비영리단체를 위한 개인정보 안전성 확보조치 이행 가이드

비영리단체를 위한 개인정보 안전성 확보조치 이행 가이드

발행일 2024년 11월
글쓴이 고아침
펴낸곳 진보네트워크센터
편집 다디잔
주소 03745 서울시 서대문구 독립문로8길 23 (천연동, 3층)
전화 02-774-4551
팩스 02-701-7104
홈페이지 https://guide.jinbo.net/data-protection-security

비영리단체를 위한
개인정보 안전성 확보조치
이행 가이드

들어가며

이 가이드는 비영리단체가 〈개인정보의 안전성 확보조치 기준〉(이하 '안전조치 기준')을 충족하여 개인정보보호법을 준수하는 데 도움을 주고자 작성하였습니다.

비영리단체는 사업과 활동을 수행하면서 회원, 후원자, 상담 내담자, 행사 참여자 등 다양한 사람들과 관계를 맺습니다. 그리고 이들과의 관계를 기록하고 관리하기 위해 각종 개인정보를 수집, 저장, 활용하게 되는데요. 이런 개인정보를 안전하게 잘 관리하는 것 역시 비영리단체의 중요한 책임입니다.

대기업이나 공공기관의 개인정보 유출 소식을 뉴스에서 종종 접해보셨을 겁니다. 비슷한 문제가 끊이지 않는 이유는 우리가 살고 있는 기술적 환경과 관련이 있습니다. 모든 데이터가 디지털 형태로 생성 및 유통되고, PC나 노트북 컴퓨터, 모바일 기기 등으로 인터넷에 접속해 업무를 처리합니다. 데이터를 저장하는 공간도, 업무 처리용 도구도 클라우드 서버를 기반으로 하는 경우가 많습니다. 이 모든 디지털 공간이 데이터 유출로 이어지는 취약점이 될 수 있습니다.

디지털 환경에서 개인정보보호의 중요성은 아무리 강조해도 지나치지 않습니다. 개인정보 역시 디지털화되기 때문에 쉽게 복제, 유통될 수 있을 뿐만 아니라, 대부분 데이터베이스로 처리되므로 개인정보가 대량 유출될 위험성을 배제할 수 없습니다. 비영리단체는 기업처럼 대량의 개인정보를 처리하지는 않지만, 규모와 상관없이 개인정보 관련 사고는 단체의 신뢰성에 치명적인 악영향을 줄 수 있습니다.

개인정보의 유출이나 남용은 외부의 해킹에 의해서도 발생할 수 있지만, 그 이전에 담당자의 무지나 부주의로 인해서 발생할 가능성도 큽니다. 특히, 전문성과 자원이 취약한 작은 단체일수록 개인정보 보호에 대한 충분한 지식과 자원을 투여하기 어렵기 때문에 이러한 문제를 마주할 수 있습니다.

보안은 하나의 정답이 있지도 않고, 한 번의 노력으로 완성되는 것도 아닙니다. 자신에게 맞는 수준의 실천을 직접 고민해 일상 속에서 꾸준히 실행하는 과정입니다. 이 가이드는 〈디지털 보안 가이드〉와 짝을 이루어 읽었을 때 더욱 효과적입니다. 〈디지털 보안 가이드〉가 보안에 관한 전반적인 내용을 폭넓게 다룬다면, 이 가이드는 비영리단체가 법적으로 꼭 충족해야 하는 안전조치 기준에 집중합니다.

안전조치 기준은 개인정보보호법에 따라 개인정보를 다루는 모든 주체가 취해야 하는 법적 요건입니다. 그러나 해당 고시를

읽어보면 일반적인 조치의 성격을 규정하고 있을 뿐 구체적으로 어떤 방법으로 그러한 조치를 취해야 하는지에 대한 기술적인 설명을 제공하고 있지는 않습니다. 이 가이드에서는 비영리단체의 상황을 최대한 반영하여 해당 조치를 어떻게 취할 수 있는지에 관한 실용적인 방안을 제시합니다.

차례

1장. 개념 설명

법령 본문에서 사용하는 개념을 살펴보고,
우리 단체 맥락에서 각 개념이 어떤 것에 해당하는지 살펴봅시다.
친숙하지 않은 용어일 뿐, 어려운 내용은 아닙니다.

핵심 용어

가장 중요하면서도 서로 비슷해 헷갈리는 개념 세 가지를 먼저 살펴봅시다. 안전성 확보조치 기준은 '개인정보처리자'의 책임을 설명하고 있습니다. 동시에 '개인정보 보호책임자'와 '개인정보취급자'라는 표현도 등장합니다.
처리자, 취급자, 책임자… 도대체 뭐가 다른 걸까요?

개인정보처리자는 '업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등'으로 규정됩니다. 즉 업무상 개인정보를 다루는 법적 주체를 말합니다. 우리 가이드에서는 여러분의 비영리단체가 바로 개인정보처리자에 해당합니다.

개인정보 보호책임자(이하 보호책임자)는 '개인정보 보호 계획의 수립 및 시행, 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 등 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자'로 규정됩니다. 한 명을 책임자로 지정하면 됩니다.

보호책임자가 될 수 있는 사람은 대표자, 임원, 임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는

부서의 장입니다(개인정보 보호법 시행령 제32조제3항. 이하 “시행령”). 비영리단체의 경우 예를 들어 대표자, 후원/모금 총책임자, IT 총책임자 등이 보호책임자가 될 수 있습니다. 개인정보 보호에 관한 실질적인 권한과 책임을 갖고 있는 사람을 보호책임자로 지정하면 됩니다.

근로자 수 10명 미만의 소상공인의 경우 별도의 보호책임자를 반드시 지정하지는 않아도 됩니다. 따로 지정하지 않으면 사업주 또는 대표자가 개인정보 보호책임자가 됩니다(시행령 제32조제1항, 개인정보 보호법 제31조제2항. 이하 “법”). 비영리단체에 대한 별도의 조항은 없으므로 비영리단체 역시 같은 기준을 적용합니다. 즉 10명 이상 단체의 경우에는 보호책임자를 지정해야 하고, 그 미만인 경우 명시적으로 지정하지 않으면 대표자가 보호책임자입니다.

5만명 이상의 민감정보/고유식별정보나 100만명 이상의 개인정보를 처리하는 경우에는 개인정보 보호책임자에게 관련 경력이 요구됩니다(시행령 제32조제4항). 여기에 해당하는 비영리단체도 존재하지만 이 가이드에서 따로 다루지는 않습니다.

개인정보취급자는 ‘개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등’으로, 실제로 개인정보를 다루는

사람을 말합니다. 우리 가이드에서는 업무상 개인정보를 처리하는 실무자, 활동가를 가리킵니다.

법률상 개념	우리 가이드에서는...
개인정보처리자	비영리단체
개인정보 보호책임자	대표자/임원 등 (1명)
개인정보취급자	활동가

용어를 하나만 더 살펴보고 법령 본문으로 넘어갑시다. 안전조치 기준에서 주요하게 다루는 개념 중 하나는 개인정보처리시스템입니다. 법령에서는 "데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템"이라고 다소 동어반복적으로 정의하고 있는데요.

단체에서 후원회원 관리를 위해 사용하는 CRM(Customer Relationship Management, 고객관계관리) 시스템을 떠올리면 이해가 쉬울 것 같습니다. 도너스, Webcm, MRM, 효성CMS+ 류의 서비스들이지요. 이런 도구는 제공업체 측에서 안전조치 기준을 지키는 데 도움이 되는 각종 기능을 제공하기도 합니다.

한편 단체에서 개인정보를 처리할 때 CRM만 사용하는 것은 아닙니다. 노트북/데스크탑 컴퓨터에 파일로 저장된 개인정보를

취급하기도 하고, 구글 독스/구글 시트처럼 여러 명이 협업 가능한 클라우드형 서비스를 이용하는 경우도 있습니다.

법령에서 '개인정보처리시스템'과 '컴퓨터'는 별개로 취급하여, 개인정보처리시스템을 이용할 때의 안전조치와 (시스템에 접속하지 않은 채로) 컴퓨터에 저장된 파일을 처리할 때의 안전조치를 구분하고 있습니다. 개인정보처리시스템은 외부 서비스의 형태를 할 수도 있고, 업무용 컴퓨터에 설치하여 운영할 수도 있습니다.

<개인정보 안전성 확보조치 기준 해설서>
(개인정보보호위원회·한국인터넷진흥원, 2020, 이하 <안전조치 해설서>)에 따르면 "데이터베이스 응용프로그램이 설치·운영되지 않는 PC, 노트북과 같은 업무용 컴퓨터는 개인정보처리시스템에서 제외된다"고 하는데요. 다시 말해 업무용 컴퓨터 역시 사용 방식에 따라 개인정보처리시스템으로 간주할 수 있습니다. 예를 들어 노트북 한 대에 회원 전체 개인정보를 파일로 저장해놓고 그 기기에서 회원 관련 업무를 처리한다면, 해당 기기를 개인정보처리시스템으로 볼 수 있습니다. 따라서 해당 노트북에 안전 조치가 적용되어야 하겠지요.

요즘은 클라우드 기반 협업 서비스를 활용해 업무를 처리하는 경우가 많지요. 이런 경우에는 '개인정보처리시스템'의

범위가 다소 모호해집니다. 클라우드 서비스는 기본적으로 데이터베이스시스템에 자료를 저장하지만, 담당자 입장에서는 업무용 컴퓨터를 이용해 해당 데이터를 파일 형식으로 다루는 경우도 있습니다. 예를 들어 구글 드라이브에 업로드한 회원 정보 엑셀 파일을 웹브라우저로 접속해 구글 시트로 편집할 경우, 이것은 '체계적으로 구성한' 개인정보처리시스템이라고 봐야 할까요?

사례

구글 드라이브를 개인정보처리시스템으로 해석한 사례는 방송통신위원회 심의·의결 제2018-47-429호[1] "개인정보보호 법규 위반사업자에 대한 시정조치에 관한 건"에서 찾아볼 수 있습니다. 당시 방통위는 구글 드라이브 계정을 이용해 가입신청서를 관리한 이동통신서비스 판매업자가 개인정보 안전성 확보조치를 어겼다고 지적하면서, 구글 드라이브를 개인정보처리시스템으로 보고 접근통제 및 접속 기록 관리의 의무를 위반했다고 의결했습니다.

해당 시정조치의 근거는 당시 정보통신망법으로 엄밀히 말해 현재의 개인정보보호법은 아니지만, 2020년 8월 개정 「개인정보 보호법」이 시행됨에 따라 정보통신망법의 개인정보 보호 관련 규정이 「개인정보 보호법」으로 통합된 것이기 때문에 안전성 확보조치의 골자는 유사합니다. 따라서 현행법에서도 구글 드라이브를 개인정보처리시스템으로 해석할 여지가 있다고 볼 수 있습니다.

방통위 사례에서 보듯 단일한 '개인정보처리시스템'이
아니라 클라우드 서비스를 사용하더라도 이것이
단체가 보유한 개인정보를 체계적으로 다루는 주요한
방식이라면 개인정보처리시스템이라고 볼 여지가 있습니다.
<안전조치 기준 해설서>에서는 "개인정보처리자의
개인정보 처리방법, 시스템 구성 및 운영환경 등에 따라"
개인정보처리시스템이 달라질 수 있다고 설명합니다.

이 가이드에서는 '개인정보처리시스템'을 가급적
보수적으로 해석합니다. 즉 노트북에 엑셀 파일로 저장된
회원명부를 한글, 엑셀 등 범용 프로그램으로 다루거나
클라우드형 서비스에 업로드한 개인정보를 (구글 시트
등) 온라인 도구로 다루는 작업도 개인정보처리시스템을
구성한 것이라고 가정하고 서술합니다.

그 이유는 두 가지입니다. 혹시라도 안전조치 기준을 잘
적용했는지 아닌지 법리를 따져야 하는 상황이 생길 경우,
조치를 덜 해두는 것보다는 많이 해두는 것이 낫겠죠. 또한
법적인 측면과 별개로 가급적 폭넓은 안전조치를 취하는 것이
실질적인 보안 측면에서 바람직하기 때문이기도 합니다.

그밖의 용어

- **개인정보**

  살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도(예: 연락처, 이메일 주소) 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함합니다.

- **개인정보 처리방침**

  개인정보처리자가 개인정보 처리에 관한 내부 방침을 정해 공개하는 자율규제 장치. 개인정보의 처리 목적, 항목, 보유 및 이용 기간, 3자 제공 또는 위탁에 관한 사항, 정보주체의 권리행사 방법 등을 포함하는 문서로, 개인정보 처리에 영향을 받는 정보주체가 자신의 개인정보가 어떻게 처리되는지 이해할 수 있도록 하는 것을 목적으로 합니다.

- **개인정보 유출**

  법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 또는 권한 없는 자의 접근을 허용하는 일.

- **공유설정**

  컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것.

- **내부관리계획**

  개인정보처리자가 개인정보를 안전하게 처리하기 위하여 내부 의사결정절차를 통하여 수립·시행하는 내부 기준.

- **공개된 무선망**

  불특정 다수가 무선접속장치(AP, 흔히 '공유기'라고 부르는 장비)를 통하여 인터넷을 이용할 수 있는 망으로, 흔히 카페, 도서관, 교통시설, 공공기관 등에 설치된 와이파이 등을 지칭합니다.

- **비밀번호**

  정보주체 및 개인정보취급자 등이 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속할 때 식별자(아이디)와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말합니다.

- **처리**

  개인정보의 수집, 생성, 기록, 저장, 보유, 가공,

편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공,
공개, 파기(破棄), 그밖에 이와 유사한 행위.

- **정보주체**

  처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람. 예컨대 후원회원 명단을 우리 단체가 처리하는 상황에서 정보주체는 후원회원입니다.

- **인증정보**

  개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등에 접속을 요청하는 자의 신원을 검증하는 데 사용되는 정보.

- **이용자**

  정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자. 법적으로는 “이용자”와 “이용자가 아닌 정보주체”를 구분하여 안전조치 기준도 별도로 적용되나, 이 가이드에서는 둘을 엄밀히 구분하지 않고 사용합니다.

- **접속 기록**

  개인정보처리시스템에 접속하는 자가 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것.

- **접근통제**

  개인정보처리시스템에서 담고 있는 개인정보를
  보호하기 위하여 기록에 대한 접근을
  제한하거나 허용하는 기록 관리 과정.

- **접근권한**

  읽기(read), 쓰기(write), 삭제(delete) 등
  디렉토리, 파일, 데이터베이스에 대해
  사용자가 접근 및 수행할 수 있는 작업 권한.

2장. 개인정보의 안전성 확보조치 기준 이해하기

본 가이드의 내용은 〈개인정보의 안전성 확보조치 기준〉
(2023. 9. 22. 시행)을 기준으로 합니다.
실제로 개인정보처리자가 따라야 하는
안전성 확보조치에 대해 알아봅시다.
주된 내용이 정의된 안전조치 기준 제2장을
중점적으로 살펴보겠습니다.

제3조 안전조치의 적용 원칙

> 개인정보처리자는 처리하는 개인정보의 보유 수, 유형 및
> 정보주체에게 미치는 영향 등을 고려하여 스스로의 환경에 맞는
> 개인정보의 안전성 확보에 필요한 조치를 적용하여야 한다.

안전조치 기준 제3조에서는 안전성 확보조치를
적용할 책임이 개인정보처리자, 즉 우리 가이드의
맥락에서는 각 단체에 있음을 명시하고 있습니다.
우리 단체가 적용해야 하는 안전조치가 무엇인지
알아야 하고, 그 조치를 이행해야 한다는 것입니다.

안전성 확보조치를 적용하지 않으면 어떤 위험이 있을까요?

- 보안이 미흡하여 개인정보가 유출/남용되는
  사고가 생길 위험이 커집니다.
- 사고 발생 여부와 무관하게, 안전조치에 관한 법적
  요구사항을 이행하지 못했다는 사실 자체도 위험이 됩니다.

개인정보 사고가 발생했을 경우, 관할 부처인
개인정보보호위원회가 벌칙을 부과할 수 있습니다.
이때 안전성 확보조치 이행 여부가 감경 사유로 작용하는

등 벌칙 판단에 영향을 미칠 수 있어, 조치를 이행하는 편이 유리합니다. 또, 사고 발생과 무관하게 안전성 확보조치 미이행은 과태료 부과 대상입니다. 통상 3천만원 이하의 과태료를 부과할 수 있습니다. (법 제75조제2항제5호)

그렇다면 안전성 확보조치는 어떻게 이행해야 할까요? 안전조치 기준 제4조의 '내부 관리계획'에서 그 윤곽을 확인할 수 있습니다. 안전조치에는 시스템이나 단말기 등에 적용하는 전산 관련 기술적 조치도 있지만, 내부 정책이나 운영방침 등을 통해 실행하여 업무방식 및 조직문화에 연관되는 사항도 있습니다.

제4조 내부 관리계획의 수립·시행 및 점검

① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다. 다만, 1만명 미만의 정보주체에 관하여 개인정보를 처리하는 소상공인·개인·단체의 경우에는 생략할 수 있다.

1. 개인정보 보호 조직의 구성 및 운영에 관한 사항
2. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
3. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항
4. 개인정보취급자에 대한 관리·감독 및 교육에 관한 사항
5. 접근 권한의 관리에 관한 사항
6. 접근 통제에 관한 사항
7. 개인정보의 암호화 조치에 관한 사항
8. 접속기록 보관 및 점검에 관한 사항
9. 악성프로그램 등 방지에 관한 사항
10. 개인정보의 유출, 도난 방지 등을 위한 취약점 점검에 관한 사항
11. 물리적 안전조치에 관한 사항
12. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
13. 위험 분석 및 관리에 관한 사항
14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항

15. 개인정보 내부 관리계획의 수립, 변경 및 승인에 관한 사항
16. 그 밖에 개인정보 보호를 위하여 필요한 사항

② 개인정보처리자는 다음 각 호의 사항을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수, 업무성격 등에 따라 차등화하여 필요한 교육을 정기적으로 실시하여야 한다.

1. 교육목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

④ 개인정보 보호책임자는 접근 권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상 점검·관리 하여야 한다.

안전조치 기준 제4조의 요지는 개인정보 보호와 관련된 내부 관리계획의 수립 및 점검, 그리고 정기 교육이 필요하다는 것입니다.

내부 관리계획

개인정보 보호 내부 관리계획(이하 '내부 관리계획')은 조직 전체에 적용되는 규정으로, 별도 문서로 작성하거나 관련 내용을 단체 내규 등에 포함시키는 형태로 작성할 수 있습니다. 대표자, 임원 등 의사결정권을 가진 당사자의 승인을 통해 수립합니다.

1만명 미만의 개인정보를 처리하는 단체의 경우 내부 관리계획을 별도로 수립하지 않아도 됩니다. 이 가이드를 읽는 단체 중 상당수가 여기 해당할 것입니다. 하지만 법적 의무가 없어도 내부 관리계획을 수립하는 것이 유용할 수 있습니다. 내부 관리계획은 안전조치 기준에서 제시하는 각종 의무 조치를 어떻게 이행할지 문서화하는 성격을 가지므로, 각 조치를 빼먹지 않고 실행하는 데 도움이 되는 일종의 체크리스트 역할을 할 뿐만 아니라 실질적인 보안을 강화하는 데도 도움이 될 수 있습니다.

가이드 뒤편에 있는 〈개인정보 내부관리 계획 예시〉 문서를 참고하여 내부 관리계획을 수립할 수 있습니다.

- **수정 이력 관리**

  내부 관리계획을 변경할 경우에는 변경사항을 즉시 반영하는 것에 더해, 수정 이력을 관리하기도 해야 합니다.

수정, 변경 사항을 각 개인정보 취급자에게 전달하여 준수할 수 있도록 하고, 내부 관리계획에 시행일자를 기록하는 등의 방식으로 기존 문서와 신규 문서를 모두 보관하도록 합니다.

- **이행 실태 점검 및 관리**

  개인정보 보호책임자는 연 1회 이상 내부 관리계획의 이행실태를 점검하여, 점검 결과를 문서로 작성합니다. 만약 점검에서 중요한 문제나 큰 영향을 끼칠 수 있는 사안을 발견할 경우, 대표/임원 등과 공유하여 대책을 마련해야 합니다. 이 가이드를 참고하는 비영리단체의 경우 상당수는 보호책임자가 곧 대표일 테니, 대표나 전체 조직 차원에서 챙겨야 하는 사안이라고 볼 수 있습니다.

교육

개인정보 보호책임자와 개인정보취급자는 개인정보 보호 관련 교육을 정기적으로 이수해야 합니다. 교육은 내부 관리계획 문서의 유무와 상관없이 꼭 진행합니다. '정기적'은 통상적으로 '연 1회 이상'을 말합니다. 단체는 내부적으로 연간 개인정보보호 교육계획을 수립해야 합니다. 교육계획은 교육 목적, 교육 대상, 교육 내용(프로그램 등 포함), 교육 일정 및 방법 등을 포함하여 자유 형식으로 작성하면 됩니다. 내부 관리계획의 일부로 포함시켜도

되고, “○○년 개인정보보호 교육 계획(안)”과 같은 별도 문서로 작성할 수도 있습니다. 내부 관리계획과 교육 계획은 모든 내부 구성원이 볼 수 있도록 공지/게시해둡니다.

가이드 뒤편에 있는 〈개인정보보호 교육계획 예시〉를 참고하여 개인정보보호 교육계획을 세울 수 있습니다.

교육 내용은 개인정보취급자의 지위·직책, 담당 업무의 내용, 업무 숙련도 등에 적합한 것으로 선정합니다. 단체의 규모나 개인정보 보유량을 고려하여 개인정보 보호 전반에 관련된 내용부터 구체적, 실무적 역할 수행에 관련된 내용까지를 다룰 수 있도록 하면 좋습니다. 교육 대상자의 역할에 따라 각기 다른 교육 내용을 배정하는 것도 가능하고, 교육 계획에 자원을 많이 투입하기 어려운 작은 조직에서는 필요한 교육을 하나 선정하여 구성원이 공통으로 수강하는 방법도 있습니다.

교육 이행 증빙을 위해 내부적으로 결과 자료(ex. 교육내용, 이수증 등이 포함된 교육 결과보고서)를 만들어 놓도록 합니다.

교육방식이 법으로 정해져 있지는 않습니다. 온라인 교육 수강, 자체 교육 진행, 강사 초빙 등 어떻게 진행해도 무방합니다. 비영리단체 입장에서는 온라인 교육을 수강하는 것이 예산이나 시간 운용 측면에서 적절할 수 있을 텐데요. 의무 수강시간 역시 법으로 정해진 것은 아니니 1~2개의 강의를 수강하면 됩니다.

개인정보보호위원회에서 운영하고 온/오프라인 교육을 제공하는 '개인정보배움터[2]'를 예로 들어보겠습니다.

개인 온라인 교육과정 안내

• 개인정보보호위원회에서는 개인정보보호 인식제고 및 역량강화를 위하여 사업자 및 국민을 대상으로 온라인 교육 서비스를 제공하고 있습니다.

대상 및 교육과정명			주요내용
개인정보 처리자	공공기관·일반사업자 일반사업자 온라인사업자	[개인정보 보호법] 주요 법 개정사항	'23년 이후 개정된 법의 주요내용
		[NEW] 개인정보 처리자 수준별교육_기본과정	개인정보의 이해, 개인정보처리시 유의사항
		[NEW] 개인정보 처리자 수준별교육_실무과정	개인정보 흐름, 개인정보위수탁 관리
		[NEW] 개인정보 안전성 확보조치	안전성 확보조치 방안 세부설명
		CCTV 관제센터 종사자 교육	실무자를 위한 영상정보처리기기 설치·운영 가이드

온라인 교육의 예. 개인정보배움터 웹사이트 갈무리

- [개인정보배움터 〉 온라인교육(개인수강) 〉 사업자 교육과정]에서 교육을 수강할 수 있습니다. (작성일 기준)
- 개인정보 관련 기초 정보와 실무상 유의사항을 다루는 '기본과정'을 수강합니다.
- 각 교육 대상자가 회원 가입/로그인 후 수강신청을 합니다. 동영상과 퀴즈로 구성된 교육을 수강 완료한 뒤 수료증을 발급받습니다.
- 발급한 수료증은 보호책임자가 수합하여 결과 자료 작성에 활용합니다.

개인정보배움터 교육에서 미처 다루지 못하는, 비영리단체의 사정에 맞는 개인정보 보호 방법에 관해서는 진보네트워크센터나 정보인권연구소 등 시민사회 관련 디지털 전문성이 있는 단체에 문의하는 것도 좋습니다.

제5조 접근 권한의 관리

① 개인정보처리자는 개인정보처리시스템에 대한
접근 권한을 개인정보취급자에게만 업무 수행에
필요한 최소한의 범위로 차등 부여하여야 한다.
② 개인정보처리자는 개인정보취급자 또는 개인정보취급자의
업무가 변경되었을 경우 지체 없이 개인정보처리시스템의
접근 권한을 변경 또는 말소하여야 한다.
③ 개인정보처리자는 제1항 및 제2항에 의한 권한
부여, 변경 또는 말소에 대한 내역을 기록하고,
그 기록을 최소 3년간 보관하여야 한다.
④ 개인정보처리자는 개인정보처리시스템에 접근할 수 있는 계정을
발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을
발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 한다.
⑤ 개인정보처리자는 개인정보취급자 또는 정보주체의
인증수단을 안전하게 적용하고 관리하여야 한다.
⑥ 개인정보처리자는 정당한 권한을 가진 개인정보취급자
또는 정보주체만이 개인정보처리시스템에 접근할 수 있도록
일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에
대한 접근을 제한하는 등 필요한 조치를 하여야 한다.

안전조치 기준 제5조의 요지는 개인정보처리시스템에
대한 접근 권한을 최소한으로 관리하고, 관련 기록을

보관하고, 적절한 인증 보안 조치를 적용해야 한다는 것입니다. 비유하자면 사무실 열쇠를 누가 사용할 수 있는지 잘 관리하는 일과 비슷합니다.

접근 권한이란?

누군가 개인정보처리시스템에 접속하거나, 개인정보를 생성·변경·열람·삭제할 수 있는 경우 해당 인물이 개인정보처리시스템에 "접근 권한이 있다"고 말합니다. 일반적으로 CRM 등에 접속하는 계정 정보를 알고 있는 사람은 해당 개인정보처리시스템에 접근 권한이 있다고 볼 수 있습니다.

최소 권한의 원칙

디지털 보안에 있어서 중요한 원칙 중 하나는, 사용자 계정에 대한 권한을 꼭 필요한 것만 부여하고 필요 없는 권한은 차단하는 것입니다. 이를 "최소 권한의 원칙"이라고 부릅니다. 권한을 최소한으로 부여해 관리함으로써 보안 사고가 발생할 수 있는 노출 지점을 줄일 수 있습니다. 1항에서 말하는 "최소한의 범위로 차등 부여"는 바로 이 최소 권한의 원칙을 가리킵니다.

예를 들어 회원 연락처를 조회하는 용도로 주로 사용하는

계정에, 주민등록번호를 조회하는 권한이나 해당 회원 정보를 수정/삭제할 수 있는 권한이 부여된다면 보안 리스크가 커진다는 것입니다. 업무 분장과 무관하게 모든 구성원에게 모든 회원에 대한 자료 열람 권한을 부여하는 것 또한 최소 권한의 원칙에 위배됩니다.

접근 권한 관리, 어떻게 하면 될까요?

- **필요한 사람만**

  실제로 개인정보를 취급하는 담당자에 한해서 접속 권한을 부여합니다. 업무상 개인정보처리시스템에 접속할 필요가 없는 개인의 경우, ID를 부여하지 않고 로그인 정보 또한 제공하지 않습니다.

- **1인 1 ID**

  같은 계정을 공유해서 사용하지 않습니다. 시스템 접근용 계정은 '정당한 사유가 없는 한' 담당자별로 따로 발급해야 합니다. 여기서 '정당한 사유'는 여러 계정을 만들어 운영하는 것이 시스템 자체에서 기술적으로 불가능한 경우를 말합니다.

  예컨대 일부 회원관리 툴에서는 대표계정 하나만 만들어 사용할 수 있는데, 이런 경우는 불가피하게 같은 계정을

공유해야 할 수도 있습니다. 이처럼 현실적으로 1인 1 ID 부여가 어려울 때도 필요한 사람(업무분장상 담당자)에게만 권한을 부여(계정 접속 정보를 제공)하는 원칙은 지켜야 합니다.

계정을 공유해 사용할 경우, 불의의 보안 사고가 발생했을 때 그 원인/책임/경로를 추적하기 어려워집니다. 어디에서 뚫렸는지 확인이 어려우니 대책 마련도 그만큼 까다로워집니다.

- **업무가 바뀌면 접근 권한도 바뀐다**

  특정 인물이 개인정보를 취급할 필요가 없어질 경우, 시스템 접근 권한 역시 이를 즉시 반영해야 합니다.

  - 담당자가 다른 사람으로 바뀌거나, 업무분장이 바뀌는 경우
  - 인사이동, 조직개편, 퇴직, 휴직, 병가 등 사용자 업무가 변경되거나 종료되는 경우 등

  안전조치 기준은 업무 수행에 필요한 선에서 접근 권한을 차등 부여하도록 요구합니다. 하지만 실무자 개인마다 어떤 개인정보에 얼마나 접근할 수 있는지 일일이 판단하고 관리하는 것은 복잡합니다. 그렇다고 일을 단순화하기 위해 모든 사람이 똑같이 모든 권한을 갖거나, 아예 하나의 관리용 아이디를 나누어 쓰는 것은 보안을 저해하는 요소가 됩니다. 특히 자원이 부족한 작은 단체일 수록 접근 권한 관리와 업무 효율 사이의 긴장이 생길 수 있는데요. 이때

활용할 수 있는 방식이 '역할 기반 권한 부여'입니다.

역할 기반 권한은 말 그대로 역할에 따라 누가 무엇을 할 수 있는지를 미리 정해둔다는 말입니다. 예를 들어 다음과 같이 세 단계로 구분하는 방법을 생각해 볼 수 있습니다.

- 관리자 : 시스템 전반에 대한 접근 권한을 가집니다. 후원회원 정보를 모두 열람하고, 새로운 직원 계정을 만들거나 삭제할 수 있습니다.
  예) 조직이 사용하는 모든 서비스에 접근할 수 있는 계정 부여
- 기획자 : 캠페인 자료, 보고서 등의 정보를 조회하고 수정할 수 있지만 재정 관련 정보나 전체 후원회원 명단은 볼 수 없습니다.
  예) 업무용 구글 드라이브에 접근할 수 있되 재정/인사 관련 폴더 접근 권한은 차단, 후원회원 관리용 CRM 권한 부여하지 않음
- 자원봉사자 : 기부자 정보에는 접근할 수 없고, 활동 스케줄이나 공지사항만 확인할 수 있습니다.
  예) 별도 계정 없이 전체 공개 문서를 통해 소통[3]

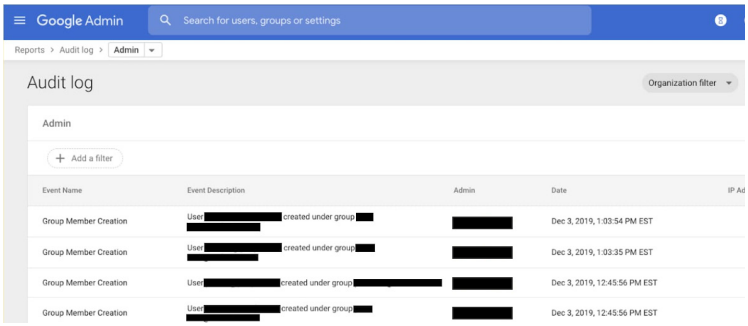
이처럼 역할 기반 권한 부여를 통해 안전성과 효율성 사이의 균형을 추구할 수 있는데요. 위의 예보다 세부화하거나 단순화할 여지도 충분히 있어, 조직의 상황과 자원, 사용하는 도구의 특성에 따라 현실적으로 알맞은 접근을 내부적으로 논의하고 찾아갈 필요가 있습니다.

예컨대 회원관리를 맡은 주 담당자가 한 명일 경우 해당 담당자에게만 권한이 부여되는 것이 원칙적으로 바람직하지만, 담당자 부재시에도 해당 업무를 보완할 수 있도록 정/부 담당자를 지정하여 권한을 동등하게 부여하는 것도 고려해볼 수 있습니다.

- **기록 보관**

  개인정보시스템에 대한 접근 권한 부여/변경/말소 내역은 최소 3년간 기록을 보관해야 합니다. CRM 등 회원관리 툴을 사용할 경우, 시스템 자체적으로 계정 관리 내역을 제공하는지 해당 업체에 문의하여 확인하고 해당 기록을 활용합니다. 구글 워크스페이스의 경우 유료 버전에서는 '어드민 콘솔'의 '감사 로그' 기능을 사용해 권한 부여 관련 기록을 확인할 수 있습니다. 다만 보관 기간이 6개월로 설정되어 있으므로, 데이터를 구글 클라우드에 저장하도록 설정하거나 별도로 백업하여 수동으로 보관할 수 있습니다.

구글 워크스페이스의 경우 유료 버전에서는 '어드민 콘솔'의 '감사 로그' 기능을 사용해 권한 부여 관련 기록을 확인할 수 있습니다. 다만 보관 기간이 6개월로 설정되어 있으므로, 데이터를 구글 클라우드에 저장하도록 설정하거나 별도로 백업하여 수동으로 보관할 수 있습니다.



구글 워크스페이스 어드민 콘솔의 감사 로그 화면 갈무리

만약 사용하는 툴이 계정 관리 내역을 제공하지 않을 경우,
불편하더라도 수동으로 기록해 둡니다.
예를 들어 일시, 권한 관리 대상, 권한 관리 주체,
내용을 기록하는 엑셀 파일을 관리할 수 있습니다.

일시	대상	직위	관리주체	내용	사유
2024. 00.00	OOO	활동가	XXX (보호책임자)	A 개인정보처리시스템 ID 생성 및 전달 (OOO@abc.xyz)	후원회원 담당자 신규 채용에 따른 CRM 접속권한 부여
2024. 00.00	△△△	활동가	XXX (보호책임자)	A 개인정보처리시스템 ID 회수 및 비밀번호 변경 (△△△@abc.xyz)	담당자 업무 변경에 따른 CRM 접속권한 말소

계정 관련 기록만 따로 관리하는 것보다, 기록 보관 절차를
명시적으로 만드는 것도 고려해볼 만합니다. 예를 들어 접근
권한을 신청/심사/승인/부여하는 절차를 명문화하여 기록이

남도록 하거나, 접근 권한 관리 내역을 인사 기록 항목에 포함하여, 인사가 발생할 경우 접근 권한 부여/변경/말소 또한 함께 처리하도록 하는 등 기존 업무에 자연스럽게 개인정보처리시스템 권한 관리 또한 포함되는 방식을 생각해 볼 수 있습니다. 어떻게 보면 번거로울 수 있지만 인사 기록이라고 보면 자주 바뀌는 정보는 아닐 것 같습니다. 각 단체의 사정에 적합한 방법을 찾아 안전조치 기준을 잘 준수해 봅시다!

인증수단이란?

'인증수단'은 특정 시스템이나 단말기에 접속하려는 사람이, 본인이 맞다는 것을 증명하기 위해 사용할 수 있는 수단입니다. 대표적인 인증수단으로는 ID와 비밀번호 조합이 있으며, 그밖에 인증서, 일회용 비밀번호(OTP), 보안토큰, MFA/2FA 등도 인증수단에 해당합니다. 인증수단을 안전하게 관리하는 법에 관해서는 〈디지털 보안 가이드〉 2장 "비밀번호와 인증의 실제"를 참고하세요.

- **인증 실패 시 접근 제한하기**

  로그인 일정 횟수 이상 인증에 실패한 경우 접근을 제한하도록 합니다. 예를 들어 아이디/비밀번호 입력을 세 번 이상 틀린 경우 추가 인증 정보를 요구한다거나, 일정 시간이 지나야 로그인을 재시도할 수 있게 하는 등의 조치를 말합니다.

이런 조치는 개인정보처리시스템 수준에서 제공되는 기능이기
때문에 각 단체에서는 활용하는 시스템에 이러한 기능이
있는지 공식 문서나 업체에 문의해서 확인할 수 있습니다.

제6조 접근통제

① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 안전조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 인터넷 프로토콜(IP) 주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 인터넷 프로토콜(IP) 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 한다. 다만, 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우 가상사설망 등 안전한 접속수단 또는 안전한 인증수단을 적용할 수 있다.

③ 개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 접속이 차단되도록 하는 등 필요한 조치를 하여야 한다.

⑤ 개인정보처리자는 업무용 모바일 기기의 분실·도난

등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.
⑥ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상인 개인정보처리자는 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등에 대한 인터넷망 차단 조치를 하여야 한다. 다만, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구성·운영하는 경우에는 해당 서비스에 대한 접속 외에는 인터넷을 차단하는 조치를 하여야 한다.

'접근통제'의 내용은 크게 두 가지로 하나는 '문을 잘 잠가야 한다', 다른 하나는 '누가 문을 따고 들어왔다면 그 사실을 파악하고 대응해야 한다'입니다. 앞서 '접근 권한의 관리'는 '열쇠 관리'에 비유할 수 있다고 말씀드렸는데, 접근통제는 열쇠를 잃어버리거나 도둑맞았을 때, 혹은 누가 열쇠 없이 자물쇠를 따려 할 때 시스템을 보호할 수 있는 조치라고 볼 수 있습니다.

대부분의 항목은 '잘 잠그기'에 관한 이야기입니다.

개인정보처리시스템 접속 권한 제한

안전조치 기준 제1항제1호에서 말하는 IP 주소 기반 제한은 특정 IP 주소에서만 접속할 수 있도록 설정하는 것을 말합니다. 즉 ID와 비밀번호를 알고 있더라도 해당 IP 주소를 사용하는 기기에서 로그인하지 않으면 접근을 차단하라는 말입니다. 예컨대 사무실 IP 주소에서만 CRM에 접속 가능하게 설정할 경우, 조직 밖의 누군가 ID/비번을 탈취하더라도 시스템에 접속하기 어려워집니다.[4]

외부 CRM 툴 등 사용하는 시스템에 IP 주소 등에 따른 제한 기능이 있는지 모르거나, 설정 방법을 모르는 경우에는 공식 문서를 확인하거나 해당 업체에 문의하여 IP 보안 관련 기능의 존재 여부와 사용 방법을 알 수 있습니다.

IP 주소 기반 제한 기능을 명시적으로 제공하지 않는 범용 툴(예: 구글)의 경우 다음 절에서 설명하는 2단계 인증 설정 등 다른 접속 보안 조치를 통해 비슷한 효과를 볼 수 있습니다.

외부 접속 시 안전한 인증수단 또는 안전한 접속수단 적용

제2항의 '외부 접속'이란 지리적으로 분리된 서버나 데이터센터 등에 접속하는 경우를 말합니다. 비영리단체가 개인정보처리시스템 서버를 사무실에 두고 자체적으로

운영하는 경우는 거의 없기 때문에 사실상 외부 CRM 업체의 서버에 접속하거나 구글 드라이브 등 클라우드 기반 협업 도구를 사용해 온라인으로 수행하는 대부분의 개인정보 관련 업무에 적용됩니다.

앞서 '인증수단'이 본인이 맞다는 것을 증명하는 수단이라고 얘기했지요. 그런데 아이디+비밀번호 조합은 다른 누군가 그 정보를 알아내기만 하면, 본인이 아니더라도 로그인이 가능해지는 한계가 있습니다. (넷플릭스 계정을 가족이나 친구와 공유할 때를 생각해 보면 됩니다.)

반면 '안전한 인증수단'은 본인이 소유한 특정 기기에 연동되어 있거나 시간제한이 있는 등의 방식으로, 다른 사람이 사칭하기 상대적으로 어려운 수단을 가리킵니다. 예를 들어 이런 것들입니다.

- 일회용 비밀번호(OTP)
- USB 키 등 물리적 보안토큰
- 인증서(공인인증서 류)

아이디+비밀번호에 더해 OTP나 인증서 등을 추가로 사용하는 인증방식을 2단계 인증(2FA)라고 하는데요. 2단계 인증의 구체적 방법은 〈디지털 보안 가이드〉 2장 "비밀번호와 인증의 실제"를 참고하세요.

제2항에는 “이용자가 아닌 정보주체”라는 표현이 나옵니다. ‘이용자가 아닌 정보주체’의 개인정보를 처리하는 개인정보처리시스템의 경우에는 반드시 안전한 인증수단을 적용하지 않아도 되고, 가상사설망(VPN)과 같은 안전한 ‘접속수단’으로 갈음할 수 있다는 것입니다. VPN에 관한 자세한 설명은 〈디지털 보안 가이드〉 5장 “통신, E-Mail 및 메신저 보안”을 참고하세요.

이런 식으로 “이용자”의 개인정보와 “이용자가 아닌 정보주체”의 개인정보를 구분해서 다른 기준을 적용하는 내용이 안전조치 기준에 여러 번 등장합니다. 이러한 구분은 기존 정보통신망법에서 다루던 정보통신망서비스 이용자 개인정보 보호 관련 내용과, 개인정보보호법이 통합된 흔적으로 보입니다.

비영리단체의 경우 보통 정보통신망서비스 제공자가 아니므로 회원 역시 ‘이용자’가 아니라고 볼 수 있습니다. 다만 회원이 온라인으로 가입하고, 회원과의 소통도 온라인으로 이루어지는 상황이라면 단체가 엄밀한 의미에서 ‘정보통신망서비스’를 제공하지 않더라도 회원과 이용자가 유사하다고 볼 여지 또한 있습니다.

이 가이드에서는 이처럼 비영리단체 특성상 ‘회원’과 ‘이용자’의 구분이 불명확할 수 있는 점과 개인정보 보호의

관점에서 모든 정보주체의 개인정보를 안전하게 관리하는 것이 바람직하다는 점을 고려해서, 법적으로 '이용자가 아닌 정보주체'에 덜 엄격한 기준이 적용되는 상황이어도 '이용자'에 대한 기준에 준해서 안전조치를 취하는 것이 바람직하다고 봅니다. 앞으로의 설명도 이와 같은 입장에서 서술합니다.

공개/유출 방지

권한이 없는 사람이 개인정보를 볼 수 없도록 개인정보처리시스템뿐만 아니라 업무에 사용하는 각종 기기에도 조치를 해야 합니다.

- **개인정보를 다루는 인터넷 홈페이지를 운영할 경우**

  정기적으로 웹 보안 취약점을 점검합니다. 서비스 제공에 사용되지 않거나, 관리되지 않는 사이트 및 세부 URL을 삭제 및 차단합니다. 이러한 사항을 웹사이트 관리자/개발자와 상의하여 안전하게 운영할 필요가 있습니다.

  홈페이지의 설계·개발 오류, 업무상 부주의 등으로 관리자 페이지가 노출되거나 개인정보를 공개된 페이지에 기록할 경우, 검색엔진을 통해 해당 정보가 외부에 노출되어 개인정보 유노출 위험을 키울 수 있습니다. 인터넷 검색엔진은 서비스 제공에 필요한 자료를 수집하기 위해 웹사이트를 자동으로

조회합니다. 단체 웹사이트가 관련 키워드 검색 결과로 등장하려면 필요한 과정인데요. 이때 어떤 페이지를 검색엔진 및 일반에 공개하고 어떤 페이지는 숨길지 주의해야 합니다.

- **공유 설정은 하지 않는 것이 원칙**

  개인정보처리시스템, 업무용 PC, 모바일 기기 등에서는 P2P나 파일 공유 설정을 사용하지 않는 것이 원칙입니다. 만약 업무상 꼭 필요하다면 전체공유로 풀어놓는 것이 아니라 권한을 구체적으로 설정하여 권한이 없는 자에게 공개되거나 유출되지 않도록 합니다. 주기적 점검을 통해 전체 폴더나 불필요한 폴더의 공유를 막고, 개인정보 파일이 포함되지 않도록 합니다.

  특히 구글 드라이브나 노션 등 클라우드를 통해 개인정보를 처리하는 경우 권한 설정에 주의하도록 합니다. 개인정보가 포함된 문서는 전체 공개 설정하지 않고, 필요한 사람에게 한해 직접 권한을 부여해서 관리하도록 합니다. 클라우드 서비스 보안에 관해서는 〈디지털 보안 가이드〉 7장 “클라우드 서비스 및 협업 툴 보안”을 참고하세요.

- **공개된 무선망을 사용할 경우**

  노트북이나 모바일 기기로 업무를 볼 경우 와이파이를 이용하게 되지요. 공개된 무선망은 불특정 다수가 무선접속장치(AP, 흔히 ‘공유기’라고 부르는 장비)를 통하여

인터넷을 이용할 수 있는 망입니다. 흔히 카페, 도서관, 교통시설, 공공기관 등에 설치된 와이파이를 지칭합니다. 개인정보처리자가 직원의 업무처리 목적으로 사무실, 회의실 등에 무선접속장치(AP)를 설치하여 운영하는 경우는 공개된 무선망으로 간주하지 않고 CDMA, WCDMA 등의 기술을 사용하는 이동통신망 역시 공개된 무선망으로 간주하지 않습니다. 이런 구분이 존재하는 이유는 '공개된' 무선망을 이용해 개인정보 취급 업무를 할 경우 추가적인 보안 조치를 요구하기 때문인데요. 단체 내부 와이파이를 사용하는 경우에도 (설령 법적 요건이 아니더라도) 보안 조치는 중요하므로, 이 가이드에서는 '공개된' 무선망과 그렇지 않은 무선망을 따로 구분해서 생각하지 않습니다. 가장 먼저, 안전한 무선망을 이용해야 합니다. 안전하다는 것은 다음과 같은 특징을 말합니다.

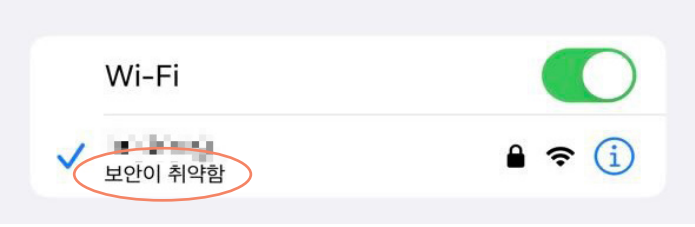
- 설치자/관리자를 신뢰할 수 있다
- 안전한 비밀번호를 적용했다
- WPA2 이상의 보안 프로토콜을 사용한다

우선 와이파이 접속 시 비밀번호를 입력하게끔 되어 있는 것을 사용해야 합니다. 또, 비밀번호를 입력한다고 반드시 안전한 보안 프로토콜을 사용하는 것은 아닌데요. 비밀번호 자체와 상관없이 해당 와이파이에 걸린 '암호화 기술'의 수준이 낮을 수 있다는 말입니다. 암호화 기술 즉

보안 프로토콜의 수준은 보통 와이파이에 접속한 다음
해당 와이파이 세부정보 화면에서 확인할 수 있습니다.

- **아이폰 등 iOS 기기를 사용할 때**

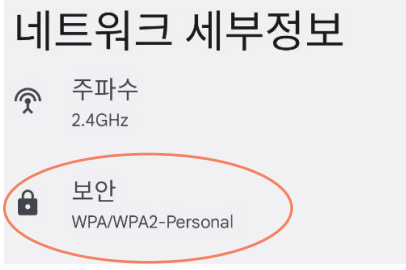
  WPA2 미만의 구형 보안 프로토콜을 이용하는
  네트워크에 접속하면 네트워크 이름 옆에
  “보안이 취약함”이라고 표시됩니다.
  와이파이 비밀번호를 입력할 때, 혹은 접속 후
  네트워크 세부정보 화면에서 확인할 수 있습니다.



iOS 기기의 와이파이 네트워크 목록

- **안드로이드 기기를 사용할 때**

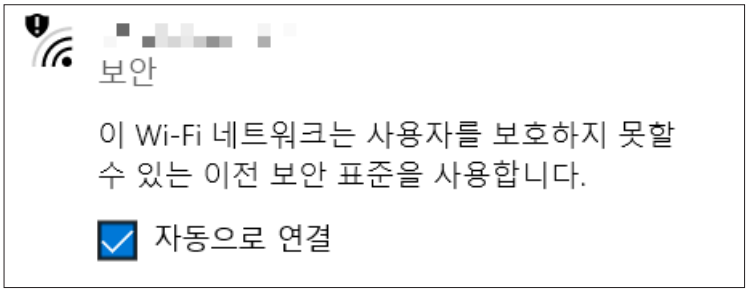
  접속 후 해당 네트워크 세부 정보로 들어가면
  보안 프로토콜이 표시됩니다.



안드로이드 기기의 네트워크
세부정보 화면

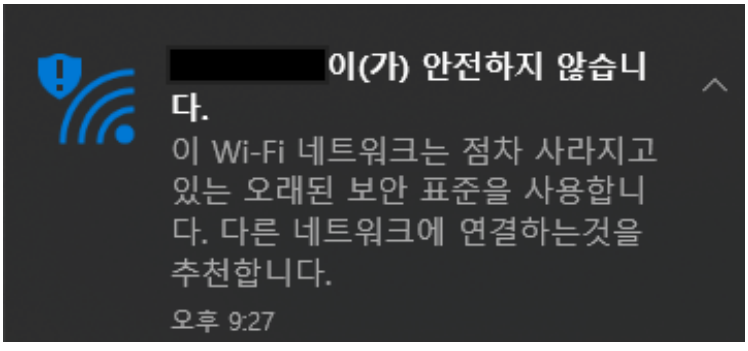
- **윈도우 기기를 사용할 때**

구형 보안 프로토콜을 사용하는 와이파이의 경우
와이파이 목록에서 경고문이 표시됩니다.



윈도우 기기의 와이파이 보안 관련 경고문 (목록에서)

구형 암호화 기술을 적용한 와이파이에 접속했을 경우
해당 네트워크가 안전하지 않다는 메시지가 나옵니다.
(표현 방식은 윈도우 버전에 따라 달라질 수 있습니다.)



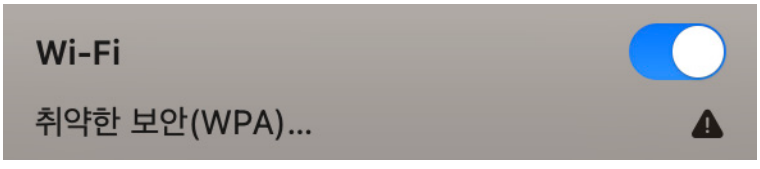
윈도우 기기의 와이파이 보안 관련 경고문 (접속 후)

- **macOS 기기를 사용할 때**

  와이파이에 접속하기 전, 비밀번호를 입력하는 화면에서
  해당 와이파이의 보안 프로토콜을 확인할 수 있습니다.
  (WPA2 혹은 WPA3 프로토콜이 바람직합니다.)

macOS 기기의 와이파이 접속 화면

구형 암호화 기술을 적용한 와이파이에 접속했을 경우
와이파이 상세 정보에서 보안이 취약하다는 메시지가 나옵니다.



macOS 기기의 와이파이 보안 경고

고유식별정보 등 개인정보가 포함된 파일을 이메일/메신저 등 온라인으로 전달하는 경우에는 파일에 비밀번호를 걸어 저장한 후 송신합니다. 공개된 무선망이건 아니건 개인정보 파일은 비밀번호 적용을 권장합니다.

개인정보처리시스템에 비밀번호를 입력하는 등 중요한 개인정보를 전송할 경우에는 전송 암호화 기능이 적용된 조건에서 전송해야 합니다. (전송 '암호화' 기술과 와이파이 '비밀번호'는 별개의 개념이라는 점을 기억합시다!) 예를 들어 웹브라우저에서 주소가 http://가 아니라 https://로 시작하는 경우, SSL 암호화 기술이 적용된 것으로 볼 수 있습니다. 메신저를 이용할 경우에도 암호화 기술이 적용된 상황에서 이용해야 합니다. 메신저의 암호화와 안전한 이용에 관해서는 〈디지털 보안 가이드〉 5장 "통신, E-Mail 및 메신저 보안"을 참고하세요.

카페 같은 곳에 설치된 무선망은 적절한 보안 프로토콜을 사용하더라도 엄밀히 말해 100% 신뢰할 수는 없습니다. 누군가 악의적으로 설치했거나, 제대로 관리가 되지 않고 있을 가능성을 배제할 수 없기 때문입니다. 이처럼 안전을 보증할 수 없는 환경이나 공개된 장소에서는 개인정보 관련 업무를 취급하지 않는 것을 원칙으로 하는 것이 바람직합니다. 정말 부득이하게 이런 환경에서 무선망을 사용할 경우에는 WPA2나 WPA3 보안 프로토콜을 사용하는 무선망인지

확인하고, 파일 및 전송 암호화를 반드시 적용하여 혹시 모를 위험에 대비하도록 합시다. 휴대폰 데이터를 테더링해서 이동통신망을 이용하는 것도 고려해 볼만합니다.

자동 접속 차단

개인정보처리시스템의 경우, 일정시간 이상 사용하지 않으면 자동으로 시스템 접속을 차단하는 세션 타임아웃을 적용해야 합니다. 보통 '자동 로그아웃'이라고 부르는 기능에 해당합니다.

일반 구글 계정의 경우 수동으로 로그아웃하기 전까지는 브라우저를 껐다 켜도 로그인 상태가 유지되므로 주의할 필요가 있습니다. (구글 워크스페이스 유료 버전 일부 요금제에서는 사용자 '세션 길이'를 설정할 수 있고, 기본값은 14일입니다.) 공용 장비에서는 사생활 창을 이용하면 창을 닫을 때 자동으로 로그아웃되는 특성을 활용할 수 있고, 아래 설명하는 것처럼 기기 자체에 시간 제한을 걸어두는 것도 방법입니다.

업무용 컴퓨터 역시 사용하는 응용프로그램/업무의 특성/위험의 정도 등을 고려해 사용자가 일정시간 이상 업무 처리를 하지 않는 경우 자동으로 접속을 차단 후, 재접속은 최초 로그인과 동일한 방법으로 접속하도록 합니다. OS 설정에서 잠금 화면 시간 제한을 적용하고,

다시 시작할 때 로그인 화면을 띄우는 설정을 켜둡니다.

비밀번호 설정

업무용 모바일 기기(스마트폰, 태블릿PC 등)는 비밀번호 설정 등 보호조치를 취해야 합니다. 기기 보안에 관해서는 〈디지털 보안 가이드〉 2-1장 “비밀번호”와 4-3장 “스마트폰 자체의 보안”을 참고하세요.

모바일 기기는 기기에 저장된 개인정보나 해당 기기를 통한 개인정보처리시스템 접속뿐만 아니라 각종 인증수단이나 메신저 등 연락망을 포함하는 경우가 많기 때문에 분실·도난 시 큰 위험이 생깁니다. 따라서 최소한 비밀번호 설정 등의 조치를 통해 보호하는 것이 좋습니다.

개인정보 유출 시도 탐지 및 대응

그밖에 제6조제1항제2호에서는 개인정보 유출 시도를 탐지 및 대응할 것을 요구합니다. 시스템에 접속한 IP 주소 등을 분석하여 유출 시도가 있었는지 확인하고, 만약 확인이 될 경우 해당 IP 주소에 대한 접근을 차단하는 등의 조치를 해야 한다는 것입니다. 그밖에 침입차단 기능을 갖는 장비를 운용하는 등 여러 방안을 권고하고 있습니다 (〈안전조치 기준 해설서〉).

개인정보 유출 시도 탐지 및 대응은 서버를 관리하는 업체의 역할이라고 볼 수 있습니다. 우리 단체에서 처리하는 개인정보가 유출 시도로부터 안전한지 확인하기 위해서, 이용하는 CRM 업체가 어떤 조치를 취하고 있는지 확인하는 것을 권장합니다. 사용하는 툴의 공식 문서나 개인정보처리방침에 해당 내용이 기재되어 있는지 확인하고, 만약 유출 시도가 발생했을 경우 이용자인 우리 단체는 그 사실을 어떻게 알 수 있는지, 어떻게 대응할 수 있는지 등을 문의해 보는 것도 좋습니다.

구글 드라이브 같은 범용 툴의 경우 평소와 다른 위치 또는 기기에서 로그인을 시도하는 등 보안상 위험이 발생했을 때 해당 접속을 차단하고 '의심스러운 로그인이 차단되었습니다'라는 연락을 주기도 합니다. 이런 연락을 받으면 계정 관리 페이지에 들어가 비밀번호를 변경하는 등 안전 점검 조치를 하는 것이 좋습니다.[5]

한편 이를 악용하여 '개인정보가 유출되었으니 손해배상을 하겠다'거나, 새로 로그인하라거나, 무언가를 설치하라는 식의 이메일이나 메시지를 보내, 중요한 정보를 빼내거나 악성프로그램 설치를 유도하는 피싱 사기도 종종 발생합니다. 이런 연락을 받았을 경우에는 보낸 사람의 메일주소가 실제 기관이나 업체의 메일주소인지 확인하고, 해당 기관/업체에 연락하여 그런 공지를 내보낸 적이 있는지

문의하는 등 의심하는 마음을 가질 필요가 있습니다.

개인정보 유출뿐만 아니라 전반적인 보안 사고가
발생했을 경우 대처 방법은 〈디지털 보안 가이드〉 9장
“이미 벌어진 보안 사고 대처하기”를 참고하세요.

제7조 개인정보의 암호화

① 개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송·수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

② 개인정보처리자는 다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

1. 주민등록번호
2. 여권번호
3. 운전면허번호
4. 외국인등록번호
5. 신용카드번호
6. 계좌번호
7. 생체인식정보

③ 개인정보처리자는 이용자가 아닌 정보주체의 개인정보를 다음 각 호와 같이 저장하는 경우에는 암호화하여야 한다.

1. 인터넷망 구간 및 인터넷망 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우
2. 내부망에 고유식별정보를 저장하는 경우(다만, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다)

가. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
나. 암호화 미적용시 위험도 분석에 따른 결과

④ 개인정보처리자는 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다.

⑤ 개인정보처리자는 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

⑥ 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

안전조치 기준 제7조는 개인정보를 저장하거나 송수신할 때 암호화 처리하도록 하는 내용입니다. 제1~4항은 주로 웹사이트나 개인정보처리시스템을 직접 구축할 때 해당하는 내용입니다. 일상적인 비영리단체 업무에 꼭 해당하는 것은 아니지만, 법령에서 어떤 내용을 강조하는지 살펴보면 유용합니다. 제5항은 중요하니 잘 읽어보세요.

앞서 제6조를 다룰 때 설명한 것처럼, 암호화 관련 조항에서도 “이용자”의 개인정보와 “이용자가 아닌 정보주체”의 개인정보를 구분해서 각기 다른 기준을 적용하고 있습니다. 이용자가 아닌 정보주체의 경우 규칙이 조금 덜 엄격한 것이죠. 이 가이드에서는 비영리단체 특성상 ‘이용자’의 개념이 때로 모호할 수 있는 점, 그리고 일반적인 개인정보 보호의 관점에서 모든 정보주체의 개인정보를 안전하게 관리하는 것이 바람직하다는 점을 고려해서 둘을 엄격히 구분하지 않고 서술합니다.

암호화란?

‘암호화’는 어떤 문구를 다른 암호문으로 변환하여, 사전에 약속된 암호키를 알지 못하는 사람은 알아볼 수 어렵게 만드는 과정을 말합니다. 사실 암호화는 비단 개인정보뿐만 아니라 디지털 정보 전반에 있어 중요한 도구입니다. 암호화 방법에 관한 자세한 설명은 〈디지털 보안 가이드〉 4-1장 “파일과 저장기기”를 참고하세요.

안전조치 기준을 읽어보면 ‘안전한 암호 알고리즘’이라는 표현이 여러 번 등장합니다. <개인정보의 암호화 조치 안내서>(개인정보보호위원회·한국인터넷진흥원, 2020)를 보면 암호화에 사용할 수 있는 암호 알고리즘을 권고하고 있는데요. 통상 사용하는 아래아한글이나 엑셀 등의

프로그램에서 문서 비밀번호를 지정할 때는 안전한 암호 알고리즘이 적용된다고 이해해도 좋습니다.

일반적으로 비영리단체가 암호화를 직접 구현할 일은 잘 없기에 해당 알고리즘을 기술적으로 파악할 필요까지는 없지만, 이런 사항이 존재한다는 것을 인지하고 웹사이트나 개인정보처리시스템을 제작/활용할 때 개발자 및 서비스 제공 업체 측에 확인해 보면 안전조치 기준 이행에 도움이 될 수 있습니다.

인증정보의 암호화

제1항은 비밀번호, 생체인식정보 등 인증정보의 암호화를 다룹니다.

정보통신망을 통해 인증정보를 송·수신할 경우 SSL 등의 암호화 기술을 활용해야 합니다. 단체 웹사이트에 회원이 로그인하는 경우, CRM 시스템에 담당자가 로그인하는 경우 등 각종 상황에 모두 적용됩니다. 또, DB 또는 파일에 비밀번호를 저장할 때는 '원본 값을 유추하거나 복호화 할 수 없는 암호화 방법'인 일방향 암호화를 적용해야 합니다.

우리 단체의 디지털 환경에서 이러한 사항이 지켜지고 있는지 웹사이트 개발자나 개인정보처리시스템

업체 등과 소통하여 확인하시기 바랍니다.
한편 일상적인 업무에서, 예컨대 특정 비밀번호를 바탕화면에 일반 텍스트 파일로 저장해놓는다거나 할 경우 문제의 소지가 있다는 뜻도 됩니다. 보안상 위험한 것은 당연하고요.

반드시 암호화해야 하는 개인정보

제2~3항은 반드시 암호화해서 저장해야 하는 개인정보 유형을 제시합니다. 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 생체인식정보 등입니다.

제3항에서는 이용자가 아닌 정보주체의 개인정보에 관해 조금 더 완만한 암호화 요건을 제시하는데요. 앞서 설명한 이유에 따라 우리 가이드에서는 '이용자 / 이용자가 아닌 정보주체'를 엄격히 구분하지 않기 때문에 이 항목의 내용은 자세히 설명하지 않습니다. (내부 인트라넷이나 자체 이메일 서버 등을 운영하지 않는 비영리단체의 경우 여기서 언급하는 DMZ나 내부망 역시 거의 해당할 일이 없다고 보면 됩니다.)

제4항의 내용은 제1항에서 다룬 것과 유사한데요. 인터넷을 통해 (인증정보뿐만 아니라) 모든 개인정보를 송·수신할 때 암호화해야 한다는 것입니다. 예를 들면 단체 웹사이트에서 회원 가입을 받는 경우, 이용자가 회원 가입 양식에 입력한

개인정보를 송·수신할 때에는 SSL 등 통신 암호 프로토콜 탑재 기술을 활용하여 암호화 전송해야 합니다. 이 또한 웹사이트 개발자 등과 소통하여 확인이 필요한 부분입니다.

개인정보를 기기에 저장할 때 암호화

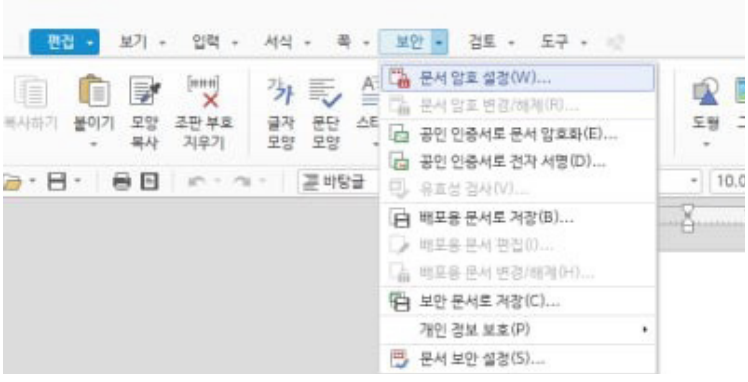
제5항에서는 개인정보를 담당자 기기/보조저장매체에 저장할 때 암호화가 필요한 경우를 설명합니다.

원칙적으로 모든 개인정보를 저장할 때는 암호화하는 것이 좋습니다. (안전조치 기준에서는 암호화해야 하는 대상을 '이용자의 개인정보' 또는 '이용자가 아닌 정보주체의 고유식별정보, 생체인식정보'로 규정합니다. 앞서 언급한 이유로 여기서도 이용자와 이용자가 아닌 정보주체를 따로 구분하지는 않겠습니다.)

암호화 방식은 크게 두 가지로 나누어 생각할 수 있습니다. 하나는 개인정보가 포함된 파일에 개별적으로 암호를 거는 것입니다. 특히 회원명부를 파일 형식으로 다운로드하여 작업하거나 공유할 경우에는 반드시 파일에 비밀번호를 설정하도록 합니다. 이렇게 하면 예컨대 이메일을 엉뚱한 수신인에게 보내는 등의 실수가 발생하더라도 받는 사람이 파일을 열어볼 위험을 줄일 수 있습니다.

엑셀이나 워드, 한글 등의 프로그램에서 제공하는 보안 기능을 이용해 비밀번호를 적용할 수 있습니다. 예를 들어 엑셀에서는 [정보 > 통합 문서 보호 > 암호 설정] 메뉴를, 한글에서는 [보안 > 문서 암호 설정]을 사용합니다. (메뉴 이름 및 위치는 프로그램 버전에 따라 다를 수 있습니다.) 이때 사용하는 암호는 다른 계정 비밀번호를 재활용하지 말고, 파일 고유의 암호를 지정하도록 합니다.

엑셀의 문서 암호 설정



한글의 문서 암호 설정

업무용 컴퓨터의 드라이브나 USB 메모리 등을 통째로 암호화하는 방법도 있습니다. 이 방법은 기기나 보조저장장치를 누군가 가져가더라도 드라이브 내용물을 보기 어렵게 해줍니다. 파일 암호화와는 상호보완적인 관계라고 볼 수 있습니다. (드라이브 암호화를 하더라도, 암호화되지 않은 개인정보 파일을 제3자에게 보내면 열어볼 수 있습니다.)

드라이브 암호화에는 윈도우 비트로커(Bitlocker), 맥 파일볼트(FileVault) 등을 활용할 수 있는데요. 자세한 방법은 〈디지털 보안 가이드〉 4-1장 “파일과 저장기기”를 참고하세요.

개인정보 다운로드 시 자동으로 비밀번호를 적용하는 기능. 이미지 출처: 도너스

CRM 툴에 따라서는 개인정보를 다운로드받을 때 자동으로 비밀번호가 적용되도록 설정할 수 있는 경우도 있습니다.

제6항 암호 키 관리절차에 관한 내용은 100만명 이상의 개인정보를 다루는 단체에 해당하기 때문에 이 가이드에서는 다루지 않습니다. 더 자세히 알고 싶은 분은 〈디지털 보안 가이드〉 5-1장 “통신 보안의 이해”를 참고하세요.

제8조 접속기록의 보관 및 점검

① 개인정보처리자는 개인정보취급자의 개인정보처리시스템에 대한 접속기록을 1년 이상 보관·관리하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 2년 이상 보관·관리하여야 한다.

1. 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우
2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우
3. 개인정보처리자로서 「전기통신사업법」제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우

② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보의 다운로드가 확인된 경우에는 내부 관리계획 등으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.

③ 개인정보처리자는 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하기 위한 조치를 하여야 한다.

접속기록을 보관하고 점검하는 주된 목적은 혹시라도 개인정보 침해사고가 발생할 경우 그 경위를 파악 및 분석하기 위해서입니다.

접속기록이란?

개인정보취급자가 개인정보처리시스템에 접속해서 수행한 업무내역의 기록으로 식별자, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무를 포함해야 합니다. 즉 누가, 언제, 어디서, 누구에 대한 정보로, 무엇을 했는지에 관한 기록입니다.

- 식별자: 개인정보처리시스템에서 접속자를 식별할 수 있는 ID 등 계정 정보
- 접속일시: 접속한 시점 또는 업무를 수행한 시점
- 접속지 정보: 접속한 자의 PC, 모바일기기 정보 또는 서버의 IP주소 등 접속 주소
- 처리한 정보주체 정보: 개인정보취급자가 누구의 개인정보를 처리하였는지를 알 수 있는 식별정보(ID, 고객번호, 학번, 사번 등)
- 수행업무: 개인정보취급자가 개인정보처리시스템에서 개인정보를 처리한 내용을 알 수 있는 정보

접속기록을 보관하는 법

그렇다면 접속 기록을 어떻게 보관하면 될까요? 담당자가 특정 회원 정보를 열람할 때마다 업무 내용을 일일이 적어둘 수는 없는 노릇일 텐데요. CRM 등 회원관리 툴에서는 접속기록 보관에 관한 기능(이른바 '감사' 기능)을 제공하는 것이 일반적입니다.

접속기록 목록의 예. 이미지 출처: 도너스

예를 들어 도너스에서는 [정보보호 〉 감사] 메뉴에서 접속 기록을 확인할 수 있습니다. 사용하는 시스템의 접속기록 보관 및 확인 방법을 모를 경우 공식문서를 확인하거나 업체에 문의하여 확인할 수 있습니다.

CRM 시스템에 따라서는 실무자가 개인정보를 다운로드할 때 사유를 입력하게끔 되어 있는 경우가 있는데, 이를 활용하여 사유를 기록해 두는 것이 좋습니다.

구글 드라이브 등 클라우드 기반 협업 서비스에서 개인정보를 처리하는 경우에는 접속기록 보관이 더 어렵습니다. 구글 드라이브의 경우 개별 문서의 수정 이력 정도는 기록이 남지만 자세한 접속 기록은 제공되지 않아, 일반 계정으로 사용할 때 법령에서 요구하는 수준의 접속기록 보관은 사실상 불가능합니다.

다만 유료 버전인 구글 워크스페이스에서는 접속기록 확인용 감사 도구를 관리자에게 제공하며, 이를 통해 접속기록을 보관 및 점검할 수 있습니다. 정식 등록된 비영리단체의 경우 구글 워크스페이스 무료 이용을 신청할 수 있으니 가급적 활용하는 것이 좋습니다.[6]

접속기록의 보관 기간은 기본적으로 1년 이상이되, 제1항에 서술된 대로 5만명 이상의 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하거나, 기간통신사업자일 경우에는 2년 이상입니다. 예를 들어 우리 단체가 회원의 (생년월일이 아니라) 주민등록번호를 수집할 경우에는 고유식별정보에 해당하기 때문에 접속기록을 2년 이상 보관해야 합니다.

- **고유식별정보란?**
  - 주민등록번호, 운전면허번호, 여권번호, 외국인등록번호

- **민감정보란?**
  - 사상·신념에 관한 정보
  - 노동조합·정당의 가입·탈퇴에 관한 정보
  - 정치적 견해에 관한 정보
  - 건강, 성생활 등에 관한 정보 (병력, 장애여부 및 등급 등)
  - 유전자검사 등의 결과로 얻어진 유전정보

- 범죄경력자료
- 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 개인을 특정할 수 있는 것 (생체인식정보: 얼굴, 지문, 홍채 등)
- 인종이나 민족에 관한 정보

또한 제8조제3항에서는 접속기록을 “안전하게 보관하기 위한 조치”가 필요하다고 명시합니다. 접속기록 자체를 조작하여 개인정보 오남용 사실을 확인하기 어렵게 만들 수 있기 때문입니다. 안전한 보관을 위해서 비영리단체는 접속기록을 수정/삭제할 수 있는 관리자 계정에 대한 접근권한 통제를 확실히 실시하도록 합니다. 외부 CRM 도구를 사용할 경우 접속기록의 보관과 백업이 어떻게 이루어지는지 해당 업체에 문의하여 확인합니다.

접속기록의 점검

보관한 접속기록은 월 1회 이상 점검해야 합니다.

취급자가 개인정보를 다운로드한 기록이 있을 경우 내부 관리계획에 따라 사유를 확인해야 하는데요. 일반적인 업무 상황에서는 접속기록에 남아 있는 다운로드 목적을 확인하는 것으로 갈음할 수 있지만 특수한 상황에서는 개인정보 보호책임자의 추가 확인이 필요할 수 있습니다.

다운로드 사유를 추가적으로 확인하는 기준은 법에서 정해진 것은 아니고, 내부 관리계획을 통해 상식적인 선에서 정하면 됩니다. 예를 들어 '일평균 처리건수에 비해 과도하게 다운로드한 경우', '업무시간 외에 단시간 여러 번 다운로드한 경우' 등이 있습니다.

비인가된 개인정보에 대한 처리, 대량의 다운로드 등 비정상 행위가 발견될 경우 추가 조사를 진행하거나 해당 개인정보취급자에게 소명을 요청하는 등 대응조치를 수행해야 합니다. 비정상 행위의 범주 또한 내부 관리계획을 통해 정할 수 있는 사항입니다. 예를 들어 다음과 같은 것들이되, 단체의 사정에 맞게 적절한 판단이 필요합니다.

- 접근권한이 부여되지 않은 계정으로 접속
- 출근시간 전, 퇴근시간 후, 새벽시간, 휴무일 등 업무시간 외에 접속
- 인가되지 않은 단말기 또는 지역에서 접속
- 특정 정보주체를 과도하게 조회하고 다운로드하는 등의 행위
- 대량의 개인정보를 조회, 정정, 다운로드, 삭제하는 등의 행위
- 짧은 시간에 하나의 계정으로 여러 지역에서 접속

법으로 요구되는 접속기록 점검을 활용하여 불필요한 개인정보 파일 파기, 접근권한 관리 등 안전조치 전반에 대한 정기점검을 수행하는 것도 좋습니다.

제9조 악성프로그램 등 방지

① 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 프로그램의 자동 업데이트 기능을 사용하거나, 정당한 사유가 없는 한 일 1회 이상 업데이트를 실시하는 등 최신의 상태로 유지
2. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

② 개인정보처리자는 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 이에 따른 업데이트 등을 실시하여야 한다.

보안 프로그램 설치

개인정보를 다루는 업무용 컴퓨터에는 보안 프로그램을 설치하고 활성화해야 합니다. 보안 프로그램은 운영체제(OS) 차원에서 제공하는 도구를 활용하거나, 별도 보안 프로그램을 사용할 수 있습니다.

윈도우 시스템의 경우 “Windows 보안” 프로그램이 기본적으로 제공됩니다. 이런저런 이유로 이 프로그램을 꺼두는 경우도 있는데, 이 프로그램을 사용하려면 [설정 〉 Windows 보안]에 들어가서 [실시간 보호] 옵션이 켜져 있는지 확인하도록 합니다.

기본 Windows 보안 프로그램 외에 다른 추가 보안 프로그램을 사용하는 경우도 있을 수 있습니다. 각각의 장단점이 달라 어느 정도 관련 리서치를 하는 편이 좋은데요. 예를 들어 무료 백신의 경우, 보안 기능을 미끼로 컴퓨터에 저장된 개인정보를 탈취해 가는 사실상 스파이웨어인 경우도 종종 있기 때문에 주의가 필요합니다. 보안 프로그램 선택에 관해서는 〈디지털 보안 가이드〉 4-2장 “컴퓨터 운영체제의 보안”을 참고해주세요.

맥 시스템의 경우 XProtect라는 내장 보안 프로그램이 항상 활성화되어 있습니다.

보안 업데이트 적용

윈도우나 맥이나 OS 업데이트에 보안 관련 최신 대응이 담겨 있는 경우가 많으므로, 시스템 설정에서 OS를 항상 최신 버전으로 관리하는 것이 좋습니다. 또 본 조 제2항에서 보안 업데이트를 즉시 실시하지 않을 수 있는 ‘정당한 사유’는 무결성 테스트나 보안 업데이트 적용

시 개인정보처리시스템에 미치는 기술적 영향을 사전 점검하는 데 필요한 현실적인 시간을 말하며, 일반적인 업무 상황에서는 해당사항이 없다고 보면 됩니다. 보안 업데이트가 생기면 바로바로 업데이트를 실행해주도록 합시다.

제10조 물리적 안전조치

① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.
② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.
③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다.
다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

안전조치 기준 제10조제1항은 개인정보를 보관하는 물리적 장소(전산실, 자료보관실)가 따로 있는 경우에 해당합니다. 예전에는 서버실 등을 직접 운영하는 경우가 있었지만 요즘은 보기 힘들지요. 다만 단체에 따라 상담 내용이나 기타 개인정보가 담긴 자료를 특정 공간에 보관하는 경우도 있으니, 이 경우에는 적절한 안전조치가 필요합니다.

물리적 장소에 대한 안전조치의 예로는
출입통제장치(번호, 카드, 자물쇠, 지문 등)를 설치하거나,

출입자, 출입일시, 출입목적, 소속 등을 확인할 수 있는 출입대장을 기록·관리하는 방법 등이 있습니다.

별도 공간이 없더라도 개인정보가 포함된 서류나 USB 메모리 등을 다루는 경우는 있지요. 제2항에 해당하는 내용입니다. 개인정보가 포함된 문서나 USB 등은 꼭 잠금 장치가 설치된 캐비닛, 서랍 등에 보관하고, 회원 명부가 책상에 놓여 있거나 해서는 곤란합니다.

제3항은 개인정보처리시스템을 직접 운영하는 경우 (예: 회원 DB을 서버실에서 관리), 해당 시스템에서 데이터를 USB 등에 담아 반출하는 경우에 대비해 보조저장매체 관련 보안대책을 명시적으로 마련해야 한다는 내용입니다. 관련 정책 및 절차를 마련하여 관리대장을 운영하고, 별도 승인이 있어야만 USB 읽기/쓰기가 가능하게 해주는 보조저장매체 통제 솔루션 도입 등 여러 방법이 있습니다. 이 가이드에서 상정하고 있는 독자와는 다소 거리가 있는 내용입니다.

제11조 재해·재난 대비 안전조치

> 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 다음 각 호의 조치를 하여야 한다.
> 1. 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검
> 2. 개인정보처리시스템 백업 및 복구를 위한 계획을 마련

안전조치 기준 제11조는 외부의 불가항력으로 시스템에 문제가 생기는 상황을 다루고 있습니다. 다만 이 조항이 비영리단체에 적용되려면 100만명 이상의 개인정보를 다루어야 하는데, 이 가이드에서 상정하고 있는 독자와는 거리가 있기에 자세히 설명하지는 않습니다.

다만 위기대응 관점에서, '재해·재난 상황에 어떻게 대처할 것인가?'라는 고민을 조직 차원에서 해보는 것은 유용할 수 있습니다. 모든 시나리오에 완벽한 해답을 마련해 둬야만 하는 것은 아니지만, 몇 가지 상황을 가정해봄으로써 조직의 회복탄력성, 유사시 기민하게 대응할 수 있는 역량에도 보탬이 될 수 있습니다.

특정한 인프라가 오작동할 경우 조직의 사업은 어떻게 영향을 받고, 그 상황에서 가장 우선적으로 해야 할 일은 무엇일까요?

- 회원관리서비스가 다운돼서 접속이 되지 않는다면 어떻게 대응해야 할까요?
- 카카오톡이나 이메일, 구글 드라이브가 먹통이 된다면?
- 사무실 인터넷과 전기가 끊긴다면?

CRM 등 제3자가 제공하는 개인정보처리시스템을 활용한다면, 해당 업체가 재해·재난 대비 안전조치를 어떻게 하고 있는지 문의해서 확인해 보는 것을 권합니다. 특히 중요한 정보에 접근할 수 없는 상황에 대비해, 다른 서비스나 외장하드 등에 데이터를 백업하고 안전하게 보관하는 작업을 주기적으로 수행하는 것도 좋습니다.

검색엔진에 "개인정보처리시스템 재해재난 대비 위기대응" 키워드를 찾아보면 공공기관에서 작성한 위기대응 매뉴얼 사례를 찾을 수 있습니다. 이들 자료를 참고하여 위기시 대응 순서, 담당자 및 비상연락망, 우선순위 설정 등의 고려사항을 살펴보는 것을 권합니다.

제12조 출력·복사시 안전조치

① 개인정보처리자는 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하여야 한다.
② 개인정보처리자는 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 안전조치를 하여야 한다.

'개인정보의 출력'이란 종이 인쇄, 화면상 표시, 파일 생성 등 어떤 매체로건 개인정보를 표현하는 행위를 말합니다.

개인정보를 출력할 때는 '용도를 특정'해야 합니다. 예를 들어 일부 툴에서 회원정보를 엑셀로 다운받기 위해서는 사유를 입력하여 기록을 남기도록 되어 있는데요. 이런 식으로 설명할 수 있는 목적이 필요하다는 것입니다. 이 목적은 안전조치 기준 제8조에서 보관하도록 요구하는 접속 기록의 '수행업무'에 해당한다고 볼 수 있습니다.

용도에 따라 '출력 항목을 최소화'해야 합니다. 다시 말해 목적 달성에 필요 없는 개인정보는 출력하지 않도록 합니다.

예컨대 최근 1개월 사이 가입한 신규 회원 안내문 발송을 위해 회원 목록을 출력한다면, 가입한 지 1개월이 넘은 기존 회원의 개인정보는 출력하지 않습니다. 또, 안내문 발송에 필요하지 않은 주민등록번호 등의 정보 역시 출력할 필요가 없겠습니다.

'숨김 처리'와 '출력하지 않는다'는 반드시 같지 않습니다. 예컨대 스프레드시트 파일에서 주민등록번호 열을 '숨기기'하면, 화면에는 보이지 않더라도 해당 필드를 숨김해제 처리하여 다시 열람할 수 있습니다. 파일 형식으로 저장할 때는 불필요한 개인정보를 확실히 삭제하는 것이 좋습니다.

웹사이트 설계상에 허점이 있을 경우, 웹페이지 소스 보기 등을 통해서 불필요한 개인정보가 출력되는 것 또한 가능합니다. 일반적인 단체에서 이러한 부분을 직접 관리하기는 어렵지만, 이런 일이 발생할 수 있다는 가능성을 인지하고 개발자/시스템 제공업체 등과 해당 위험이 어떻게 방지되고 있는지 커뮤니케이션하는 것이 좋습니다.

개인정보처리시스템과 직접 관련된 내용은 아니지만, 실무 과정에서 많이 발생하는 한 가지 실수는 이메일 주소 유출입니다. 회원이나 이해관계자에게 단체공지를 이메일로 전달하는 과정에서 각 수신자를 '숨은참조'로 입력하거나 별도의 메일링리스트를 사용하는 대신, 일반 수신자 항목에 모든 이메일 주소를 입력하는 것입니다.

이렇게 이메일을 보낼 경우 받는 사람이 다른 수신자의 이메일 주소도 전부 확인할 수 있기 때문에 개인정보 유출이 될 수 있습니다. 그중 한 명이 '전체회신'으로 답장을 보내기라도 하면 더 골치 아파지겠죠. 이메일 발송 전에 수신인 항목을 잘 확인하여 이런 일을 미연에 방지합시다.

또한 종이 인쇄물이나 USB 등 외부 저장매체에 개인정보를 출력·복사해서 사용할 경우에도 안전조치가 필요합니다. 여기서 말하는 안전조치는 예를 들어 출력·복사 기록이나 외부 반출입 관리대장 등인데요. (<안전조치 기준 해설서>) 안 그래도 일손이 부족한 비영리단체에서 서류 및 저장매체 관리대장까지 운영하기에는 부담이 있을 수 있습니다. 가급적 개인정보를 인쇄물·외부 저장매체에 출력·복사하는 일을 삼가는 것이 좋습니다.

제13조 개인정보의 파기

① 개인정보처리자는 개인정보를 파기할 경우
다음 각 호 중 어느 하나의 조치를 하여야 한다.
1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비(자기장을 이용해 저장장치의
데이터를 삭제하는 장비)를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행
② 개인정보처리자가 개인정보의 일부만을 파기하는 경우,
제1항의 방법으로 파기하는 것이 어려울 때에는
다음 각 호의 조치를 하여야 한다.
1. 전자적 파일 형태인 경우 : 개인정보를 삭제한
후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인
경우 : 해당 부분을 마스킹, 구멍 뚫기 등으로 삭제
③ 기술적 특성으로 제1항 및 제2항의 방법으로 파기하는
것이 현저히 곤란한 경우에는 법 제58조의2에 해당하는
정보로 처리하여 복원이 불가능하도록 조치를 하여야 한다.

보관 기한이 지났거나 용도를 다한 개인정보는 파기해야 합니다. 불필요한 개인정보 파기를 통해 개인정보 유출 및 노출을 예방할 수 있고, 유출이나 노출이 발생하지 않더라도 파기해야 할 개인정보를 파기하지 않고 보관하는

행위는 과태료 부과 대상이 될 수 있습니다. 보관 기한이 지난 개인정보는 바로바로 파기하고, 정기점검을 실시하여 미처 파기하지 못한 사례를 찾아 시정하도록 합니다.

보관 기한은 보통 개인정보 처리방침에서 명시하게 되어 있습니다. 일시적 개인정보 수집(구글 설문지를 통한 캠페인 참여, 탄원서 제출 등) 및 제3자 제공(단체 간 공동활동 등)의 경우에도 마찬가지로 단체의 개인정보 처리방침이나 정보 수집 서식 등에 안전한 관리 방안을 명시하고 따르도록 합니다. 개인정보 처리방침 작성에 관한 구체적인 설명은 〈비영리단체를 위한 개인정보 처리방침 권고안〉(2022)[7]을 참고하세요.

안전조치 기준 제13조제1항에서는 완전파괴(소각, 파쇄), 전용 소자장비(디가우저), 초기화/덮어쓰기 등 무서운 단어가 등장합니다.

개인정보가 포함된 종이문서의 경우에는 파쇄해야 합니다. 나무를 아끼는 마음에서 종이문서를 이면지로 사용하는 경우가 있는데, 절대 그러면 안 됩니다! 파쇄할 때 손으로 찢어 버리는 정도로는 충분하지 않습니다. 문서세단기나 파쇄 전문 업체를 활용해 확실히 처리하도록 합니다.

디지털 정보의 경우, 제13조제1항에서 설명하는 내용은 하드디스크 등을 통째로 파기해야 할 때 해당합니다.

윈도우에서는 소거 프로그램을 다운받아 사용할 수 있고, 맥에서는 기본 내장된 '디스크 유틸리티'에서 해당 내용을 제공합니다. 데이터가 복원되지 않도록 하는 방법은 예컨대 다음과 같은 것이 있습니다.

- 3회 이상 되풀이해서 완전포맷 실행 ('빠른포맷'이 아님)
- 데이터 영역에 0, 1 등의 무작위값을 덮어쓰기
- 드라이브를 암호화 저장 후 삭제 및 무작위 값으로 덮어쓰기

하지만 대부분의 업무 상황에서는 드라이브를 통째로 삭제하기보다 자료 중 일부, 개인정보가 담긴 특정 파일을 삭제하는 것이 더 일반적일 텐데요. 제13조제2항이 여기 해당하는 내용입니다.

디지털 파일의 경우, 삭제해야 할 파일을 휴지통에만 넣고 완전삭제하는 것을 잊어버리는 일이 없도록 유의합니다. 개인 컴퓨터 휴지통뿐만 아니라 구글드라이브, 노션 등 클라우드 기반 서비스도 파일 삭제 시 일정 기간 휴지통에 보관하는 경우가 있습니다. 바로 삭제해야 하는 파일은 휴지통에서도 복원이 되지 않도록 신경씁니다.

파일을 삭제하지 않고 특정 개인정보만 삭제하는 경우도 있습니다. 예를 들어 회원 명부 사본 엑셀 파일에서 특정 회원에 해당하는 행을 삭제하거나, 주민등록번호 열을

삭제할 수 있겠지요. 이때 문서 도구나 웹하드 도구의 버전 관리, 수정 이력 관리 기능 때문에 분명히 삭제한 정보를 복원할 수 있는 경우도 발생합니다. 이럴 때는 개인정보가 제거된 문서의 사본을 만들어 해당 사본을 활용하고, 기존 이력이 남아 있는 파일은 삭제하는 등 개인정보를 복구하기 어렵게 만드는 것이 좋습니다.

또한 누군가 실수로 혹은 악의적으로 파일을 복구하는 일이 발생하지 않도록, 정기점검 등을 통해 관련 기록 및 활동을 관리 및 감독해야 합니다. 디지털 정보의 완전한 삭제는 생각보다 까다로워서, 분명히 삭제한 파일도 포렌식 기술을 동원해 복원할 수 있는 경우가 있습니다. 하지만 위에서 언급한 삭제 방식뿐만 아니라 관리/감독 노력을 통해 복원 위험을 줄일 수 있습니다.

디스크나 파일 삭제 방법에 관한 보다 자세한 설명은 〈디지털 보안 가이드〉 4장 “파일과 기기, 운영체제의 보안”을 참고하세요.

기록물, 인쇄물 등 기타 기록매체의 일부만 삭제할 경우에는 삭제할 부분을 사인펜으로 확실히 마스킹하거나 펀치로 구멍을 뚫습니다.

제13조제3항은 블록체인 등 기술적 특성으로 자료의 파기

자체가 불가능한 상황에 해당합니다. 이 가이드북에서 상정하는 상황과는 다소 거리가 있어 자세히 설명하지 않습니다.

3장. 안전성 확보조치 체크리스트

개인정보 안전성 확보조치 이행을 위해 필요한 일반적인 사항을 점검하는 데 활용할 수 있는 체크리스트입니다. 단체의 상황에 따라서는 꼭 들어맞지 않는 내용이 있을 수도 있고, 여기 적힌 내용만으로는 부족함이 있을 수도 있을 텐데요. 비영리단체 맥락에 보다 적합한 개인정보 보호 체크리스트를 앞으로 발전시켜 나갈 필요가 있겠습니다.

개인정보보호 정책, 자원	그렇다	아니다	해당없음
개인정보 보호책임자가 지정되어 있다			
개인정보 보호책임자는 교육, 관리·감독 등 역할을 수행하고 있다			
개인정보의 안전한 처리를 위한 내부 관리계획이 수립되어 있다			
(CCTV 운영시) 개인영상정보 보호책임자 지정 및 역할을 수행하고 있다			

개인정보보호 교육	그렇다	아니다	해당없음
개인정보보호 교육계획이 수립되어 있다			
개인정보 보호책임자가 교육을 받고 있다			
개인정보보호 교육을 수행하고 있다			

개인정보처리방침	그렇다	아니다	해당없음
개인정보처리방침을 공개하고 있다			
개인정보처리방침의 내용(처리 및 보유기간, 위탁사항 등)이 적절하다			
개인정보처리방침의 변경 내용을 지속적으로 공개 및 이력관리한다			

개인정보처리시스템 보안운영	그렇다	아니다	해당없음
개인정보를 처리하는 시스템·업무용컴퓨터에 백신소프트웨어를 설치·운영 하고 있다			
(서비스 제공 업체가) 개인정보 유출 시도 탐지 및 대응, 비인가 접근 등에 대한 모니터링을 수행하고 있다			
(웹사이트 운영시) 인터넷 홈페이지 취약점 점검 등을 수행하고 있다			

개인정보처리시스템의 접근통제	그렇다	아니다	해당없음
개인정보처리시스템의 중요도(민감도) 및 업무연관성 등을 고려하여 담당자별 차등 접근권한 절차를 마련하고 있다			
전보 또는 퇴직 인력에 대해 개인정보처리시스템의 접근권한을 즉시 삭제하고 있다			
접근권한 부여·변경·말소에 대한 이력관리를 수행하고 최소 3년간 보관하고 있다			
비인가된 P2P, 웹하드, 공개된 무선망 등 공유설정에 대한 차단을 하고 있다			
개인정보처리시스템 접근관련, 개인정보취급자 별로 사용자계정 발급 및 사용자 인증(PKI, IP제한 등)을 하고 있다			
전산실, 자료보관실 등 개인정보를 취급하는 공간에 대해 출입통제 절차를 수립.운영 하고 있다			

개인정보가 포함된 서류 및 저장매체(USB, CD) 등에 대한 보안대책을 마련하고 있다			
계정정보 또는 비밀번호의 일정 횟수 이상 잘못 입력 시 접근제한 등 필요적 기술 조치를 하고 있다			
일정시간 이상의 업무처리 중지 시 자동 시스템 접속 차단을 실시하고 있다			

개인정보 암호화	그렇다	아니다	해당없음
사용자 단말기에 저장된 개인정보파일을 암호화하고 있다			
암호화된 개인정보의 안전한 보관을 위하여 안전한 암호키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하고 있다			
(서비스 제공 업체가) 고유식별정보(주민등록번호, 여권번호 등), 비밀번호, 바이오정보(지문, 얼굴 등)는 암호화하고 있다			
(서비스 제공 업체가) 비밀번호는 일방향 암호화를 적용하여 저장한다			
(서비스 제공 업체가) 개인정보 암호화 시, 안전한 알고리즘을 사용하고 있다			
(서비스 제공 업체가) 사용자 단말기부터 웹서버 구간 간 암호화를 적용하고 있다			

개인정보처리시스템 로그 관리	그렇다	아니다	해당없음
개인정보처리시스템 접속기록을 1년 이상(5만 명 이상의 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 경우는 2년이상) 보관·관리하고 있다			
개인정보처리시스템 접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관하고 있다			
개인정보처리시스템의 접속기록 점검 및 후속조치를 월 1회 이상 수행 하고 있다			

개인정보 수집 동의	그렇다	아니다	해당없음
개인정보 수집 시, 정보주체의 동의를 받고 있다			
만 14세 미만 아동의 개인정보를 수집 시, 법정대리인에게 동의를 받고 있다			

개인정보 수집, 이용 및 제공	그렇다	아니다	해당없음
서비스 제공을 위해 꼭 필요한 최소한의 정보만을 수집한다			
정보주체 이외로부터 수집한 개인정보를 처리할 때, 정보주체에게 알려주고 있다			
제3자 제공에 관한 사항을 정보주체에게 알리고 동의를 받고 있다			

개인정보 수집 목적을 넘어 이용하거나 제공하는 경우, 별도동의를 받거나 다른 법률에 근거하고 있다			
영업양도, 합병 등으로 개인정보를 다른 사람에게 이전하는 경우, 정보주체에게 그 사실을 알린다			
개인정보의 국외 이전 시, 정보주체에게 알리고 동의를 받는다			

개인정보 운영, 파기	그렇다	아니다	해당없음
개인정보파일의 보유기간이 타당하다			
개인정보파일이 불필요하게 되었을 때 지체 없이 파기한다			
개인정보 처리목적 달성 시, 지체 없이 파기한다			
개인정보를 파기할 때, 다시 복원하거나 재생할 수 없는 형태로 완벽하게 파기한다			
개인정보 파기에 관한 사항을 기록하고 관리하고 있다			
다른 법령에 따라 개인정보를 파기하지 않고 보존하는 경우, 다른 개인정보와 분리하여서 저장·관리한다			

주민등록번호 처리 제한	그렇다	아니다	해당없음
주민등록번호 처리 현황에 대해 파악하고 있다			
주민등록번호를 처리할 경우, 암호화처리를 하고 있다			

개인정보 유·노출 대응절차	그렇다	아니다	해당없음
개인정보의 유·노출 및 침해사고에 대한 대응절차가 수립되어 있다			
당해년도에 개인정보 유출 또는 노출 사고가 발생하지 않았다			
개인정보 유출사고 발생에 따른 유출통지 및 신고를 하였다			

4장. 그밖의 참고자료

- 개인정보포털
  https://www.privacy.go.kr/

- 개인정보배움터
  https://edu.privacy.go.kr/

- 개인정보보호위원회 - 지침·가이드라인
  https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS217&mCode=D010030000

- 정보인권연구소·진보네트워크센터 - 정보인권가이드
  https://guide.jinbo.net/

비영리단체를 위한 개인정보 내부관리 계획(예시)

아래 예시는 내부관리 계획에 일반적으로 포함되는 내용을
정리한 것으로, 필요에 따라 수정해 활용하면 됩니다.
다만 공공기관이나 일반 기업 사례를 참고하여 작성한 것이기에,
비영리단체에 꼭 들어맞지 않는 내용도 포함되어 있을 수 있습니다.
비영리단체 맥락에 보다 적합한 개인정보 내부관리 계획
양식을 앞으로 발전시켜 나갈 필요가 있겠습니다.

표지

OOOOO(단체명)

개인정보 내부 관리계획

20XX. XX. XX

[단체 직인]

수정 이력

순번	구분	시행 일자	주요내용
1	제정	OOOO. OO. OO.	
2	일부개정	OOOO. OO. OO.	[사유] OOOO. OO. OO. 개인정보보호법 개정 내용 반영 [수정사항] → 1. XXXXX
3	전부개정	OOOO. OO. OO.	1. OOOOO 2. OOOOO 3. OOOOO

제1장 총칙

제1조(목적)

ㅇㅇㅇㅇㅇ(단체명)(이하 '단체'라 한다) 개인정보 내부관리계획(이하 '본 계획' 또는 '내부관리계획'이라 한다)은 「개인정보 보호법」제29조(안전조치의무)와 '개인정보의 안전성 확보조치 기준'(**제2023-6호**)에 따라 제정된 것으로, **ㅇㅇㅇㅇㅇ(단체명)**가 개인정보를 처리함에 있어서 개인정보가 분실, 도난, 유출, 위조, 변조 또는 훼손되지 아니하도록 함을 목적으로 한다.

제2조(적용범위)

본 계획은 정보통신망을 통하여 수집, 이용, 제공 또는 관리되는 개인정보뿐만 아니라 서면, 전화, 팩스 등 정보통신망 이외의 수단을 통해서 수집, 이용, 제공 또는 관리되는 개인정보에 대해서도 적용되며, 이러한 개인정보를 취급하는 내부 임직원 및 **ㅇㅇㅇㅇㅇ(단체명)**의 개인정보 처리 업무를 위탁받아 처리하는 수탁자에게는 본 계획이 적용된다.

제3조(용어 정의)

본 계획에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. "개인정보"란 생존하는 개인에 관한 정보로서 성명/주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호/문자/음성/음향 및 영상 등의 정보(해당 정보만으로 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.
2. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
3. "개인정보보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자를 말한다.
5. "개인정보취급자"란 사업장 내에서 고객의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.

6. “개인정보처리시스템”란 개인정보를 처리할 수 있도록
체계적으로 구성한 데이터베이스시스템을 말한다.

제2장 내부관리계획의 수립 및 시행

제4조(내부관리계획의 수립 및 승인)

① 개인정보보호책임자는 **○○○○○(단체명)**의 개인정보보호를 위한
전반적인 사항을 포함하여 내부관리계획을 수립하여야 한다.
② 개인정보보호책임자는 개인정보보호를 위한 내부관리계획의
수립 시 개인정보보호와 관련한 법령 및 관련 규정을
준수하도록 내부관리계획을 수립하여야 한다.
③ 개인정보보호책임자는 개인정보보호 관련 법령의 제·개정 사항 등을 반영하기
위하여 매년 11월말까지 내부관리계획의 타당성과 개정 필요성을 검토하여야 한다.
⑤ 개인정보보호책임자는 모든 항목의 타당성을 검토한 후 개정할 필요가 있다고
판단되는 경우 12월말까지 내부관리계획의 개정안을 수립하여야 한다.

제5조(내부관리계획의 공표)

① 개인정보보호책임자는 제4조에 따라 승인한 내부관리계획을
매년 1월말까지 단체 전 임직원에게 공표한다.
② 내부관리계획은 임직원이 언제든지 열람할 수 있는 방법으로
비치하여야 하며, 변경사항이 있는 경우에는 이를 공지하여야 한다.

제3장 개인정보보호책임자의 의무와 책임

제6조(개인정보보호책임자의 지정)

단체는 다음 각 호의 어느 하나에 해당하는 지위에 있는 자
중에서 1인 이상을 개인정보보호책임자로 임명한다.

1. 단체의 대표 또는 임원
2. 개인정보 처리 관련 업무를 담당하는 부서의 장

제7조(개인정보보호책임자의 역할과 책임)

① 개인정보보호책임자는 개인정보 보호를 위하여 다음 각 호의 임무를 수행한다.

1. 개인정보취급자의 의무와 책임의 규정 및 총괄관리
2. 내부관리계획의 수립 및 승인
3. 개인정보의 안전성 보호조치 기준 이행 총괄
4. 임직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검, 대응, 사후조치 총괄
5. 고객으로부터 제기되는 개인정보에 관한 고충이나 의견의 처리 및 감독 총괄
6. 임직원 및 개인정보취급업무 수탁자 등에 대한 교육 총괄
7. 본 계획에 규정된 개인정보보호와 관련된 제반 조치의 시행 총괄
8. 기타 고객의 개인정보보호에 필요한 사항

② 개인정보보호책임자는 개인정보취급자를 최소한으로 제한하여 지정하고 수시로 관리·감독하여야 하며, 임직원에 대한 교육 및 보안서약 등을 통해 개인정보 침해사고를 사전에 예방한다.

제8조(개인정보취급자의 범위 및 역할과 책임)

① 개인정보취급자의 범위는 단체 내에서 개인정보 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 수행하는 자를 말하고, 정규직 이외에 임시직, 계약직 직원도 포함될 수 있다.

② 개인정보취급자는 고객의 개인정보보호와 관련하여 다음과 같은 역할 및 책임을 이행한다.

1. 개인정보보호 활동 참여
2. 내부관리계획의 준수 및 이행
3. 개인정보의 안전성 보호조치 기준 이행
4. 임직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검 등
5. 기타 개인정보 보호를 위해 필요한 사항의 이행

제4장 개인정보의 안전성 확보조치

제9조(접근권한의 관리)

① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 개인정보취급자에게만 업무 수행에 필요한 최소한의 범위로 차등 부여하여야 한다.
② 개인정보처리자는 개인정보취급자 또는 개인정보취급자의 업무가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.
③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.
④ 개인정보처리자는 개인정보처리시스템에 접근할 수 있는 계정을 발급하는 경우 정당한 사유가 없는 한 개인정보취급자 별로 계정을 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 한다.
⑤ 개인정보처리자는 개인정보취급자 또는 정보주체의 인증수단을 안전하게 적용하고 관리하여야 한다.
⑥ 개인정보처리자는 정당한 권한을 가진 개인정보취급자 또는 정보주체만이 개인정보처리시스템에 접근할 수 있도록 일정 횟수 이상 인증에 실패한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 조치를 하여야 한다.

제10조(접근 통제)

① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 안전조치를 하여야 한다.
1. 개인정보처리시스템에 대한 접속 권한을 인터넷 프로토콜(IP) 주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 인터넷 프로토콜(IP) 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응
② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 인증서, 보안토큰, 일회용 비밀번호 등 안전한 인증수단을 적용하여야 한다. 다만, 이용자가 아닌 정보주체의 개인정보를 처리하는 개인정보처리시스템의 경우 가상사설망 등 안전한 접속수단 또는 안전한 인증수단을 적용할 수 있다.
③ 개인정보처리자는 처리하는 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 개인정보취급자의 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.
④ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는

자동으로 접속이 차단되도록 하는 등 필요한 조치를 하여야 한다.
⑤ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

제11조(개인정보의 암호화)

① 개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송·수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.
② 개인정보처리자는 다음 각 호의 해당하는 이용자의 개인정보에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다.

1. 주민등록번호
2. 여권번호
3. 운전면허번호
4. 외국인등록번호
5. 신용카드번호
6. 계좌번호
7. 생체인식정보

③ 개인정보처리자는 이용자가 아닌 정보주체의 개인정보를 다음 각 호와 같이 저장하는 경우에는 암호화하여야 한다.

1. 인터넷망 구간 및 인터넷망 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우
2. 내부망에 고유식별정보를 저장하는 경우(다만, 주민등록번호 외의 고유식별정보를 저장하는 경우에는 다음 각 목의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다)
   가. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
   나. 암호화 미적용시 위험도 분석에 따른 결과

④ 개인정보처리자는 개인정보를 정보통신망을 통하여 인터넷망 구간으로 송·수신하는 경우에는 이를 안전한 암호 알고리즘으로 암호화하여야 한다.
⑤ 개인정보처리자는 이용자의 개인정보 또는 이용자가 아닌 정보주체의 고유식별정보, 생체인식정보를 개인정보취급자의 컴퓨터, 모바일 기기 및 보조저장매체 등에

저장할 때에는 안전한 암호 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

제12조(접속 기록 보관 및 점검)

① 개인정보처리자는 개인정보취급자의 개인정보처리시스템에 대한 접속기록을 2년 이상 보관·관리하여야 한다.
② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보의 다운로드가 확인된 경우에는 내부 관리계획 등으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.
③ 개인정보처리자는 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하기 위한 조치를 하여야 한다.

제13조(악성프로그램 등 방지)

① 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.
1. 프로그램의 자동 업데이트 기능을 사용하거나, 정당한 사유가 없는 한 일 1회 이상 업데이트를 실시하는 등 최신의 상태로 유지
2. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

② 개인정보처리자는 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 정당한 사유가 없는 한 즉시 이에 따른 업데이트 등을 실시하여야 한다.

제14조(물리적 안전조치)

① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.
② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.
③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여

개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제15조(출력 복사시 보호조치)

① 개인정보처리자는 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하여야 한다.
② 개인정보처리자는 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 안전조치를 하여야 한다.

제16조(개인정보의 파기)

① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비(자기장을 이용해 저장장치의 데이터를 삭제하는 장비)를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 구멍 뚫기 등으로 삭제

③ 기술적 특성으로 제1항 및 제2항의 방법으로 파기하는 것이 현저히 곤란한 경우에는 개인정보보호법 제58조의2에 해당하는 정보로 처리하여 복원이 불가능하도록 조치를 하여야 한다.

제5장 개인정보보호 실태 점검

제17조(개인정보보호 실태 점검의 실시)

① 개인정보보호책임자는 개인정보보호를 위한 내부관리 계획 및 관련 법령에서

정하는 개인정보보호 규정을 성실히 이행하는지를 주기적으로 점검·관리 하여야 한다.
② 개인정보보호책임자는 개인정보보호 실태 점검의 실시에
관하여 필요한 별도의 계획을 수립할 수 있다.
③ 개인정보보호 실태 점검은 연1회 이상 실시한다.

제18조(점검 결과 반영)

① 개인정보보호책임자는 개인정보 보호를 위한 점검 실시 결과, 개인정보의
관리·운영상의 문제점을 발견하거나 관련 직원이 본 계획의 내용을 위반할
때에는 시정·개선 또는 인사발령 등 필요한 조치를 취하여야 한다.
② 개인정보보호책임자는 개인정보 위반사실에 대한 시정·개선 조치가 이행되지
않거나, 개인정보보호에 심각한 영향이 발생할 수 있는 우려가 되는 경우
개인정보 취급자 등에 대한 인사발령 등의 필요한 추가 조치를 취할 수 있다.

제6장 개인정보보호 교육

제19조(개인정보보호 교육 계획의 수립)

① 개인정보보호책임자는 다음 각 호의 사항을 포함하는 연간
개인정보보호 교육계획을 매년 12월말까지 수립한다.

1. 교육목적 및 대상
2. 교육내용
3. 교육 일정 및 방법

② 개인정보보호책임자는 수립한 개인정보보호 교육 계획을 실시한 이후에 교육의
성과와 개선 필요성을 검토하여 차년도 교육계획 수립에 반영하여야 한다.

제20조(개인정보보호 교육의 실시)

① 개인정보보호책임자는 고객정보보호에 대한 직원들의 인식제고를 위해
노력해야 하며, 개인정보의 오·남용 또는 유출 등을 적극 예방하기 위해 임·직원을
대상으로 매년 정기적으로 연1회 이상의 개인정보보호 교육을 실시한다.
② 교육 방법은 집체 교육뿐만 아니라, 인터넷 교육, 그룹웨어
교육 등 다양한 방법을 활용하여 실시하고, 필요한 경우 외부

전문기관이나 전문요원에 위탁하여 교육을 실시할 수 있다.
③ 개인정보보호에 대한 중요한 전파 사례가 있거나 개인정보보호 업무와 관련하여 변경된 사항이 있는 경우, 개인정보보호책임자는 부서 회의 등을 통해 수시 교육을 실시할 수 있다.

부칙

본 계획은 OOOO년 OO월 OO일부터 시행한다.

비영리단체를 위한 개인정보 교육계획(예시)

다음 교육계획에서는 개인정보를 취급하는 활동가가 개인정보 관련 기초 정보와 실무상 유의사항을 다루는 '기본과정', 개인정보 보호책임자는 개인정보 처리 전반을 좀 더 깊게 다루는 사업자용 실무과정을 수강하는 것으로 구분해서 작성했습니다. 이는 역할에 맞는 교육계획을 세부적으로 구성하는 예를 제시하기 위한 것이고, 반드시 둘을 구분해서 계획을 작성해야 하는 것은 아닙니다. 간단하게라도 교육을 실행하는 것이 중요하기에, 단체의 실정에 맞게 조정해서 계획 및 실시하면 됩니다.

OOOO년도 개인정보보호 교육계획

● 교육 목적

- 교육을 통한 개인정보 인식제고 및 정보보호 문화 확산
- 개인정보보호 수준 향상으로 정보의 유·노출 사전 예방

● 교육 대상

- 개인정보보호 책임자
- 개인정보취급자

● 대상자별 교육내용

교육대상	중점 교육내용	추진일정	방법
개인정보 보호책임자	• 개인정보보호 업무 총괄 책임자로서 전문성 강화	연1회 (O월)	※ 개인정보보호 포털을 통한 온라인교육 등
개인정보 취급자	• 개인정보 수집·이용에서 파기까지 단계별 조치사항 • 개인정보보호 규정, 개인정보보호법에 의한 요구사항 등	연1회 (O월)	※ 개인정보보호 포털을 통한 온라인교육 등

※ 내부사정 또는 내부교육 추진 일정에 따라 변경 될 수 있음

● 대상자별 교육일정

교육대상	주관	교육과정	일정
개인정보보호 책임자	개인정보 배움터	[NEW] 개인정보 처리자 수준별교육_기본과정, [NEW]개인정보 안전성 확보조치 (총 2건 수강)	1. 2. ~ 12. 31.
개인정보취급자	개인정보 배움터	[NEW] 개인정보 처리자 수준별교육_실무과정	1. 2. ~ 12. 31.

OOOO년도 개인정보보호 교육 결과

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

- **교육 내용**
  - 개인정보보호 관련 법·제도 현황
  - 개인정보보호 규칙
  - 개인정보 침해 유형·대응 및 피해구제 사례 소개
  - 개인정보 보안관리 방안
  - 업무수행 시 의무사항 및 벌칙
  - 개인정보 보호책임자 역할
  - 개인정보 취급자 역할
  - 개인정보의 안전성 보호조치에 관한 사항 등

- **교육 결과**

교육일자	대상	대상인원	참석인원	이수율	비고
0000. 0. 0.	책임자	1	1	100%	이수증(별첨)
0000. 0. 0.	취급자	5	5	100%	이수증(별첨)

후주

1 https://www.kcc.go.kr/download.do?fileSeq=47904

2 https://edu.privacy.go.kr/user/course/infoGuide.do

3 구글 드라이브, 노션 등에서 전체 공개 설정(링크 주소만 알면 누구나 문서를 읽을 수 있음)을 이용할 때는 개인정보 등 민감한 내용이 포함되는 문서를 공유하지 않도록 유의해야 합니다. 민감한 문서는 어떤 경우에도 전체 공개하지 않고, 필요한 사람에게 직접 권한을 부여해서 관리하도록 합니다.

4 IP 주소 말고도, 일종의 기기 고유 번호에 해당하는 MAC 주소를 활용하여 알려진 기기(예: 조직에서 보유한 노트북)만 접속을 허용하는 방법도 있습니다.

5 https://support.google.com/accounts/answer/6063333?hl=ko

6 “Google 비영리단체 프로그램” 검색하여 신청. 자격요건은 (1) 세금 공제 기부를 수령할 수 있는 공익 단체, (2) 기부금 수령 자격이 있는 비영리 민간 단체, (3) 기타 비영리단체, 비정부 조직

7 https://docs.google.com/document/d/1idgiX9dM06QQwPz8oi1LqxGvM2nbtY-kj7yN1Oz0aI4/edit?usp=sharing