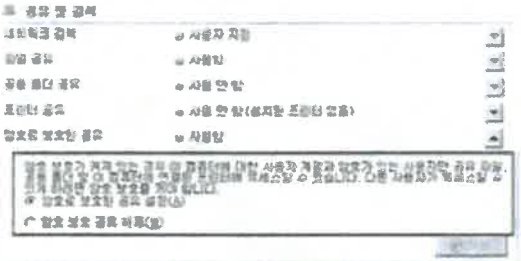
- **설계 유추 가능한 관리자 페이지 접속 주소 변경**

개인정보 보안 점검 이슈 사항

공유 폴더

○ 무분별한 공유 폴더 사용

공유폴더에 대해 접근통제 미설정되어 있어, 누구나 이용 가능
-> 악의적인 사용자로부터 개인정보 유출시고 위험이 존재함
-> 프린터 사용 목적으로 공유 폴더 미처단



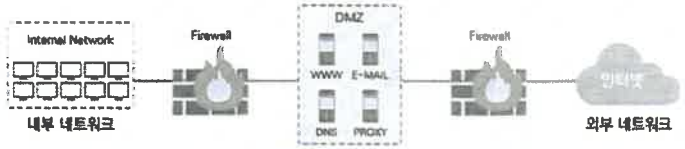
삼성화재

개인정보 보안 점검 이슈 사항

네트워크

○ N/W에서 개인정보처리시스템/내부망에 대한 안전한 보안 설정 필요

* 침입차단 및 침입탐지 정책 설정, 개인정보처리시스템에 접속한 이상 행위 대응, 로그 훼손 방지 등 적절한 운영·관리가 필요



삼성화재

개인정보 보안 점검 이슈 사항

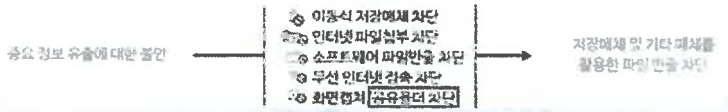
공유 폴더

○ 공유 폴더 사용 시 보안 조치 필요

공유 폴더 사용 시 특정 사용자만 접근 가능하도록 통제

NAS 사용 시 각 계정 별 권한 부여를 통해 접근 제어
-> 추후 보안사고 시 추적을 위한 로그 기능 설정

DLP(데이터 유출 방지) 솔루션을 이용하여 공유 폴더 비활성화 강제화
-> 공유 폴더 사용 시 특정 경로만 사용 가능



삼성화재

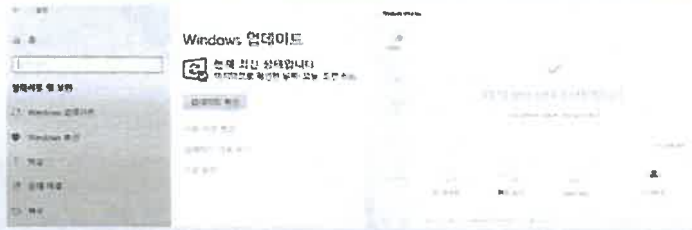
개인정보 보안 점검 이슈 사항

Server/PC

○ 개인정보처리시스템 서버/PC 보안 조치 필요

EoS(End Of Service) 된 OS는 최신 서버로 업데이트 필요
-> EoS되어 있는 OS 대상으로 신규 취약점 발견 시 악의적인 사용자로부터 해킹의 대상이 되어 개인정보 유출사고 위험 존재

Linux 서버에 백신 S/W 설치 필요



삼성화재

6. 개인정보 보호 상담 사례를 통한 Q&A

삼성화재 SAMSUNG

개인정보 보안 점검 이슈 사항

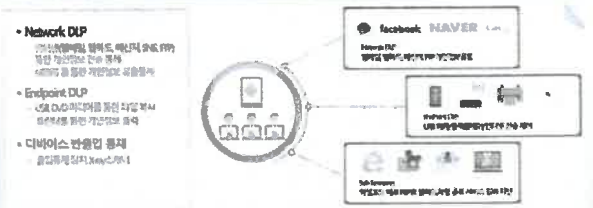
DLP/DRM

○ 보안프로그램(DLP, DRM) 조치 필요

DLP, DRM, 개인정보검출솔루션, 백신 S/W 설치 필요
-> 보안프로그램 미사용 시 개인정보 유출사고 발생 위험

DLP, DRM 사용 시 주기적인 정책관리 및 로그기록 검토 필요
-> 사용정책 미비 시 업무상 필요한 정보 유출, 유출사고 발생 시 원인 추적 가능

개인정보 검출 시 주기적인 개인정보책임자 검토 필요
-> 비정상 개인정보 검출 시 조치를 통한 개인정보 유출사고 위험감소



삼성화재 SAMSUNG

개인정보 상담 사례를 통한 Q&A

차량번호 하나만으로는 개인정보라고 볼 수 없나요?

A 구체적으로 해당 차량번호가 수집 및 이용되는 상황에 따라 판단이 달라질 수 있지만 차량 번호 하나만으로는 개인을 식별할 여지가 있더라도 자동차등록원부 등과 쉽게 결합하여 등록자 개인을 식별할 수 있으므로 개인정보로 볼 수 있습니다.

삼성화재 SAMSUNG

개인정보 보안 점검 이슈 사항

메신저

○ 메신저 사용 시 보안 조치 필요

업무용 메신저 사용을 권고하지만, 상용 메신저 사용 시 회사 대표 계정을 통해 사용 필요
-> 개인 계정 마음하여 메신저 사용 시 고객정보(중요 서, 등록증, 사진) 유출 가능성 고위험

DLP 솔루션 내 파일첨부 차단 정책 사용 필요
-> 파일첨부 차단 정책 사용 시 메신저를 통한 파일첨부 불가능하여 개인정보 유출 위험감소

월 1회 자체 보안 점검 시 모바일 체크리스트 추가 필요
-> 모바일 내 개인정보 사진 / 백신 설치 / 업데이트 안됨 확인 등의 보안 조치 필요

삼성화재 SAMSUNG

개인정보 상담 사례를 통한 Q&A

내부 직원에 대한 교육을 외부 업체에 위탁할 때 위탁에 대한 동의를 받아야 하나요?

A 「표준 개인정보보호 지침」 에서는 근로자와 사용자가 근로계약을 체결하는 경우, 임금지급, 교육, 증명서 발급, 근로자 복지 등을 위하여 근로자 동의 없이 개인정보를 수집·이용할 수 있도록 규정하고 있습니다. 따라서 내부 직원에 대한 교육위탁은 별도 동의는 필요치 않지만, 위탁내용과 수탁자는 고지하여야 합니다.

참고

[illegible]

개인정보 상담 사례를 통한 Q&A

Q2 차량번호 하나만으로는 개인정보라고 볼 수 없나요?

A 구체적으로 해당 차량번호가 수집 및 이용되는 상황에 따라 판단이 달라질 수 있지만 차량번호 하나만으로는 개인을 식별할 여지가 없더라도 자동차등록원부 등과 쉽게 결합하여 등록자 개인을 식별할 수 있으므로 개인정보로 볼 수 있습니다.

참고

주요 개념 정의

- 개인정보파일: 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)
- 개인정보 처리: 개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위
- 정보주체: 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람
- 개인정보처리자: 업무등 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관 법인, 단체 및 개인 등

개인정보 상담 사례를 통한 Q&A

비밀번호는 반드시 8자리 이상으로 설정해야 하나요?

A 「개인정보의 안전성 확보조치 기준」 제5조에 따르면, 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하도록 하고 있습니다.
즉, 안전하지 못한 비밀번호를 사용할 경우 정보가 노출될 위험성이 있으므로, 생일, 전화번호 등 추측하기 쉬운 숫자나 문자 등을 비밀번호로 이용하지 않도록 비밀번호 작성규칙을 수립하고 개인정보처리시스템에 적용하여야 합니다.
이 때 비밀번호의 최소 길이는 구성하는 문자의 종류에 따라 최소 10자리 또는 8자리 이상의 길이로 구성하여야 합니다. 참고로 비밀번호 작성규칙은 아래와 같습니다.

참고

비밀번호 작성규칙

최소 10자리 이상: 영대문자(A-Z, 26개), 영소문자(a-z, 26개), 숫자(0-9, 10개) 및 특수문자(32개) 중 2종류 이상으로 구성

최소 8자리 이상: 영대문자(A-Z, 26개), 영소문자(a-z, 26개), 숫자(0-9, 10개) 및 특수문자(32개) 중 3종류 이상으로 구성

개인정보 상담 사례를 통한 Q&A

스마트폰에 저장된 전화번호 단독으로도 개인정보로 볼 수 있나요?

A 전화번호는 단독으로도 개인정보가 될 수 있습니다. 단, 「개인정보 보호법」 상 의무를 부담하는 대상(개인정보처리자)은 업무를 목적으로 개인정보를 처리하는 경우에 한정됩니다.
사적인 친분관계를 위하여 스마트폰에 전화번호, 이메일 등을 저장하는 경우는 개인정보처리자에 해당하지 않습니다.

참고

[illegible]

개인정보 상담 사례를 통한 Q&A

Q 대학교 홈페이지에서 비밀번호 찾기를 하면 회원께서 자의 비밀번호를 그대로 보여줍니다. 업서 비밀번호를 부여하는 다른 사이트와 비교해 볼 때 좋지 않은 것 같아요.

A 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 합니다.

개인정보처리자는 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술을 적용하는 등 필요한 조치를 취하여야 합니다. 이 경우에 비밀번호는 암호화하여 저장하여야 하고, 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 합니다.

주민등록번호 등 일방향 암호화는 저장되면 원래의 값으로 복호화 할 수 없으므로 본인 확인을 위한 수단으로는 적절하지 않습니다. 따라서 주민등록번호 등 원래의 값을 확인할 필요가 있는 경우에는 양방향 암호화 방식을 사용하여야 합니다.

양방향 암호화는 저장된 값으로 원래 값을 유추할 수 없도록 암호화 하는 것으로 인증정보 저장에 적합한 방식입니다. 사용자가 입력한 비밀번호를 동일한 함수에 적용하여 얻은 결과 값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인하는 것입니다.

따라서 이 사례에서 비밀번호를 그대로 보여 주는 것은 원본 값을 유추하거나 복호화 할 수 없도록 한 일방향 암호화에 해당되지 않습니다.

Q 사이트 대표로 사이트를 회원 로그인을 하는데 최근 해킹 문제 프로그램을 통해 확인해 보니 가입할 비밀번호가 전송과정에서 암호화가 되지 않고 그대로 보여 집니다.

A 비밀번호는 정보통신망을 통해 송신하는 경우 암호화하여야 합니다.

개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장 매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 합니다.

비밀번호란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않아야 하는 수도인 정보입니다. 만약 비밀번호가 암호화되지 않으면 인터넷에서 구할 수 있는 재산 분석프로그램 등을 통해 쉽게 비밀번호를 확인할 수 있습니다.

따라서 정보통신망을 통하여 비밀번호를 송신하는 경우에는 SSL 등의 통신 암호 프로토콜에 탑재된 기술을 활용하여 암호화하여야 합니다.

개인정보 상담 사례를 통한 Q&A

3-6 SNS 채팅방 개인정보 노출

Q 승우원 학원 업체 직원이 1000여명의 美 힘공사 지원자 명단 파일을 SNS 오픈 채팅방에 게시하여 지원자 개인정보 다수가 노출되었습니다.

A 개인정보처리자는 노출된 개인정보 파일이 더 이상 유포되지 않도록 삭제 등의 필요한 조치를 취하여야 합니다.

개인정보처리자는 취급 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 합니다.

이 사례의 경우 업무담당자가 업무 수행을 하는 과정에서 개인정보가 포함된 파일을 정당한 권한이 없는 자가 열람할 수 있는 SNS 오픈채팅방에 업로드하면서 개인정보가 노출되었습니다. 우선 개인정보가 포함된 엑셀 파일을 삭제하여야 하고, 해당 채여지 검속자 수 및 파일 다운로드 건수 등을 파악하여 노출 현황을 파악하여야 합니다. 그리고 만약 해당 파일이 노출되었다면 무료 전화 연결 등을 통해 해당 정보가 인터넷 상에 유포되었는지 유무를 확인하여 해당 검색엔진 업체 등에 개인정보 삭제를 요청하여야 합니다.

- 수탁업체에서 업무 편의를 위해 고객에게 개인정보가 담긴 사진(주민등록증, 운전면허증, 통장사본, 차량등록증 등등) 개인 SNS 채팅방(카카오톡, 네이트온, 밴드)를 통해 개인정보 수집
- 이러한 정보를 업무 효율 상 쉽게 공유하기 위해 개인 SNS 단체 채팅방에 공유
- 업무용PC에 업로드, 출력을 위해 본인 SNS채팅창으로 사진 전송
- 개인정보 목적 달성 후 삭제 되어야 할 개인정보 SNS 채팅창에 존재함.

개인정보 범위

등급	등급설명	분류	해당 개인정보
1등급	그 자체로 개인의 식별이 가능하거나 매우 민감한 개인정보 또는 관련 법령에 따라 처리가 엄격하게 제한된 개인정보	고유식별정보	• 주민등록번호, 여권번호, 운전면허번호, 외국인 등록번호 ※ 개인정보보호법 제24조 및 동법 시행령 제19조
		민감정보	• 사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 병력(病歷), 신체적 · 정신적 장애, 성적(性的) 취향, 유전자 검사 정보, 범죄 경력정보 등 사생활 침처하게 침해할 수 있는 정보 ※ 개인정보보호법 제23조 및 동법 시행령 제18조
		연금 정보	• 네일번호, 바이오정보(홍채, 지문, 정맥 등) ※ 개인정보의 안전성 확보조치 기준 고시 제7조
		신용정보/금융정보	• 신용정보, 신용카드번호, 계좌번호 등 ※ 신용정보의 이용 및 보호에 관한 법률 제2조, 제19조 및 동법 시행령 제2조, 제16조, 제21조, 별표2 등 ※ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제15조제4항제2호 및 관련 고시(개인정보의 기술적 · 관리적 보호조치 기준) 제6조제2항
		의료 정보	• 건강상태, 진료기록 등 ※ 의료법 제22조, 제23조 및 동법 시행규칙 제14조 등
		위치정보	• 개인 위치정보 등 ※ 위치정보의 보호 및 이용에 관한 법률 제2조, 제16조 등
2등급	조합되면 명확히 개인의 식별이 가능한 정보	개인 식별 정보	• 이름, 주소, 전화번호, 핸드폰번호, 이메일주소, 생년월일, 성별 등
		개인 관련 정보	• 학력, 직업, 키, 몸무게, 혼인여부, 가족상황, 취미 등
3등급	개인식별정보와 조합되면 부가적인 정보를 제공하는 간접 개인정보	자동생성정보	• IP주소, MAC주소, 사이트 방문기록, 쿠키 등
		가공정보	• 통계형 정보, 가입사 성향 등
		계량적 콘텐츠 식별정보	• 회원번호, 사번, 내부용 개인식별정보 등

출처: KISA

개인정보 상담 사례를 통한 Q&A

4-1 개인정보 파기 시점

Q 더 이상 이용하지 않은 사이트의 회원 탈퇴를 하려 합니다. 그런데 탈퇴 후 개인정보 파기와 관련해서 회원가입시 동의한 내용과 회사에서 명하는 파기 시점이 제 각각입니다. 회원탈퇴 후 언제 개인정보가 파기되어야 하는 건가요?

A 개인정보 수집·이용에 대해 동의시 고지된 보유기간이 경과하면 파기하여야 합니다.

개인정보처리자는 개인정보가 불필요하게 되었을 때에는 지체 없이 해당 개인정보를 파기하여야 한다. "개인정보가 불필요하게 되었을 때"란 개인정보의 처리목적이 달성되었거나, 해당 서비스의 폐지, 사업이 종료된 경우 등이 포함됩니다. 다만 다른 법령에 따라 보존하여야 하는 경우에는 파기하여서는 안 됩니다.

("개인정보가 불필요하게 되었을 때" 경우 예시)

① 개인정보처리자가 당초 고지하고 동의를 받았던 보유기간의 경과
② 동의를 받거나 법령 등에서 인정된 수집·이용·제공 목적의 달성
③ 계명, 계약관계 종료, 동의철회 등에 따른 개인정보처리의 법적 근거 소멸
④ 개인정보처리자의 폐업·청산
⑤ 대금 완제일이나 채권소멸시효기간의 만료

이 사례의 경우 회원 가입시 개인정보 수집·이용에 대한 동의시 당초 고지 받았던 보유기간이 있다면 해당 보유기간이 경과하면 개인정보를 파기하여야 합니다. 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 그때로부터 5일 이내에 해당 개인정보를 파기하여야 합니다.

- 위·수탁사 개인정보 파기 이해 사점이 상이함

ex) 위탁사 : 보고서 업로드 일로부터 5일 이내 삭제

수탁사 : 수임료 입금일로부터 5일 이내 삭제

- 개인정보의 처리 목적이 달성되어 삭제 해야 하는 개인정보를 현업 담당자가 추후 되물는 경우를 대비해 삭제하지 않는 경우