2015.2.

개인정보의 안전성 확보조치 기준 해설서

행정자치부

KISA 한국인터넷진흥원
Korea Internet & Security Agency

개인정보의 안전성 확보조치 기준 해설서

본 기준 해설서는 “개인정보 보호법”에 따라 개인정보처리자가 개인정보의 안전성 확보를 위해 이행해야 할 기술적 · 관리적 보호조치 등의 세부 기준 제시를 목적으로 합니다.

Contents

개인정보의
안전성 확보조치
기준 해설서

개인정보의 안전성 확보조치 기준 해설서

개인정보의 안전성 확보조치 기준

01 개인정보의 안전성 확보조치 기준

제정 2011. 9. 30. 행정안전부고시 제2011-43호
개정 2014. 12. 30. 행정자치부고시 제2014-7호

제1조(목적) 이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제24조제3항 및 제29조와 같은 법 시행령(이하 "영"이라 한다) 제21조 및 제30조에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실 · 도난 · 유출 · 변조 · 훼손되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 세부적인 기준을 정하는 것을 목적으로 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
2. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
3. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
4. "소상공인"이란 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」 제2조에 해당하는 자를 말한다.
5. "중소사업자"란 상시 근로자 수가 5인 이상 50인 미만인 개인정보처리자를 말한다. 다만 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」 제2조제1항제1호에 따른 광업 · 제조업 · 건설업 및 운수업의 경우에는 상시근로자 수가 10인 이상 50인 미만인 개인정보처리자를 말한다.
6. "개인정보 보호책임자"라 함은 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항제1호 및 제2호에 해당하는 자를 말한다.

7. “개인정보취급자”란 개인정보처리자의 지휘 · 감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다.

8. “정보통신망”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집 · 가공 · 저장 · 검색 · 송신 또는 수신하는 정보통신체계를 말한다.

9. “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다. 다만 소상공인 또는 중소사업자가 내부 직원의 개인정보만을 보유한 시스템은 제외한다.

10. “내부망”이라 함은 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

11. “내부관리계획”이란 개인정보처리자가 개인정보를 안전하게 처리하기 위하여 내부 의사결정절차를 통하여 수립 · 시행하는 내부 기준을 말한다.

12. “비밀번호”라 함은 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

13. “접속기록”이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속자를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.

14. “바이오정보”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

15. “보조저장매체”라 함은 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결 · 분리할 수 있는 저장매체를 말한다.

16. “위험도 분석”이란 개인정보처리시스템에 적용되고 있는 개인정보 보호를 위한 수단과 개인정보 유출시 정보주체의 권리를 해할 가능성 및 그 위험의 정도를 분석하는 행위를 말한다.

17. “모바일 기기”라 함은 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보처리에 이용되는 휴대용 기기를 말한다.

18. “공개된 무선망”이라 함은 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

제3조(내부관리계획의 수립 · 시행) ① 개인정보처리자는 개인정보의 안전한 처리를 위하여 다음 각 호의 사항을 포함하는 내부관리계획을 수립 · 시행하여야 한다.

1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보의 안전성 확보에 필요한 조치에 관한 사항
4. 개인정보취급자에 대한 교육에 관한 사항
5. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
6. 그 밖에 개인정보 보호를 위하여 필요한 사항

② 소상공인은 제1항에 따른 내부관리계획을 수립하지 아니할 수 있다.

③ 개인정보처리자는 제1항 각호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

제4조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근권한을 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 접속할 수 있는 사용자계정을 발급하는 경우, 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

제5조(접근통제) ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하여야 한다.

③ 개인정보처리자는 인터넷 홈페이지에서 다른 법령에 근거하여 정보주체의 본인확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 추가적인 정보를 확인하여야 한다.

④ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.

⑤ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출 · 변조 · 훼손되지 않도록 연 1회 이상 취약점을 점검하여야 한다.

⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다.

⑦ 개인정보처리자는 업무용 모바일 기기의 분실 · 도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

제6조(개인정보의 암호화) ① 영 제21조 및 영 제30조제1항제3호에 따라 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말한다.

② 개인정보처리자는 제1항에 따른 개인정보를 정보통신망을 통하여 송 · 수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

③ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

④ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

⑤ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 위험도 분석에 따른 결과

⑥ 개인정보처리자는 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

제7조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관 · 관리하여야 한다.

② 개인정보처리자는 개인정보의 유출 · 변조 · 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.

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

제8조(악성프로그램 등 방지) 개인정보처리자는 악성프로그램 등을 방지 · 치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치 · 운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시

제9조(물리적 접근 방지) 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.

제10조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각 · 파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려운 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, 천공 등으로 삭제

부칙 <제2011-43호, 2011. 9. 30.>

제1조 이 기준은 고시한 날부터 시행한다.

제2조(영상정보처리기기에 대한 안전성 확보조치의 적용 제외) 영상정보처리기기에 대한 안전성 확보조치에 대해서는 「표준 개인정보 보호지침」중에서 영상정보처리기기 설치 · 운영 기준이 정하는 바에 따른다.

제3조(전산센터, 클라우드컴퓨팅센터 등의 운영환경에서의 안전조치) 개인정보처리자가 전산센터(IDC : Internet Data Center), 클라우드컴퓨팅센터(Cloud Computing Center) 등에 계약을 통해 하드웨어, 소프트웨어 등을 임차 또는 임대하여 개인정보를 처리하는 경우에는 계약서 또는 서비스수준협약서(SLA : Service Level Agreement)에 이 기준에 준하는 수준의 안전조치 내용이 포함되어 있으면 이 기준을 이행한 것으로 본다.

부칙 <제2014-7호, 2014. 12. 30.>

이 기준은 고시한 날부터 시행한다.

개인정보의 안전성
확보조치 기준 해설서

개인정보의 안전성 확보조치 조문별 해설

02 개인정보의 안전성 확보조치 기준

1. 목적

제1조(목적) 이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제24조제3항 및 제29조와 같은 법 시행령(이하 "영"이라 한다) 제21조 및 제30조에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실 · 도난 · 유출 · 변조 · 훼손되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 세부적인 기준을 정하는 것을 목적으로 한다.

취지

- 개인정보 보호법 제24조 제3항 및 제29조와 같은 법 시행령 제21조 및 제30조에 근거한 기준으로서, 법률 및 시행령의 규정을 구체화하여 개인정보가 분실 · 도난 · 유출 · 변조 · 훼손 등이 되지 아니하도록 안전성을 확보하기 위한 세부적 기준 제시를 목적으로 한다.

해설

- 이 기준은 모든 개인정보처리자에게 적용된다. 따라서 업무를 목적으로 개인정보를 처리하는 모든 공공기관, 법인, 단체 및 개인 등은 이 기준을 준수하여 개인정보의 안전성 확보에 필요한 조치를 이행하여야 한다

TIP

- 개인정보 보호법 제2조에서 “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등으로 정의함
  - 개인정보 보호법은 개인정보 보호를 위한 일반법이므로 개인정보를 수집, 이용, 제공 등 처리하는 모든 자에 적용될 수 있도록 “개인정보처리자”의 개념을 폭넓게 정의

    : 공공기관, 영리목적의 민간분야 사업자, 협회 · 동창회 등 비영리 기관 · 단체를 모두 포괄

    ※ 예시 : 중앙행정기관, 중앙선거관리위원회, 국회 등 헌법기관, 정유사, 대형마트, 비디오대여점, 렌트카업체, 부동산중개업자, 자동차매매업자, 학교, 보험회사, 은행, 통신사, 여행사, 항공사, 호텔, 학원, 협회, 동창회, 동호회 등
  - 사적인 영역에서의 개인정보 처리는 배제하기 위하여 판례상 확립된 ‘업무상 목적’으로 ‘개인정보파일을 운용하기 위하여’ 개인정보를 처리하는 자로 한정

    ※ 예시 : 사적인 친분관계를 위하여 개인이 휴대폰에 저장한 연락처 정보, 이메일 주소록 등

2. 정의

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
2. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
3. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
4. “소상공인”이란 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」 제2조에 해당하는 자를 말한다.
5. “중소사업자”란 상시 근로자 수가 5인 이상 50인 미만인 개인정보처리자를 말한다. 다만 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」 제2조제1항제1호에 따른 광업 · 제조업 · 건설업 및 운수업의 경우에는 상시근로자 수가 10인 이상 50인 미만인 개인정보처리자를 말한다.
6. “개인정보 보호책임자”라 함은 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항 제1호 및 제2호에 해당하는 자를 말한다.
7. “개인정보취급자”란 개인정보처리자의 지휘 · 감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다.
8. “정보통신망”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집 · 가공 · 저장 · 검색 · 송신 또는 수신하는 정보통신체계를 말한다.
9. “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다. 다만 소상공인 또는 중소사업자가 내부 직원의 개인정보만을 보유한 시스템은 제외한다.
10. “내부망”이라 함은 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
11. “내부관리계획”이란 개인정보처리자가 개인정보를 안전하게 처리하기 위하여 내부 의사결정절차를 통하여 수립 · 시행하는 내부 기준을 말한다.
12. “비밀번호”라 함은 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진

자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

13. “접속기록”이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속자를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
14. “바이오정보”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
15. “보조저장매체”라 함은 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.
16. “위험도 분석”이란 개인정보처리시스템에 적용되고 있는 개인정보 보호를 위한 수단과 개인정보 유출시 정보주체의 권리를 해할 가능성 및 그 위험의 정도를 분석하는 행위를 말한다.
17. “모바일 기기”라 함은 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보처리에 이용되는 휴대용 기기를 말한다.
18. “공개된 무선망”이라 함은 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

취지

- 법 제2조(정의)에서 정의한 용어 이외에 같은 법 시행령과 「개인정보의 안전성 확보조치 기준」의 신규 용어에 대한 해석상의 혼란을 방지하기 위함이다.

해설

1. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

- “정보주체”는 처리되는 정보에 의하여 알아볼 수 있는 사람으로서, 개인정보 보호법에 의해 보호대상이 되는 존재를 말한다.

2. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

- “개인정보파일”은 개인의 이름이나 고유식별자 등을 사용하여 색인 · 분류되어 있는 등 일정한 기준에 따라 쉽게 개인정보를 검색할 수 있도록 체계적으로 배열 또는 구성된 개인정보의 집합물을 말한다.

3. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

- “개인정보처리자”란 법 제2조제5호에 따라 개인정보를 처리하는 모든 공공기관, 영리목적의 사업자, 협회 · 동창회 등 비영리기관 · 단체, 개인 등을 말한다.
- “개인정보 처리”란 개인정보를 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
- “공공기관”이란 법 제2조제6호 및 시행령 제2조에 따른 기관을 말한다.

[개인정보 보호법 제2조제6호]

제2조(정의) 이법에서 사용하는 용어의 정의는 다음과 같다.

6. “공공기관”이란 다음 각 목의 기관을 말한다.

가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체

나. 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관

4. “소상공인”이란 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」 제2조에 해당하는 자를 말한다.

■ “소상공인”은 “소기업 및 소상공인 지원을 위한 특별조치법”의 제2조제2호에서 정의하고 있는 사업자로서, ‘광업 · 제조업 · 건설업 및 운수업’의 경우에는 10인 미만의 사업자, 그 외의 업종의 경우에는 5인미만의 사업자를 말한다.

[소기업 및 소상공인 지원을 위한 특별조치법 제2조]

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “소기업”이란 「중소기업기본법」 제2조제2항에 따른 소기업을 말한다.
2. “소상공인”이란 소기업 중 상시 근로자가 10명 미만인 사업자로서 업종별 상시 근로자 수 등이 대통령령으로 정하는 기준에 해당하는 자를 말한다.

[전문개정 2011.5.24.]

[소기업 및 소상공인 지원을 위한 특별조치법 시행령 제2조]

제2조(소상공인의 범위 등) ① 「소기업 및 소상공인 지원을 위한 특별조치법」(이하 “법”이라 한다) 제2조제2호에서 “업종별 상시 근로자 수 등이 대통령령으로 정하는 기준에 해당하는 자”란 주된 사업에 종사하는 상시 근로자의 수가 다음 각 호의 어느 하나에 해당하는 사업자를 말한다.

1. 광업 · 제조업 · 건설업 및 운수업의 경우: 10명 미만
2. 제1호 외의 업종의 경우: 5명 미만

② 제1항에 따른 주된 사업의 기준과 상시 근로자의 범위 및 인원 산정방법에 관하여는 「중소기업기본법 시행령」제4조 및 제5조를 준용한다.

③ 중소기업청장은 소기업 또는 소상공인에 해당하는지를 확인하기 위하여 필요하다고 인정하는 경우에는 그 확인 방법 및 절차에 관한 사항을 따로 정하여 고시할 수 있다.

[전문개정 2013.12.24]

5. “중소사업자”란 상시 근로자 수가 5인 이상 50인 미만인 개인정보처리자를 말한다. 다만 「소기업 및 소상공인 지원을 위한 특별조치법 시행령」 제2조제1항제1호에 따른 광업 · 제조업 · 건설업 및 운수업의 경우에는 상시근로자 수가 10인 이상 50인 미만인 개인정보처리자를 말한다.

6. “개인정보 보호책임자”라 함은 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항제1호 및 제2호에 해당하는 자를 말한다.

- “개인정보 보호책임자”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자로서, 법 제31조와 시행령 제32조에 따른 지위에 해당하는 자를 말한다.
- 법령에서 특정한 지위를 갖는 자가 개인정보 보호 업무를 총괄하거나 업무처리를 최종 결정하도록 정하고 있는 것은 사내의 중요 의사결정을 수행하는 중역으로서 개인정보 보호 요구사항을 적극적으로 반영할 수 있도록 하기 위함이다.

7. “개인정보취급자”란 개인정보처리자의 지휘 · 감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다.

- “개인정보취급자”란 개인정보처리자의 지휘 · 감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 직접 개인정보에 관한 업무를 담당하는 자와 그 밖에 업무상 필요에 의해 개인정보에 접근하여 처리하는 모든 자를 말한다.

  ※ ‘개인정보취급자’는 기업 · 단체 · 공공기관의 임직원, 외부기관에서 또는 외부기관으로 파견된 근로자, 계약직원, 아르바이트 직원 등의 시간제근로자 등이 해당될 수 있다.

8. “정보통신망”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집 · 가공 · 저장 · 검색 · 송신 또는 수신하는 정보통신체계를 말한다.

- 정보통신망은 전기통신기본법 제2조제2호에 따라 전기통신을 하기 위한 기계 · 기구 · 선로 등 기타 전기통신에 필요한 설비를 이용하거나 컴퓨터 및 컴퓨터 이용기술을 활용하여 정보를

수집 · 가공 · 저장 · 검색 · 송신 또는 수신하는 정보통신체계를 의미한다.

9. "개인정보처리시스템"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다. 다만 소상공인 또는 중소사업자가 내부 직원의 개인정보만을 보유한 시스템은 제외한다.

- "개인정보처리시스템"이란 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스 시스템을 말한다.
- 개인정보처리시스템은 일반적으로 개인정보의 체계적인 처리를 위한 DBMS (Database Management System)을 말한다.

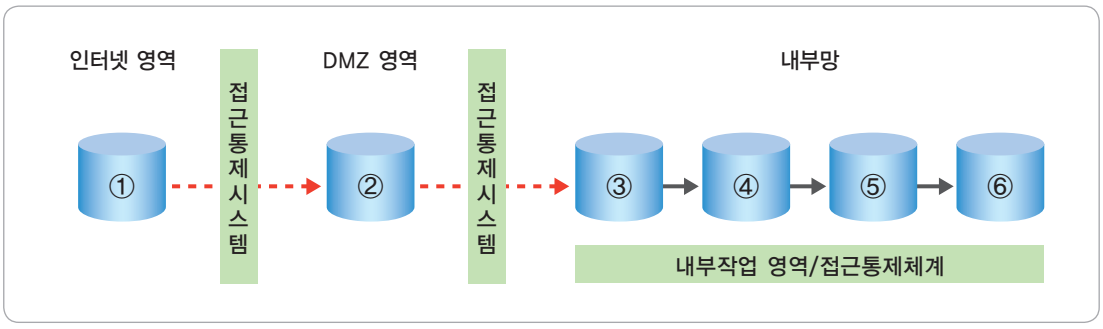
TIP

- 데이터베이스(DB) 응용프로그램이 설치 · 운영되지 않는 PC, 노트북과 같은 업무용 컴퓨터는 개인정보처리시스템에서 제외된다.

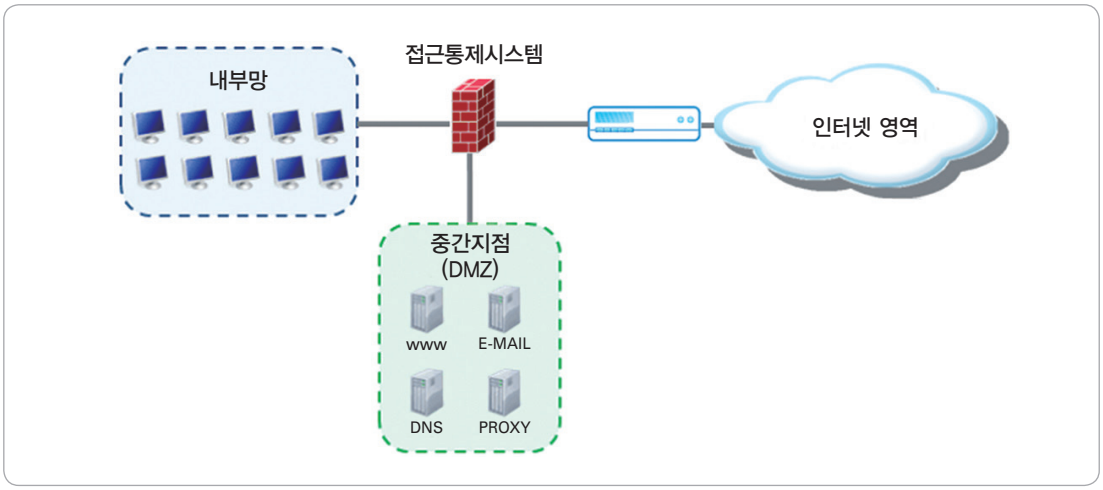
10. "내부망"이라 함은 물리적 망분리, 접근통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

- "내부망"이란 인터넷 구간과 물리적으로 망이 분리 되어 있거나, 비인가된 불법적인 접근을 차단하는 기능 등을 가진 접근통제시스템에 의하여 인터넷 구간에서의 직접 접근이 불가능하도록 통제 · 차단되어 있는 구간을 말한다.

[내부망 구성도 예시 1]



[내부망 구성도 예시 2]



11. “내부관리계획”이란 개인정보처리자가 개인정보를 안전하게 처리하기 위하여 내부 의사결정 절차를 통하여 수립 · 시행하는 내부 기준을 말한다.

- ‘내부관리계획’은 개인정보처리자가 정보주체의 개인정보를 보호하기 위하여 수립하는 것으로 기본 지침 또는 계획을 의미한다. 내부관리계획에는 개인정보처리자가 취급하는 개인정보가 분실 · 도난 · 누출 · 변조 또는 훼손되지 아니하도록 안전성을 확보하기 위한 개인정보 보호 교육 · 감사 등 개인정보 보호 활동에 대한 조직 내부의 개인정보 관리내용 등을 포함하여야 한다.

12. “비밀번호”라 함은 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

- ‘비밀번호’는 허가 없이 개인정보처리시스템 또는 업무용 컴퓨터에 인가된 사용자만 접속할 수 있도록 하기 위한 대책의 한 가지로서, 정보주체 또는 개인정보취급자가 컴퓨터 시스템 또는 통신망에 접속할 때 사용자 ID와 함께 입력하여 정당한 사용자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열이다. 회원제로 운영되는 온라인 정보 서비스의 경우, 비밀번호가 없으면 이용할 수 없으며, 서비스 제공자는 입력된 사용자 ID와 비밀번호를 시스템에 등록되어 있는 것과 대조하여 일치해야 접속을 허용하게 된다.

■ ‘타인에게 공개되지 않는 정보’의 의미는 개인정보취급자 중 계정관리자라 할지라도 정보주체 및 개인정보취급자의 비밀번호를 알 수 있는 형태로 관리되어서는 안 된다는 것이다. 비밀번호가 알 수 있는 형태로 관리되는 경우 해당 정보에 접근할 수 있는 내부자, 해커 등의 외부공격자 등에 의한 도용이 가능하기 때문이다.

13. “접속기록”이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속자를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.

■ “접속기록”은 개인정보취급자, 개인정보처리자 등이 개인정보처리시스템에 접속하여 운영하였던 이력정보로서, 시스템 식별 · 인증 정보(일시, 컴퓨터 · IP 명, 접속지역, ID 등), 서비스 이용정보(생성, 수정, 삭제, 검색, 출력 등) 등이 개인정보처리시스템에 있는 로그 파일에 자동으로 기록되는 것이다.

■ ‘접속하여 수행한 업무 내역’이라 함은 개인정보취급자가 개인정보처리시스템을 이용하여 수행한 업무를 알 수 있는 정보이다. 개인정보처리자 측면에서는 정보주체의 개인정보에 대한 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄) 등의 업무를 의미한다.

■ ‘식별자, 접속일시, 접속지를 알 수 있는 정보’는 접속한 사실을 확인하는데 필요한 정보를 말한다. 개인정보취급자의 사용자 계정 또는 사용자명 등이 식별자에 해당하며, 접속일시는 접속한 시점 또는 업무를 수행한 시점의 “년-월-일, 시:분:초”가 해당된다. 접속지를 알 수 있는 정보로는 개인정보처리시스템에 접속한 자의 PC 또는 서버의 IP 주소를 의미하며, 접속기록상의 “수행업무”는 개인정보에 대한 수집, 저장, 검색, 출력, 복사, 제공, 공개, 파기 등의 행위 중 어떤 행위를 수행했는지를 알 수 있는 구체적인 정보를 의미한다.

TIP

- 개인정보취급자가 특정 정보주체의 개인정보를 처리 한 경우, ‘수행업무’에는 해당 정보주체를 식별할 수 있는 정보도 포함된다.

■ ‘전자적으로 기록한 것’의 의미는 개인정보취급자가 수기로 작성한 문서가 아니라 시스템 로그와 같이 자동적으로 기록된 정보를 의미한다.

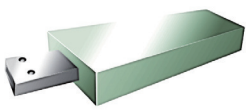
14. “바이오정보”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

- 지문, 얼굴, 홍채, 정맥, 음성, 필적 등의 바이오정보는 각 개인마다 고유의 특징을 가지기 때문에 개인을 식별하는 정보로 사용되며, 이러한 바이오정보는 신체적 특징과 행동적 특징을 기반으로 생성된 정보로 다음과 같은 것들이 있다.
  - 신체적 특징 : 지문, 얼굴, 홍채, 정맥, 음성, 망막, 손 모양, 손가락 모양, 열상 등
  - 행동적 특징 : 필적, 키보드 타이핑, 입술 움직임, 걸음걸이 등
- 바이오정보는 사람의 신체적 또는 행동적 특징을 입력장치를 통해 최초로 수집되어 가공되지 않은 ‘원본정보’와 그 중 특정 알고리즘을 통해 특징만을 추출하여 생성된 ‘특징정보’로 구분된다.

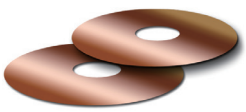
15. “보조저장매체”라 함은 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결 · 분리할 수 있는 저장매체를 말한다.

- “보조저장매체”는 컴퓨터에 장착된 하드디스크 등의 저장매체 이외에 전자적으로 자료를 저장할 수 있는 매체로서 이동형 하드디스크, SSD(Solid State Drive), USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk), 플로피디스켓, 자기 테이프 등 개인정보처리시스템, 업무용 컴퓨터 또는 개인용 컴퓨터 등과 용이하게 연결 · 분리할 수 있는 저장매체를 말한다.

[보조저장매체 예시]



[USB메모리]



[CD]

[이동형 하드디스크]

16. “위험도 분석”이란 개인정보처리시스템에 적용되고 있는 개인정보 보호를 위한 수단과 개인정보 유출시 정보주체의 권리를 해할 가능성 및 그 위험의 정도를 분석하는 행위를 말한다.

■ “위험도 분석”이란 개인정보처리시스템에 적용되고 있는 개인정보 보호를 위한 수단과 개인정보 유출시 정보주체의 권리를 해할 가능성과 그 위험의 정도를 분석하는 행위를 말한다.

TIP

• “위험도 분석”을 위한 세부 기준은 행정자치부에서 공고한 “개인정보 위험도 분석 기준 및 해설서”로서, 개인정보보호 종합지원 포털(http://www.privacy.go.kr)의 자료마당에서 다운로드 할 수 있다.

17. “모바일 기기”라 함은 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.

■ “모바일 기기”는 이동통신망, Wi-Fi 등의 무선망을 이용하여 개인정보 처리에 이용되는 휴대용 기기로서, 이러한 기기에는 스마트폰, 태블릿PC, PDA(Personal Digital Assistant) 등이 있다.

[모바일 기기 예시]

[스마트폰]

[태블릿 PC]

[PDA]

■ “개인정보 처리에 이용되는 휴대용기기”의 의미는 개인정보처리자가 업무를 목적으로 개인정보취급자로 하여금 개인정보 처리에 이용하도록 하는 휴대용 기기를 말한다.

– 개인 소유의 휴대용기기라 할지라도 개인정보처리자의 업무 목적의 개인정보 처리에 이용되는 경우 모바일 기기에 포함된다.

TIP

• 개인정보처리자의 ①“업무 목적”으로 ②“개인정보를 처리”에 이용되지 않는 휴대용기기는 “모바일 기기”에서 제외된다.

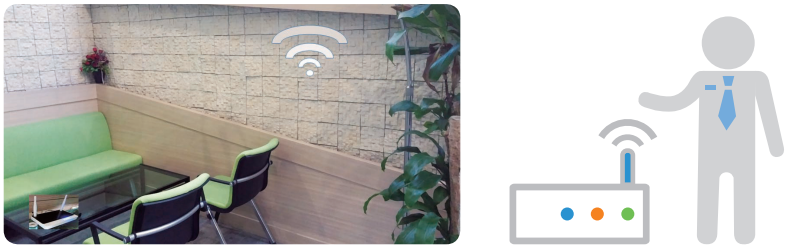
18. “공개된 무선망”이라 함은 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

■ “공개된 무선망”이란 공개된 장소 등에서 불특정 다수가 무선 접속장치(AP)를 통해 인터넷을 이용할 수 있는 망을 의미한다.

※ 무선접속장치(AP: Access Point) : 와이파이(Wi-Fi), 블루투스 관련 표준을 이용하여 유선 장치(예: 유선 LAN)와 무선 장치(예: 무선 LAN)를 연결시켜주는 컴퓨터 네트워크 장치중의 하나로서, 두 장치간 데이터를 중계할 수 있으며 라우터, 이더넷 허브 등에 연결하여 사용할 수 있다.

– 예를 들어, 커피전문점, 도서관, 병원 등에서 여러 방문객이나 고객이 인터넷을 이용할 수 있도록 무선접속장치(AP)를 설치 · 운영하는 망의 경우 “공개된 무선망”에 해당한다.

[공개된 무선망(커피전문점) 예시]



TIP

• 개인정보처리자가 업무 목적을 위해 개인정보취급자용 무선접속장치(AP)를 설치하여 운영하는 경우 “공개된 무선망”에서 제외된다.

예) 회사가 사무실, 회의실 등에서 직원 업무용 무선접속장치(AP)를 설치 · 운영하는 경우의 무선망

■ “공개된 무선망”이 설치된 장소의 예로는 커피전문점, 도서관, 공항, 철도역, 버스터미널, 대학, 병원, 유통센터, 호텔, 이동통신사, 개인정보처리자 등이 다수 고객이나 방문객용으로 무선접속장치(AP)를 설치한 매장, 로비, 대합실, 회의실, 휴게실, 주차장 등의 장소가 이에 해당한다.

TIP

• CDMA, WCDMA 등의 기술을 사용하는 이동통신망은 “공개된 무선망”에서 제외된다.

3. 내부관리계획의 수립·시행

제3조(내부관리계획의 수립 · 시행) ① 개인정보처리자는 개인정보의 안전한 처리를 위하여 다음 각 호의 사항을 포함하는 내부관리계획을 수립 · 시행하여야 한다.

1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보의 안전성 확보에 필요한 조치에 관한 사항
4. 개인정보취급자에 대한 교육에 관한 사항
5. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
6. 그 밖에 개인정보 보호를 위하여 필요한 사항

② 소상공인은 제1항에 따른 내부관리계획을 수립하지 아니할 수 있다.

③ 개인정보처리자는 제1항 각호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

취지

- 정보주체의 개인정보를 보호하기 위한 조치를 적절히 시행하기 위해서는 개인정보처리자 전체에 통용되는 내부규정이 필요하다. 이를 기초로 세부 지침이나 안내서를 마련하여 개인정보취급자 전원이 동일한 행동을 취할 수 있도록 할 필요가 있다.
- 개인정보처리자는 취급하는 개인정보가 분실 · 도난 · 누출 · 변조 또는 훼손 되지 아니하도록 안전성을 확보하기 위하여 개인정보 보호 활동에 대한 조직 내부의 개인정보 관리를 위한 내부관리계획을 수립하고, 개인정보 관련 모든 임직원 및 관련자에게 알림으로써 이를 준수할 수 있도록 하여야 한다.
  - 이와 같이 내부관리계획을 수립하도록 하는 이유는 개인정보 보호 활동이 임기응변식이 아니라 체계적이고 전사적인 계획 내에서 수행될 수 있도록 하는데 목적이 있으며, 이를 위하여 경영층의 방향제시와 지원이 필수적이다.

해설

- 내부관리계획에는 개인정보 보호 조직의 구성 및 운영에 관한 다음과 같은 사항을 포함하여야 한다.
  - 개인정보 보호책임자의 지정에 관한 사항
  - 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
  - 개인정보의 안전성 확보에 필요한 조치에 관한 사항
    - 제4조(접근 권한의 관리), 제5조(접근통제), 제6조(개인정보의 암호화), 제7조(접속기록의 보관 및 점검), 제8조(악성프로그램 등 방지), 제9조(물리적 접근 방지), 제10조(개인정보의 파기) 등
  - 개인정보취급자에 대한 교육에 관한 사항
  - 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
  - 그 밖에 개인정보 보호를 위하여 필요한 사항
- 내부관리계획은 전사적인 계획내에서 개인정보가 관리될 수 있도록 최고경영층으로부터 내부결재 등의 승인을 받아 모든 임직원 및 관련자에게 알림으로써 이를 준수할 수 있도록 하여야 한다.

TIP

- 내부관리계획의 문서 제목은 가급적 “내부관리계획”이라는 용어를 사용하는 것이 바람직하나, 개인정보처리자의 내부 상황에 따라 다른 용어를 사용 할 수 있다.
- 공공기관의 경우에는 ‘개인정보 보호 추진계획’이라는 이름으로 용어가 사용되기도 한다.

[개인정보 내부관리계획 목차 (예시)]

제1장 총칙

제1조(목적)

제2조(용어정의)

제3조(적용범위)

1. 개인정보 보호책임자의 지정에 관한 사항

■ 개인정보 보호책임자의 자격요건

- 원칙적으로 법 제31조제1항 및 시행령 제32조에 따라 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자(CPO: Chief Privacy Officer) 직제를 신설하거나, 정보주체의 개인정보 보호 업무를 위해 조직된 부서의 장 등을 지정할 수 있다.
- 또는, 개인정보처리자의 사업 환경에 따라 정보주체 개인정보를 주로 활용하는 업무를 수행하는 부서(고객 응대, 마케팅, 경영지원 등)나 정보보호 업무를 수행하는 부서에서 본연의 업무와 동시에 개인정보와 관련된 정보주체의 고충처리를 담당하게 되는 경우 해당 부서의 장이 개인정보 보호책임자에 지정될 수도 있다.
- 조직 내에 정보보호(Security) 업무를 총괄하는 정보보호책임자(CSO: Chief Security Officer)가 별도로 있는 경우에는 기술적 조치에 관하여 상호간의 업무를 분명하게 분장하여야 한다. 개인정보처리자는 개인정보 보호책임자와 정보보호 책임자로 동일인을 지정할 수도 있다.
- 개인정보 보호책임자는 정보보호 관련 지식뿐만 아니라 개인정보 취급에 관한 법 · 제도적인 측면 등의 다양한 지식을 습득할 필요가 있다.

[개인정보 보호법 시행령 제32조 제2항]

제32조(개인정보 보호책임자의 업무 및 지정요건 등) ② 개인정보처리자는 법 제31조제1항에 따라 개인정보 보호책임자를 지정하려는 경우에는 다음 각 호의 구분에 따라 지정한다.

1. 공공기관의 경우: 다음 각 목의 구분에 따른 기준에 해당하는 공무원 등
   - 가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관: 고위공무원단에 속하는 공무원(이하 “고위공무원”이라 한다) 또는 그에 상당하는 공무원
   - 나. 가목 외에 정무직공무원을 장(長)으로 하는 국가기관: 3급 이상 공무원(고위공무원을 포함한다) 또는 그에 상당하는 공무원
   - 다. 가목 및 나목 외에 고위공무원, 3급 공무원 또는 그에 상당하는 공무원 이상의 공무원을 장으로 하는 국가기관: 4급 이상 공무원 또는 그에 상당하는 공무원
   - 라. 가목부터 다목까지의 규정에 따른 국가기관 외의 국가기관(소속 기관을 포함한다): 해당 기관의 개인정보 처리 관련 업무를 담당하는 부서의 장
   - 마. 시 · 도 및 시 · 도 교육청: 3급 이상 공무원 또는 그에 상당하는 공무원
   - 바. 시 · 군 및 자치구: 4급 공무원 또는 그에 상당하는 공무원
   - 사. 제2조제5호에 따른 각급 학교: 해당 학교의 행정사무를 총괄하는 사람

아. 가목부터 사목까지의 규정에 따른 기관 외의 공공기관: 개인정보 처리 관련 업무를 담당하는 부서의 장으로서 공공기관의 장이 지정하는 사람

2. 공공기관 외의 경우: 다음 각 목의 어느 하나에 해당하는 사람

가. 사업주 또는 대표자

나. 개인정보 처리 관련 업무를 담당하는 부서의 장 또는 개인정보 보호에 관한 소양이 있는 사람

■ 개인정보 보호책임자의 지정

– 개인정보처리자는 개인정보 보호책임자의 자격요건에 부합하는 사람을 개인정보 보호책임자로 지정하여야 한다. 개인정보 보호책임자의 지정 시에는 인사발령 등을 통해 공식적으로 책임과 역할을 부여하여야 한다.

TIP

- 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 개인정보 보호책임자를 지정하지 않아도 된다.
- 근거 : 개인정보 보호법 제58조(적용의 일부 제외) ③ 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 제15조, 제30조 및 제31조(개인정보 보호책임자의 지정)를 적용하지 아니한다.

2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항

■ 개인정보 보호책임자의 역할

– 개인정보 보호책임자는 개인정보의 처리에 관한 업무를 총괄해서 책임지는 역할을 수행하는 사람으로, 개인정보 보호를 위해 개인정보와 관련된 내부지침을 준수하도록 기술적 · 관리적 보호조치를 실시하고 관리 · 감독하는 책임을 진다.

– 또한, 정보주체의 불만사항 접수 및 처리에 대한 책임을 지며, 개인정보를 취급하는 직원에 대해 교육훈련을 실시하여야 한다. 개인정보를 취급하는 업무를 외부에 위탁한 경우, 개인정보 보호책임자는 해당 위탁자의 개인정보 관리현황을 지속적으로 확인해야 한다.

[개인정보 보호법 제31조 제2항]

제31조(개인정보 보호책임자의 지정) ② 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용 · 남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리 · 감독
7. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무

[개인정보 보호법 시행령 제32조 제1항]

제32조(개인정보 보호책임자의 업무 및 지정요건 등) ① 법 제31조제2항제7호에서 "대통령령으로 정한 업무"란 다음 각 호와 같다.

1. 법 제30조에 따른 개인정보 처리방침의 수립 · 변경 및 시행
2. 개인정보 보호 관련 자료의 관리
3. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

■ 개인정보취급자의 역할 및 책임

– "개인정보취급자"는 개인정보처리자의 지휘 · 감독을 받아 개인정보를 처리하는 자로서 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 해야 한다.

– "개인정보취급자"는 기업 · 단체 · 공공기관의 임직원, 외부기관에서 또는 외부기관으로 파견된 근로자, 계약직원, 아르바이트 직원 등의 시간제근로자 등이 해당될 수 있다.

[개인정보취급자의 역할 및 책임 예시]

- 개인정보 보호 활동 참여
- 내부관리계획의 준수 및 이행
- 개인정보의 안전성 확보조치 기준 이행
- 소속 직원 또는 제3자에 의한 위법 · 부당한 개인정보 침해행위에 대한 점검 등

3. 개인정보의 안전성 확보에 필요한 조치에 관한 사항

- 개인정보의 안전성 확보에 필요한 조치에 관한 사항을 빠짐없이 내부관리계획에 포함해야 한다. 세부내용은 해설서 각 항목에 해당하는 부분을 확인한다.

TIP

- 안전성 확보에 필요한 조치 사항 : 제4조(접근 권한의 관리), 제5조(접근통제), 제6조(개인정보의 암호화), 제7조(접속기록의 보관 및 점검), 제8조(악성프로그램 등 방지), 제9조(물리적 접근 방지), 제10조(개인정보의 파기)

4. 개인정보취급자에 대한 교육에 관한 사항

- 개인정보 보호 교육의 목적은 안전하게 개인정보가 관리될 수 있도록 개인정보취급자의 개인정보 보호에 대한 인식을 제고시키고 개인정보 보호 대책의 필요성을 이해시키는 것이다.
- 개인정보처리자는 개인정보 보호책임자 및 개인정보취급자를 대상으로 매년 정기적으로 개인정보 보호 교육을 실시하여야 한다. 특히, 개인정보취급자가 정보주체의 개인정보를 훼손 · 침해 · 누설할 경우에는 중벌에 처해지므로, 교육 시 이러한 점을 개인정보취급자에게 인식시키기 위해 노력해야 한다.
- 개인정보 보호 교육의 구체적인 사항에는 교육을 하는 목적, 교육 대상, 교육 내용(프로그램 등 포함), 교육 일정 및 방법 등을 포함하고, 내부관리계획 또는 임직원의 결재를 얻은 "○○년 개인정보 보호 교육 계획(안)"과 같은 문서를 통해 관리하도록 한다.
- 교육 방법은 집체교육 뿐 아니라 조직의 환경을 고려하여 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하도록 하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시할 수도 있다.

TIP

- 행정자치부가 운영하는 개인정보보호 종합지원 포털(http://www.privacy.go.kr)에서 제공하는 온라인 교육 프로그램, 개인정보 보호 교육교재 등을 활용할 수 있다.

■ 교육내용에는 해당 업무를 수행하기 위한 분야별 전문기술 교육뿐만 아니라 개인정보 보호 관련 법률 및 제도, 사내 규정 등 필히 알고 있어야 하는 기본적인 내용을 포함하여 교육을 실시하도록 한다. 교육내용에 포함될 수 있는 예시는 다음과 같은 사항들이 있다.

[개인정보 보호 교육내용 예시]

- 개인정보 보호의 중요성 설명
- 내부관리계획의 준수 및 이행
- 위험 및 대책이 포함된 조직 보안 정책, 보안지침, 지시 사항, 위험관리 전략
- 개인정보처리시스템의 안전한 운영 · 사용법(하드웨어, 소프트웨어 등)
- 개인정보의 안전성 확보조치 기준
- 개인정보 보호 위반을 보고해야 할 필요성
- 개인정보 보호업무의 절차, 책임, 작업 설명
- 개인정보 보호 관련자들의 금지 항목들
- 개인정보 보호 준수사항 이행 관련 절차
- 개인정보 유 · 노출 및 침해신고 등에 따른 사실 확인 및 보고, 피해구제 등 업무절차 등

5. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항

■ 개인정보처리자는 개인정보 처리업무 위탁시 수탁자에게 제공된 개인정보를 안전하게 관리할 책임이 있다. 따라서 개인정보 처리업무를 위탁하는 경우, 개인정보보호법 제26조 및 동법 시행령에 규정된 사항을 준수하고 수탁자가 개인정보를 안전하게 처리할 수 있도록 수탁자 관리 및 감독에 관한 사항을 내부관리계획에 포함해야 한다.

[개인정보보호법 제26조]

제26조(업무위탁에 따른 개인정보의 처리 제한) ① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적 · 관리적 보호조치에 관한 사항
3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항

② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.

④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실 · 도난 · 유출 · 변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

■ 개인정보 처리 업무 위탁시 문서화(예: 위탁계약서) 하는 경우 수탁자의 무분별한 개인정보 재위탁, 개인정보 관리 소홀, 개인정보 유출 등을 예방하고 의무 위반시 손해배상 책임 등을 명확하게 하기 위해 다음의 사항을 포함하여 작성하여야 한다.

[개인정보 처리 업무 위탁 문서화(예: 위탁계약서)시 포함사항]

- 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
- 개인정보의 기술적 · 관리적 보호조치에 관한 사항
- 위탁업무의 목적 및 범위
- 재위탁 제한에 관한 사항
- 접근통제 등 안전성 확보 조치에 관한 사항
- 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
- 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등에 관한 사항 등

- 내부관리계획에는 개인정보 처리업무 위탁 문서화 내용에 따라 수탁자 교육, 관리 · 감독이 정확하게 실제적으로 이루어지도록 관련 사항을 구체적으로 포함해야 한다.
  - 예를 들어 내부관리계획에 "수탁자 관리 · 감독"항목을 만들고 여기에 위탁계약서의 각 내용별로 관리 · 감독하기 위한 방법, 절차, 시기, 항목 등을 서술하는 방법이 있다.
- 개인정보처리자는 내부관리계획에 정해진 바에 따라 정기적으로 수탁자에 대해 관리 · 감독 및 교육을 실시하고, 그 결과에 대한 기록을 남겨야 하며 문제점이 발견된 경우 그에 따른 개선 조치를 하여야 한다.

[수탁자 개인정보보호 교육내용 예시]

- 수탁업무의 목적 · 범위, 목적외 개인정보 처리 금지 사항
- 수탁자 개인정보처리시스템 및 업무용 PC의 접근 권한의 관리, 접근통제, 개인정보의 암호화, 접속기록의 보관 및 점검, 악성프로그램 방지 등 개인정보의 안전성 확보조치 기준
- 수탁받은 개인정보 처리업무의 안전성 확보조치 방법
- 수탁받은 개인정보 처리업무의 목적 달성 또는 계약 해지시 개인정보 파기
- 개인정보취급자의 의무
- 수탁업무와 관련하여 개인정보 관리 현황 점검 등 감독에 관한 사항
- 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등에 관한 사항

6. 그 밖에 개인정보 보호를 위하여 필요한 사항

- 개인정보처리자의 개인정보 처리(수집 · 이용 · 저장 · 제공 · 파기 등) 환경 및 중요도(민감정보 처리 등)를 고려하여 보안서약서 작성 등 개인정보 보호를 위하여 필요한 사항을 기술할 수 있다.
- 보안서약서 작성
  - 조직에서 임직원들의 기밀정보 유출 위험을 최소화하고, 임직원에게 개인정보 보호에 대한 책임을 명확히 주지시키기 위해 보안서약서에 서명하도록 한다.
  - 보안서약서의 서명은 개인정보 보호를 위한 기본적인 절차 중 하나로 인식되고 이행될 필요가 있다. 이러한 절차는 일반적으로 신규 인력 채용 시 인력관리 부서에 의해 수행될 수 있다.
  - 보안서약서에는 일반적으로 '고객 개인정보 보호, 회사 영업비밀 보호 등의 의무'에 관한 내용과 서명날짜, 서명자 정보 및 서명을 포함하여야 한다.

4. 접근 권한의 관리

제4조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근권한을 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 접속할 수 있는 사용자계정을 발급하는 경우, 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

취지

- 접근권한 관리의 목적은 개인정보처리시스템에 대하여 업무 목적 외 불필요한 접근을 최소화하고, 인사이동 등 권한 변경 사항 발생에 따른 인가되지 않는 접근을 차단하는데 있다.
- 접근권한은 업무 수행에 필요한 최소한의 범위로 업무 담당자에게 차등 부여되어야 하며 인사이동이나 권한변경 발생 시 지체없이 해당 권한을 변경 또는 말소 하고, 개인정보 유출 예방 및 대응 등을 위해 개인정보취급자 별로 사용자계정을 발급하여 관리하여야 한다.

해설

① 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

■ 개인정보의 분실 · 도난 · 유출 · 변조 또는 훼손을 방지하기 위하여 개인정보처리시스템에 대한 접근권한은 업무 수행 목적에 따라 필요 최소한의 범위로 업무담당자에게 차등 부여하고 접근통제를 위한 조치를 취해야 한다.

TIP

• 예를 들어 개인정보 보호책임자에게는 전체권한(읽기/쓰기/변경)을 부여하고, 개인정보취급자에게는 일부권한(읽기)만 부여하는 등 접근권한에 차등을 두어야 한다.

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 한다.

③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

■ 조직 내의 임직원 전보 또는 퇴직 등 인사이동 등으로 사용자 계정의 변경 · 말소가 필요한 경우에는 공식적인 사용자 계정 관리절차에 따라 통제될 수 있도록 한다.

– 내부 인력의 퇴직 시 해당 인력의 계정을 지체없이 변경하도록 지침에 반영하여 이행하도록 한다.

– 임직원의 퇴직 시 계정 말소를 효과적으로 이행하기 위해서는 퇴직 점검표에 사용계정의 말소 항목을 반영하여, 계정의 말소 여부에 대해 확인을 받을 수 있다.

■ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경, 말소에 대한 내역을 기록하고 해당 기록을 최소 3년간 보관하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우, 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

■ 개인정보처리시스템에 접속할 수 있는 사용자계정은 개인정보취급자 별로 발급하고 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

– 다수의 개인정보취급자가 동일한 업무를 수행한다 하더라도 하나의 사용자계정을 공유하지

않도록 개인정보취급자 별로 아이디(ID)를 발급하여 사용하고, 각 개인정보취급자별 개인정보 처리내역에 대한 책임 추적성(Accountability)을 확보하여야 한다.

※ 책임 추적성이란 개인정보 취급에 따른 문제 발생시 사용자계정을 기반으로 책임소재를 파악하는 것을 말한다.

TIP

- 한명의 개인정보취급자가 여러 업무를 수행해야 하는 경우, 해당 개인정보취급자에게 각 업무별로 사용자계정을 발급 할 수 있다.

  (예: 개인정보취급자 1명이 서로 권한이 다른 조회, 삭제 등 2개의 업무 수행시, 조회업무용과 삭제업무용으로 구분하여 2개의 사용자계정 발급 가능)

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

■ 개인정보처리자는 개인정보취급자나 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템, 접근통제시스템 등에 적용하여 운영하여야 한다. 다만, 정보주체의 비밀번호는 정보주체의 편의성 등을 고려하여 개인정보처리자가 자율적으로 적절한 수준을 설정하는 것이 필요하다.

– 비밀번호는 산업스파이, 침입자, 비인가자가 추측하기 어려운 문자와 숫자를 포함하도록 하거나, 전에 사용된 비밀번호를 다시 사용하지 않는 등의 다음과 같은 비밀번호 설정 원칙을 참고하여 생성하도록 한다.

- 비밀번호의 최소 길이 : 비밀번호는 구성하는 문자의 종류에 따라 최소 10자리 또는 8자리 이상의 길이로 구성하여야 하며, 이는 정보주체에 대한 비밀번호 작성규칙과는 달리 반드시 준수하여야 한다

  ※ 컴퓨터 관련 기술의 발달에 따라 비밀번호의 최소 길이는 늘어날 수 있고, 변경주기는 짧아질 수 있다.

- 최소 10자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개)중 2종류 이상으로 구성한 경우
- 최소 8자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개) 및 특수문자(32개) 중 3종류 이상으로 구성한 경우

  ※ 특수문자 32개 예시

~ · ! @ # $ % ^ & * ( ) _ – + = [ ] [ ] |

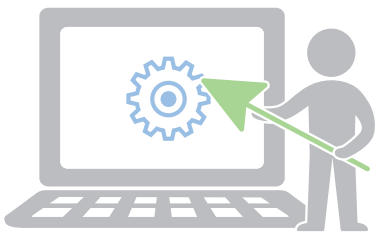
– 추측하기 어려운 비밀번호의 생성 :

  • 생성한 비밀번호에 12345678 등과 같은 일련번호, 전화번호 등과 같은 쉬운 문자열이 포함되지 않도록 한다.

  • love, happy 등과 같은 잘 알려진 단어 또는 키보드 상에서 나란히 있는 문자열도 포함되지 않도록 한다.

– 비밀번호의 주기적인 변경 : 비밀번호에 유효기간을 설정하고 적어도 6개월마다 변경함으로써 동일한 비밀번호를 장기간 사용하지 않는다.

– 동일한 비밀번호 사용 제한 : 2개의 비밀번호를 교대로 사용하지 않는다.



5. 접근통제

제5조(접근통제) ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하여야 한다.

③ 개인정보처리자는 인터넷 홈페이지에서 다른 법령에 근거하여 정보주체의 본인확인을 위해 성명, 주민등록번호를 사용할 수 있는 경우에도 정보주체의 추가적인 정보를 반드시 확인하여야 한다.

④ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.

⑤ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출 · 변조 · 훼손되지 않도록 연 1회 이상 취약점을 점검하여야 한다.

⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다.

⑦ 개인정보처리자는 업무용 모바일 기기의 분실 · 도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

취지

- 접근통제의 목적은 정보통신망을 통해 개인정보처리시스템에 대한 인가되지 않은 불법적인 접근을 차단하는 것으로, 정보통신망, 인터넷 홈페이지, 업무용 컴퓨터나 모바일 단말 등 개인정보를

처리하는 각 요소에서 적절한 접근통제 정책의 구현을 통해 불법적인 접근이 적절히 차단되어야 한다.

- 이를 위해 정보통신망에서 IP 주소를 통한 비인가자의 접근 제한, 가상사설망(VPN) 등을 이용한 안전한 접속, 인터넷 홈페이지의 취약점 점검, 업무용 컴퓨터 또는 모바일 기기의 보호조치 등의 접근통제 조치가 필요하다.

해설

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

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지

- 개인정보처리자는 개인정보처리시스템에서 정보통신망을 통한 불법적인 접근 및 침해사고를 방지하기 위해 아래의 기능을 포함한 장비 설치 · 운영 등의 조치를 하여야 한다.
  - 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한 (침입차단 기능)
  - 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지 (침입탐지 기능)
- 침입차단 및 침입탐지 기능을 갖춘 장비의 설치 방법 예시
  - 침입차단시스템 및 침입탐지시스템을 설치 · 운영하거나, 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템(IPS : Intrusion Prevention System), 웹방화벽 또는 보안 운영체제(Secure OS) 등을 도입할 수 있다.
  - 또한, 스위치 등의 네트워크 장비에서 제공하는 ACL(Access Control List : 접근제어목록) 등 기능을 이용하여 IP 주소 등을 제한함으로써 침입차단 기능을 구현할 수 있다.
  - 인터넷데이터센터(IDC), 클라우드 서비스, 보안업체 등에서 제공하는 보안서비스(방화벽, 침입방지, 웹방화벽 등)를 활용함으로써 초기 투자비용 등을 줄일 수 있다.
  - 공개용(무료) 소프트웨어를 사용하거나, 운영체제(OS)에서 제공하는 기능을 활용하여 해당

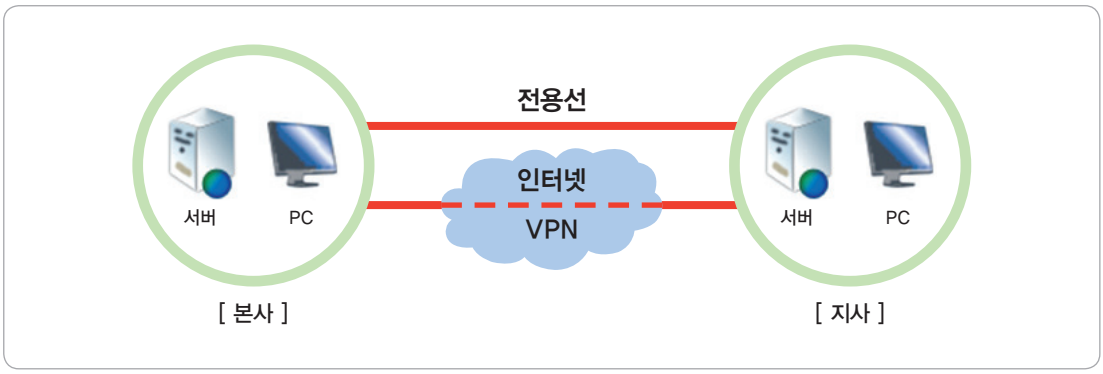
기능을 포함한 시스템을 설치·운영할 수 있다. 다만, 공개용(무료) 소프트웨어를 사용하는 경우에는 적절한 보안이 이루어지는지를 사전에 점검하여야 한다.

- 불법적인 접근 및 침해사고 방지를 위해서는 침입차단 및 침입탐지 기능을 갖는 장비 설치와 더불어 적절한 침입차단 및 침입탐지 정책 설정, 로그 분석 및 이상 행위 대응, 로그 훼손 방지 등 적절한 운영·관리가 필요하다.

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하여야 한다.

- 외부망으로부터 개인정보처리시스템에 대한 접속은 원칙적으로 차단하여야 한다. 다만 개인정보처리자가 외부망을 통해 개인정보처리시스템에 접속이 필요한 경우에는 가상사설망(VPN : Virtual Private Network) 또는 전용선 등의 안전한 접속수단을 적용하여야 한다.
  - 노트북과 같은 업무용 컴퓨터, 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속하는 경우에도 가상사설망, 전용선 등의 안전한 접속수단을 적용하여야 한다.
  - 가상사설망(VPN : Virtual Private Network)은 개인정보 취급자가 사업장 내의 개인정보처리시스템에 대해 원격으로 접속할 때 IPsec이나 SSL 기반의 암호 프로토콜을 사용한 터널링 기술을 통해 안전한 암호통신을 할 수 있도록 해주는 보안 시스템을 의미한다.
    - ※ IPsec(IP Security Protocol)은 인터넷 프로토콜(IP) 통신 보안을 위해 패킷에 암호화 기술이 적용된 프로토콜 집합
    - ※ SSL(Secure Sockets Layer)은 웹 브라우저와 웹 서버간에 데이터를 안전하게 주고받기 위해 암호화 기술이 적용된 보안 프로토콜
    - ※ IPsec, SSL 등의 기술이 사용된 가상사설망을 안전하게 사용하기 위해서는, 잘 알려진 취약점(예: Open SSL의 Heart Bleed 취약점)들을 조치하고 사용 할 필요가 있다.

[가상사설망 및 전용선 구성 예시]



③ 개인정보처리자는 인터넷 홈페이지에서 다른 법령에 근거하여 정보주체의 본인확인을 위해 성명, 주민등록번호를 이용하는 경우에도 정보주체의 추가적인 정보를 반드시 확인하여야 한다.

- 인터넷 홈페이지에서 성명, 주민등록번호만으로 정보주체의 본인 여부를 확인한 후 서비스를 제공할 경우 해커 등 타인이 유출된 개인정보를 도용하여 서비스를 이용할 수 있다. 이를 방지하기 위해 정보주체의 추가정보를 반드시 확인하여야 한다.
- 정보주체의 추가적인 정보를 확인하는 방법에는 i-PIN, 공인인증서, 휴대전화, 주민등록증 발급일자, 전자우편(e-mail) 주소 등의 수단 중 하나의 수단을 이용한 정보주체의 본인확인, 인증 등이 이에 해당한다.

[추가적인 정보 확인 예시]

[실명확인] [아이핀] [휴대폰] [공인인증서]

④ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치를 하여야 한다.

- 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지를 통해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 다음과 같은 항목 등을 고려하여 조치 할 수 있다.
  - 잘 알려진 웹 취약점 항목들을 포함함 웹 취약점 점검 및 조치
    - ※ 웹 취약점 점검 항목 예시 : SQL_Injection 취약점, CrossSiteScript 취약점, File Upload 취약점, ZeroBoard 취약점, Directory Listing 취약점, File Download 취약점 등
    - ※ 잘 알려진 웹 취약점 점검 항목은 행정자치부, OWASP(국제웹표준기구), 국가사이버안전센터(NCSC) 등에서 발표하는 항목 참조
  - 인터넷 홈페이지 중 서비스 제공에 사용되지 않거나 관리되지 않는 사이트 또는 URL(Uniform Resource Locator)에 대한 삭제 또는 차단 조치

– 관리자 페이지 홈페이지에 대해 노출 차단 등의 보호조치

– 웹 취약점 점검과 함께 정기적으로 웹 쉘 등을 점검하고 조치하는 경우 취급중인 개인정보가 인터넷 홈페이지를 통해 열람권한이 없는 자에게 공개되거나 유출되는 위험성을 더욱 줄일 수 있다.

■ 개인정보처리자는 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기에서 P2P, 공유설정은 기본적으로 사용하지 않는 것이 원칙이나, 업무상 꼭 필요한 경우에는 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 취급중인 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 하여야 한다.

– 업무상 꼭 필요한 경우라도 드라이브 전체 또는 불필요한 폴더가 공유되지 않도록 조치하고, 공유폴더에 개인정보 파일이 포함되지 않도록 정기적으로 점검하여 조치하도록 한다.

※ P2P, 웹하드 등의 사용을 제한하는 경우에도 단순히 사용금지 조치를 취하는 것이 아니라 시스템 상에서 해당 포트를 차단하는 등 근본적인 조치를 취하는 것이 필요하다.

■ 개인정보처리자는 공개된 무선망을 이용하여 개인정보를 처리하는 경우 취급중인 개인정보가 신뢰되지 않은 무선접속장치(AP), 무선 전송 구간 및 무선접속장치(AP)의 취약점 등에 의해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터 및 모바일 기기 등에 조치를 하여야 하며, 다음과 같은 방식들을 활용 할 수 있다.

– 개인정보 송 · 수신시 SSL, VPN 등의 보안기술이 적용된 전용 프로그램을 사용하여 송 · 수신 또는 암호화 송 · 수신

※ 예시: 모바일 기기, 노트북에서 개인정보처리시스템에 개인정보 전송시, 전송 암호화 기능이 탑재된 별도의 앱(App)이나 프로그램을 설치하고 이를 이용하여 전송

– 개인정보가 포함된 파일 송 · 수신시 파일 암호화 저장 후 송 · 수신

※ 예시: 모바일 기기, 노트북에서 개인정보처리시스템에 개인정보가 포함된 파일 전송시, 암호화 저장한 후 전송

– 개인정보 유출 방지조치가 적용된 공개된 무선망 이용

※ 예시: 모바일 기기, 노트북에서 설치자를 신뢰할 수 있고 관리자 비밀번호 등을 포함한 알려진 보안취약점이 조치된 무선접속장치(AP)에 안전한 비밀번호를 적용한 WPA2(Wi-Fi Protected Access 2) 보안 프로토콜을 사용하는 공개된 무선망 사용

– 기타

※ 공개된 무선망에서 개인정보 송 · 수신시 유출방지 기술이 적용된 방법 사용

⑤ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출 · 변조 · 훼손되지 않도록 연 1회 이상 취약점을 점검하여야 한다.

■ 인터넷 홈페이지를 통해 고유식별정보(주민등록번호, 운전면허번호, 외국인등록번호, 여권번호)를 처리하는 경우에, 개인정보처리자는 고유식별정보가 유출 · 변조 · 훼손되지 않도록 해당 인터넷 홈페이지에 대해 연 1회 이상 취약점을 점검하여야 하며, 문제점이 발견된 경우 그에 따른 개선조치를 하여야 한다.

– 고유식별정보를 처리하는 인터넷 홈페이지의 웹 취약점 점검시 잘 알려진 웹 취약점 항목들이 포함되도록 할 필요가 있다.

※ 웹 취약점 점검 항목 예시 : SQL_Injection 취약점, CrossSiteScript 취약점, File Upload 취약점, ZeroBoard 취약점, Directory Listing 취약점, File Download 취약점 등

※ 잘 알려진 웹 취약점 점검 항목은 행정자치부, OWASP(국제웹표준기구), 국가사이버안전센터(NCSC) 등에서 발표하는 항목 참조

TIP

• 고유식별정보를 처리하지 않는 인터넷 홈페이지는 연 1회 이상 취약점 점검이 필수는 아니나, 개인정보 유출 등에 대비해서 가급적 취약점 점검을 권장한다.

– 웹 취약점 점검과 함께 시큐어 코딩을 적용하고, 정기적으로 관리자 페이지 노출 및 웹 쉘 등을 점검하고 조치하는 경우 인터넷 홈페이지를 통한 고유식별정보의 유출 · 변조 · 훼손의 위험을 더욱 줄일 수 있다.

■ 인터넷 홈페이지의 취약점 점검시에는 기록을 남겨 책임 추적성 확보 및 향후 개선조치 등에 활용할 수 있도록 할 필요가 있다.

■ 인터넷 홈페이지의 취약점 점검은 개인정보처리자의 자체인력, 보안업체 등을 활용할 수 있으며, 취약점 점검은 상용 도구, 공개용 도구, 자체 제작 도구 등을 사용할 수 있다.

TIP

• 인터넷 홈페이지 취약점 점검 및 조치에 활용할 수 있는 기술문서는 다음을 포함한 다양한 자료가 있다.

소프트웨어 개발보안 가이드(안전행정부, 2013.11.)
시큐어코딩가이드(C, Java)(행정안전부, 2012.9.)
Web 2.0 정보보호 실무가이드(행정안전부, 2010.5.)
홈페이지 취약점 진단 · 제거 가이드(KISA, 2013.12.)

• 인터넷 홈페이지 취약점 점검을 위해 소상공인, 중소사업자, 비영리단체는 한국인터넷진흥원(KISA)에서 제공하는 무료 웹 취약점 점검 서비스 이용할 수 있으며, 개인정보보호 종합지원 포털(http://www.privacy.go.kr)에서 점검을 신청할 수 있다.

⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근통제 기능을 이용할 수 있다.

■ 개인정보처리시스템을 이용하지 않고 단순히 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 저장하는 등의 처리를 하는 경우 운영체제나 보안프로그램에서 제공하는 접근통제 기능을 이용할 수 있다.

– PC, 노트북 등의 업무용 컴퓨터의 운영체제(OS)에서 제공하는 접근통제 기능 설정 방법은 다음과 같으며, 별도의 보안프로그램을 사용하여 접근통제 기능을 설정하고 이용 할 수도 있다.

[업무용 컴퓨터(윈도우의 경우) 방화벽 설정 방법]

• 업무용 컴퓨터 : 제어판 ▶ Windows 방화벽 ▶ Windows 방화벽 설정 또는 해제

※ 업무용 컴퓨터 운영체제에서 제공하는 개인용 방화벽 설정시 외부 IP로부터 시도되는 불법적인 접근 등을 차단한다.

– 스마트폰, 태블릿PC 등 모바일 기기에서도 운영체제(OS)나 별도의 보안 프로그램에서 제공하는 접근통제 기능을 이용할 수 있다.

※ 모바일 기기에서는 불필요한 네트워크 소프트웨어 통제, 인입 포트 차단 등의 접근통제 기능을 제공하는 운영체제를 사용할 수 있으며, 이러한 기능을 제공하지 않거나 보다 확장된 접근통제 기능을 사용이 필요한 경우에는 접근통제 기능을 제공하는 별도의 방화벽 등의 어플리케이션(App)을 설치 · 운영이 필요 할 수 있다.

⑦ 개인정보처리자는 업무용 모바일 기기의 분실 · 도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

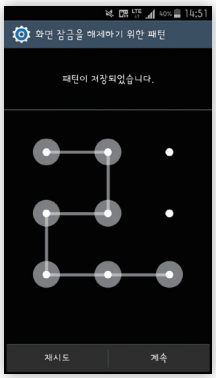
■ 업무용 모바일 기기는 성능이 높아 대량의 개인정보를 저장하거나 전송할 수 있으나, 휴대와 이동이 편리하여 기기 분실 · 도난시 해당 기기에 저장된 또는 해당 기기의 개인정보처리시스템 접속 등을 통한 개인정보 유출의 위험성이 높다.

■ 따라서, 스마트폰, 태블릿PC와 같이 업무에 사용되는 모바일 기기는 분실 · 도난으로 개인정보가 유출되지 않도록 개인정보처리자의 기기 운영 환경 및 처리되는 개인정보의 중요도 등을 고려하여 조치가 필요하며, 다음과 같은 항목들을 조치항목으로 고려 할 수 있다.

– 비밀번호, 패턴, PIN 등을 사용하여 화면 잠금 설정

[화면 잠금 설정 예시]

[비밀번호]



[패턴입력]

– 디바이스 암호화로 애플리케이션, 데이터 등 암호화

– USIM 카드에 저장된 개인정보 보호를 위한 USIM 카드 잠금설정

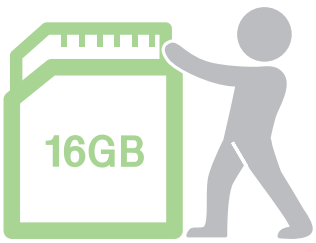
– 모바일 기기 제조사 및 이동통신사가 제공하는 기능을 이용한 원격 잠금, 원격 데이터 삭제 등의 조치

TIP

• 모바일 기기의 도난 또는 분실 시 원격 잠금, 데이터 삭제 등을 위해 제조사별로 지원하는 '킬 스위치(Kill Switch) 서비스'나 이동통신사의 '잠금 앱 서비스'를 이용할 수 있다.

– 중요한 개인정보를 처리하는 모바일 기기는 MDM(Mobile Device Management) 등 모바일 단말 관리 프로그램을 설치하여 원격 잠금, 원격 데이터 삭제, 접속 통제 등의 조치

※ MDM은 무선망을 이용해 원격으로 스마트폰, 태블릿PC 등의 모바일 기기를 제어하는 솔루션으로, 분실된 모바일 기기의 위치를 추적, 원격 잠금 설정, 원격 정보 삭제, 특정 사이트 접속 제한, 카메라 등 기능 제어, 앱 설치 통제 등의 기능 제공



6. 개인정보의 암호화

제6조(개인정보의 암호화) ① 영 제21조 및 영 제30조제1항제3호에 따라 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말한다.

② 개인정보처리자는 제1항에 따른 개인정보를 정보통신망을 통하여 송 · 수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

③ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

④ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

⑤ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 위험도 분석에 따른 결과

⑥ 개인정보처리자는 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장하여야 한다.

취지

- 비밀번호, 바이오정보, 주민등록번호 등과 같은 주요 개인정보가 암호화되지 않고 개인정보처리시스템에 저장되거나 네트워크를 통해 전송될 경우, 노출 및 위 · 변조 등의 위험이 있으므로 암호화 등의 안전한 보호조치가 제공되어야 한다.

※ "암호화"는 개인정보취급자의 실수 또는 해커의 공격 등으로 인해 개인정보가 비인가자에게 유 · 노출되더라도 그 내용 확인을 어렵게 하는 보안기술이다.

해설

① 영 제21조 및 영 제30조제1항제3호에 따라 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말한다.

- “고유식별정보”는 개인을 고유하게 구별하기 위하여 부여된 식별정보를 말하며 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호가 여기에 해당한다.
- “비밀번호”는 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
- “바이오정보”는 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 최초로 수집되어 가공되지 않은 ‘원본정보’와 가공되거나 생성된 특징정보를 포함한다.

② 개인정보처리자는 제1항에 따른 개인정보를 정보통신망을 통하여 송 · 수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

- 개인정보처리자는 정보통신망을 통하여 내 · 외부로 송 · 수신 할 고유식별정보(주민등록번호, 운전면허번호, 외국인등록번호, 여권번호), 비밀번호, 바이오정보에 대해서는 암호화하여야 한다.

TIP

- 내부망 내에서 송 · 수신되는 고유식별정보는 업무상 필요할 경우 암호화 대상에서 제외할 수 있으나, 비밀번호와 바이오정보는 반드시 암호화하여야 한다.
- 전용선을 이용하여 개인정보를 송 · 수신하는 경우, 암호화가 필수는 아니나 내부자에 의한 개인정보 유출 등에 대비해서 가급적 암호화 전송을 권장한다.

- 정보통신망을 통한 개인정보 암호화 전송을 위해 SSL 등의 통신 암호 프로토콜이 탑재된 기술을 활용하거나, 개인정보를 암호화 저장한 후 이를 전송하는 방법 등을 사용할 수 있다.

※ SSL(Secure Sockets Layer)은 웹 브라우저와 웹 서버간에 데이터를 안전하게 주고받기 위해 암호화 기술이 적용된 보안 프로토콜이다.

[SSL 적용 예시]

[일반 웹주소] [SSL 적용 웹주소]

[인증기관(CA)] [SSL설치 웹서버] [사용자]

※ 개인정보 암호화 전송기술 사용시 안전한 전송을 위해 잘 알려진 취약점(예: Open SSL 사용시 HeartBleed 취약점)들을 조치하고 사용 할 필요가 있다.

- "보조저장매체"를 통해 고유식별정보, 비밀번호, 바이오정보를 전달하는 경우에도 암호화 하여야 하며, 이를 위해 다음과 같은 방법 등이 사용 될 수 있다.
  - 암호화 기능을 제공하는 보안USB 등의 보조저장매체에 저장하여 전달
  - 해당 개인정보를 암호화 저장 한 후 보조저장매체에 저장하여 전달

③ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

- 개인정보처리자는 비밀번호, 바이오정보(지문, 홍채 등)가 노출 또는 위 · 변조되지 않도록 암호화하여 저장하여야 하며, 특히 비밀번호의 경우에는 복호화되지 않도록 일방향 (해쉬 함수) 암호화하여야한다.
- 일방향 암호화는 저장된 값으로 원본값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로, 인증검사 시에는 사용자가 입력한 비밀번호를 일방향 함수에 적용하여 얻은 결과값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인한다.

[일방향(해쉬 함수) 암호화]

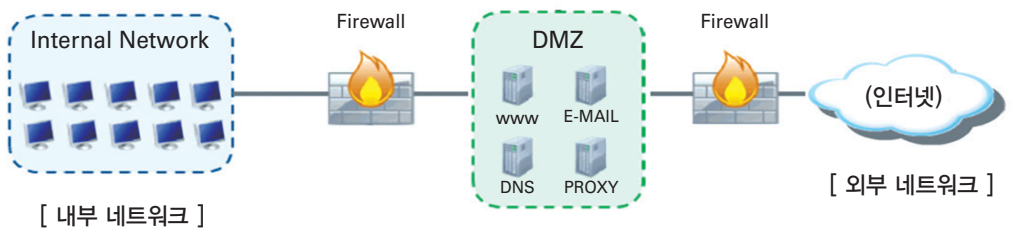
- 일방향(해쉬 함수) 암호화는 입력된 데이터를 자르고 치환하거나 위치를 바꾸는 등의 방법을 사용해 길이가 고정된 결과를 만들어 내는 방법을 의미한다.
- 일방향(해쉬 함수) 암호화의 가장 기본적인 성질은 두 해쉬 결과가 다르다면 원래의 데이터도 어딘가 다르다는 것을 의미하며, 원래 입력의 한 비트만 바뀌더라도 해쉬 결과는 크게 달라진다.

■ 바이오정보의 경우, 복호화가 가능한 양방향 암호화 저장이 필요하나, 이는 식별 및 인증 등의 고유기능에 사용되는 경우로 한정되며 콜센터 등 일반 민원 상담시 저장되는 음성기록이나 일반 사진 정보는 암호화 대상에서 제외된다.

④ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

■ 인터넷 구간은 개인정보처리시스템과 인터넷이 직접 연결되어 있는 구간, DMZ 구간은 인터넷과 내부망과 인터넷 구간 사이에 위치한 중간 지점으로 침입차단시스템 등으로 접근제한 등을 수행하지만 외부망에서 직접 접근이 가능한 영역을 말한다. 내부망은 접근통제시스템 등에 의해 차단되어 외부에서 직접 접근이 불가능한 영역을 말한다.

[DMZ 구간 예시]



■ 인터넷 구간이나 DMZ 구간은 외부에서 직접 접근이 가능하므로 외부자의 침입을 받을 가능성이 있다. 이에 따라 DMZ 구간에 주민등록번호, 외국인등록번호, 운전면허번호, 여권번호 등의 고유식별정보를 저장하는 경우 암호화하여 저장해야 한다. 제2항에 따른 비밀번호 및 바이오정보를 저장하는 경우에도 암호화하여 저장해야한다.

■ 주민등록번호를 암호화 저장하는 경우, 속도 등 성능을 고려하여 일부 정보만 암호화 조치를 취할 수 있으며, 이 경우 뒷 자리 6개 번호 이상을 암호화 조치하는 것이 바람직하다.

※ 일부 암호화의 예시: 010101-3******

⑤ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
2. 위험도 분석에 따른 결과

■ 내부망에 고유식별정보를 저장하는 경우, 개인정보 영향평가 및 위험도 분석 결과에 따라 암호화 적용여부 및 적용범위를 정하여 시행할 수 있다.

■ 영 제38조에 따라 영향평가의 대상이 되는 개인정보파일을 운용하는 공공기관은 해당 개인정보 영향평가의 결과에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

– 개인정보 영향평가의 실시대상이 아니거나 공공기관 이외의 개인정보처리자는 위험도 분석을 실시한 후 그 결과에 따라 고유식별정보의 암호화 적용여부 및 적용범위를 정하여 시행할 수 있다.

■ 다만, 주민등록번호에 대해서는 “개인정보 보호법” 에 따라 2016년 1월 1일부터 내부망에 저장 시에도 개인정보 영향평가나 위험도 분석의 결과에 관계없이 암호화 하여야 하며, 암호화 적용 대상 및 대상별 적용 시기 등은 “개인정보 보호법” 시행령에 따른다.

TIP

• 개인정보 영향평가 수행을 위한 “개인정보 영향평가 수행 안내서” 등의 관련 자료는 개인정보보호 종합지원 포털(http://www.privacy.go.kr)에서 다운로드 할 수 있다.

■ “위험도 분석”은 개인정보처리시스템에 적용되고 있는 개인정보 보호를 위한 수단과 유출시 정보주체의 권리를 해할 가능성과 그 위험의 정도를 분석하는 행위를 말한다.

– 세부적으로 위험도 분석은 개인정보 유출에 영향을 미칠 수 있는 다양한 위협에 대한 시스템 취약점과 이로 인해서 예상되는 손실을 분석하여 위험요소를 식별, 평가하고 그러한 위험요소를 적절하게 통제할 수 있는 수단을 체계적으로 구현하고 운영하는 전반적인 행위 및 절차로서 위험관리의 일부분이다.

– "위험도 분석"은 개인정보를 저장하는 정보시스템에서 개인정보파일 단위로 수행하고 각 개별 개인정보파일의 위험점수에 따라 개별 개인정보파일 단위로 암호화 여부를 결정해야하며, 위험도 분석을 수행한 결과는 최고경영층으로부터 내부결재 등의 승인을 받아야 한다.

TIP

- 위험도 분석을 위한 세부 기준인 "개인정보 위험도 분석 기준 및 해설서"는 개인정보보호 종합지원 포털(http://www.privacy.go.kr)에서 다운로드 할 수 있다.

⑥ 개인정보처리자는 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

■ 암호화 대상인 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호), 비밀번호, 바이오정보를 암호화 하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 하며, "안전한 암호알고리즘"이란 국내 및 미국, 일본, 유럽 등의 국외 암호 연구 관련 기관에서 권고하는 알고리즘을 의미한다.

TIP

- 안전한 암호알고리즘, 암호화 방식 등은 "개인정보 암호화 조치 안내서"를 참조하고, 해당 자료는 개인정보보호 종합지원 포털(http://www.privacy.go.kr)에서 다운로드 할 수 있다.
- 국내외 암호 연구 관련 기관은 한국인터넷진흥원(KISA)의 암호이용활성화 홈페이지(http://seed.kisa.or.kr)의 "암호 표준화 및 유관기관"에서도 확인 가능하다.

■ 안전한 암호알고리즘을 사용하더라도 암호화 키가 잘못 관리되어 유 · 노출 되는 경우에는 암호화된 정보들이 유 · 노출될 수 있으므로 이를 안전하게 관리하여야 한다.

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

■ 고유식별정보를 업무용 컴퓨터 또는 모바일 기기에 저장하여 관리하거나, 개인정보처리시스템으로부터 개인정보취급자의 업무용 컴퓨터, 모바일 기기에 내려 받아 저장할 때는 안전한 암호화 알고리즘이 탑재된 암호화 소프트웨어 등을 이용하여 암호화함으로써 불법적인 유·노출 및 접근으로부터 차단하여야 한다.

[오피스에서 파일 암호화 설정방법]

- 한컴 오피스 : 파일 ▶ 다른이름으로 저장하기 ▶ 문서 암호 설정에서 암호 설정 가능
- MS 오피스 : 파일 ▶ 다른이름으로 저장하기 ▶ 도구 ▶ 일반옵션에서 암호 설정 가능

7. 접속기록의 보관 및 점검

제7조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관 · 관리하여야 한다.

② 개인정보처리자는 개인정보의 유출 · 변조 · 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.

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

취지

- 접속기록은 개인정보의 입 · 출력 및 수정사항, 파일별 · 담당자별 데이터접근내역 등을 자동으로 기록하는 로그 파일을 생성하여 불법적인 접근 또는 행동을 확인할 수 있는 중요한 자료이며, 접속기록의 백업은 개인정보 DB의 무결성을 유지하기 위한 중요한 요소이다.
- 따라서, 접속기록을 6개월 이상 안전하게 보관 · 관리하고 반기별 1회 이상 정기적으로 점검하여야 하며, 이를 통해 비정상행위에 대해 적절한 조치를 취할 필요가 있다.

해설

① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 6개월 이상 보관 · 관리하여야 한다.

- 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우, 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등의 접속기록을 6개월 이상 저장하고 정기적으로 확인 · 감독 하여야한다.

[접속기록 항목 예시]

필수 기록 항목	설명
ID	개인정보취급자 식별정보
날짜 및 시간	접속 일시
접속자 IP 주소	접속자 정보
수행 업무	열람, 수정, 삭제, 인쇄, 입력 등

TIP

- 개인정보처리시스템에 접속한 기록이 아닌 경우에는 6개월 보관 · 관리가 필수는 아니다.

  (예: 개인정보처리시스템으로 볼 수 없는 업무용 PC만으로 개인정보 처리시, 이 업무용 PC에 접속한 기록은 6개월 보관 · 관리가 필수는 아님)

– 정보주체에 대한 접속기록까지 보관 · 관리하고 정기적으로 확인 · 감독하는 경우 불법적인 접근 및 비정상 행위에 대한 조치 등을 강화할 수 있다.

② 개인정보처리자는 개인정보의 유출 · 변조 · 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.

■ 개인정보처리자는 개인정보의 유출 · 변조 · 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록을 반기별 1회 이상 정기적으로 점검하여야 한다.

– 이를 통해 비인가된 개인정보 처리, 대량의 개인정보의 조회, 정정, 다운로드, 삭제 등의 비정상 행위를 탐지하여 적절한 대응조치를 할 필요가 있다.

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

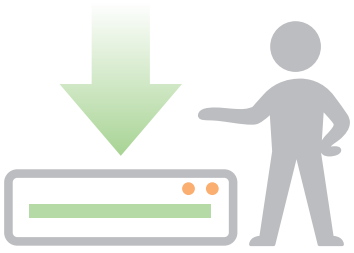
■ 개인정보처리자는 개인정보처리시스템의 접속기록이 위 · 변조 및 도난, 분실되지 않도록 안전하게 보관하여야 한다.

– 즉, 정기적으로 접속기록 백업을 수행하여 개인정보처리시스템 이외의 별도의 보조저장매체나 별도의 저장장치에 보관하는 등의 조치가 필요하다.

– 접속기록에 대한 위 · 변조를 방지하기 위해서는 CD-ROM 등과 같은 덮어쓰기 방지 매체를 사용하는 것이 바람직하다.

– 접속기록을 수정 가능한 매체(하드디스크, 자기 테이프 등)에 백업하는 경우에는 무결성 보장을 위해 위 · 변조 여부를 확인할 수 있는 정보를 별도의 장비에 보관 · 관리할 수 있다.

※ 접속기록을 HDD에 보관하고, 위 · 변조 여부를 확인할 수 있는 정보(MAC 값, 전자서명 값 등)는 별도의 HDD 또는 관리대장에 보관하는 방법으로 관리할 수 있다.



8. 악성프로그램 등 방지

제8조(악성프로그램 등 방지) 개인정보처리자는 악성프로그램 등을 방지 · 치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치 · 운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시

취지

- 악성프로그램이란 제작자가 의도적으로 피해를 주고자 악의적 목적으로 만든 프로그램 및 실행 가능한 코드를 의미하는 것으로 악성 코드라고 불리기도 한다. 컴퓨터 바이러스(Computer Virus), 인터넷 웜(Internet Worm), 트로이목마, 스파이웨어 등의 형태로 나눌 수 있다.
- 악성프로그램은 컴퓨터에서 동작하는 일종의 프로그램으로 자료를 손상 · 유출하거나 프로그램을 파괴하여 정상적인 작업을 방해한다. 이를 방지하기 위해 백신 소프트웨어 등의 보안 프로그램을 이용하여 해당 프로그램을 제거하거나 예방할 필요가 있다.

해설

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

- 개인정보처리자는 악성프로그램 등을 통해 개인정보가 위 · 변조, 유출되지 않도록 이를 방지하고 치료할 수 있는 백신 소프트웨어 등 보안 프로그램을 설치 · 운영하여야 한다.
- 백신 소프트웨어 등의 보안 프로그램은 실시간 감시 등을 위해 항상 실행된 상태를 유지해야 한다.
- 백신 소프트웨어 등 보안 프로그램은 자동 업데이트 기능을 사용하거나 일 1회 이상 주기적으로 업데이트를 실시하여 최신의 상태로 유지해야 한다.

– 실시간으로 신종 · 변종 악성 프로그램이 유포됨에 따라 백신 상태를 최신의 업데이트를 적용하여 유지해야 하며, 백신 소프트웨어 등에서 제공하는 자동 업데이트 기능 등을 활용하면 편리하고 신속하게 조치할 수 있다.

– 특히 대량의 개인정보를 처리하거나 민감한 정보 등 중요도가 높은 개인정보를 처리하는 경우에는 키보드, 화면, 메모리해킹 등 신종 악성 프로그램에 대해 대응 할 수 있도록 보안프로그램을 운영할 필요가 있으며, 항상 최신의 상태로 유지하여야 한다.

[백신 소프트웨어 설정 예시]

[자동, 예약 업데이트]

[실시간, 예약 검사]

2. 악성프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시

■ 운영체제(OS) · 응용 프로그램의 보안 취약점을 악용하는 악성 프로그램 경보가 발령되었거나, 응용 프로그램, 운영체제 제작업체에서 보안 업데이트 공지가 있는 경우에는 감염을 예방하고 감염된 경우 피해를 최소화하기 위해 즉시 업데이트를 실시하여야 한다.

– 운영체제나 응용 프로그램 보안 업데이트시 현재 운영중인 응용 프로그램의 업무 연속성이 이루어 질 수 있도록 보안 업데이트를 적용하는 것이 필요하며, 가능한 자동으로 보안 업데이트가 설정되도록 할 필요가 있다.

※ 한글 Office나 MS Office 등 개인정보처리에 자주 이용되는 응용프로그램은 자동업데이트 설정시, 보안 업데이트 공지에 따른 즉시 업데이트가 용이하다.

9. 물리적 접근 방지

제9조(물리적 접근 방지) 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 보안 대책을 마련하여야 한다. 다만 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

취지

- 개인정보를 대량으로 보관하고 있는 전산실 · 자료보관실 등 물리적 보관장소를 별도로 가지고 있는 경우, 출입자에 의한 개인정보 대량 유출의 위험이 있으므로 이에 대한 출입통제 절차를 수립하여 운영하고 보조저장매체의 반 · 출입 통제를 위한 보안대책을 마련하여 대응할 필요가 있다.
- 또한 사무실 등에서 개인정보가 포함된 보조저장매체 분실 등으로 인한 개인정보 유출의 위험성이 있으므로 이에 대한 대책 또한 필요하다.

해설

① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립 · 운영하여야 한다.

- 개인정보를 대량으로 보관하고 있는 전산실 · 자료보관실을 별도로 두고 있는 경우에는 비인가자의 출입에 의한 개인정보가 포함된 정보자산의 절도, 파괴 등 물리적 위협에 대응하기 위해 출입통제 절차를 수립 · 운영하여야 한다.

- 전산실 · 자료보관실의 출입을 통제하는 방법으로 물리적 접근 방지를 위한 장치를 설치 · 운영하고 이에 대한 출입 내역을 전자적인 매체 또는 수기문서 대장에 기록하는 방법 등이 있다.
  - 물리적 접근 방지를 위한 장치(예시): 비밀번호 기반 출입통제 장치, 스마트 카드 기반 출입통제장치, 지문 등 바이오정보 기반 출입통제 장치 등
    ※ 전산실은 다량의 정보시스템을 운영하기 위한 별도의 물리적인 공간으로 전기시설(UPS(Uninterruptible Power Supply), 발전기 등), 공조시설(항온항습기 등), 소방시설(화재감지기, 소화설비 등)등을 갖춘 시설을 의미한다.
    ※ 자료보관실은 가입신청서 등의 문서나 DAT(Digital Audio Tape), LTO(Linear Tape Open), DLT(Digital Linear Tape), CD(Compact Disc), DVD(Digital Versatile Disk), 하드디스크, SSD(Solid State Drive) 등 전자적 기록매체가 다량으로 보관된 물리적 저장장소를 의미한다.

② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

- 개인정보처리자는 개인정보가 포함된 서류나 보조기억매체(USB, CD 등) 등은 잠금장치가 부착되어 있는 안전한 장소에 보관하여야 한다.
  - 플로피디스켓, 이동형 하드디스크, USB메모리, SSD, CD, DVD 등의 보조기억매체는 금고 또는 잠금장치가 있는 캐비넷 등에 안전하게 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.

- 개인정보처리자는 사무실 등 개인정보를 처리하는 업무공간에서 개인정보가 저장된 USB메모리, CD, 이동형 하드디스크 등의 보조저장매체 반 · 출입에 의해 개인정보가 유출되지 않도록 반출 · 입 통제를 위한 보안대책을 마련하여야 한다.
- 보조저장매체 반 · 출입 통제를 위한 보안대책 마련시 다음과 같은 내용이 포함되도록 고려할 필요가 있다.
  - 보조저장매체 보유 현황 파악 및 반 · 출입 관리 계획
  - 개인정보취급자(임직원, 파견근로자, 시간제근로자 등) 및 용역업체의 직원 등에 의한 비인가된 보조저장매체 반 · 출입에 대한 대응

– 개인정보처리시스템, 업무용 PC, 모바일 기기 등에서 보조저장매체의 안전한 사용 방법 및 비인가된 사용에 대한 대응 등

■ 보조저장매체 반 · 출입 통제를 위한 보안대책은 전사적으로 수립되어 운영되도록 할 필요가 있다.

TIP

• 보조저장매체 반 · 출입 통제를 위한 보안대책은 별도의 대책으로 마련 할 수도 있고, 내부관리계획, 지침, 내규 등 다른 관리계획의 일부에 포함될 수도 있다.

■ 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 보조저장매체 반 · 출입 통제를 위한 보안대책 마련이 필수는 아니나, 관련 대책 마련을 권장한다.

※ 예를 들어 소상공인이 사무실에 업무용 PC만 사용하여 개인정보를 처리하는 경우

10. 개인정보의 파기

제10조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각 · 파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

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

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

취지

- 개인정보처리자는 개인정보 수집목적 달성, 보존기간이 경과 등 개인정보가 불필요하게 되었을 때 개인정보의 유출 및 오남용 방지를 위해 개인정보를 복원이 불가능한 방법으로 파기가 필요하다.
  ※ '복원이 불가능한 방법'이란 사회 통념상 현재의 기술수준에서 적절한 비용이 소요되는 방법을 의미한다.
- 또한, 개인정보 파기 방법 중 개인정보의 일부만 파기시 완전파괴 방법 등을 사용하기 어려운 특정 환경에서도 복구 및 재생되지 않도록 조치하는 방법이 필요하다.

해설

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

1. 완전파괴(소각 · 파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

■ 개인정보처리자는 개인정보를 파기하는 경우 복구 또는 재생되지 아니하도록 개인정보가 저장된 매체 형태에 따라 다음 중 어느 하나의 조치를 하여야 한다.

– 완전파괴(소각 · 파쇄 등)

※ 예시: 개인정보가 저장된 회원가입신청서 등의 종이문서, 하드디스크나 자기테이프를 파쇄기로 파기하거나 용해, 또는 소각장, 소각로에서 태워서 파기 등

– 전용 소자장비를 이용하여 삭제

※ 예시: 디가우저(Degausser)를 이용해 하드디스크나 자기테이프에 저장된 개인정보 삭제 등

– 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

※ 예시: 개인정보가 저장된 하드디스크에 대해 완전포맷(3회 이상 권고), 데이터 영역에 무작위 값, 0, 1 등으로 덮어쓰기(3회 이상 권고), 해당 드라이브를 안전한 알고리즘 및 키 길이로 암호화 저장 후 삭제하고 암호화에 사용된 키 완전 폐기 및 무작위 값 덮어쓰기 등의 방법 사용

TIP

- 개인정보 파기시 파기를 전문으로 수행하는 업체를 활용 할 수 있다.
- 개인정보 파기의 시행 및 파기 결과의 확인은 개인정보 보호책임자의 책임하에 수행되어야 하며, 파기에 관한 사항을 기록 · 관리하여야 한다.

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려운 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, 천공 등으로 삭제

■ "개인정보의 일부만 파기하는 경우"는 저장중인 개인정보 중 보유기간이 경과한 일부 개인정보를 파기하는 경우를 말하며, 다음과 같은 경우 등이 있다.

– 운영 중인 개인정보가 포함된 여러 파일 중, 특정 파일을 파기하는 경우

– 개인정보가 저장된 백업용 디스크나 테이프에서 보유기간이 만료된 특정 파일이나 특정 정보주체의 개인정보만 파기하는 경우

– 운영 중인 데이터베이스에서 탈퇴한 특정 회원의 개인정보를 파기하는 경우

– 회원가입신청서 종이문서에 기록된 정보 중, 특정 필드의 정보를 파기하는 경우 등

■ 개인정보처리자가 개인정보의 일부만 파기하는 경우 복구 또는 재생되지 아니하도록 개인정보가 저장된 매체 형태에 따라 다음 중 어느 하나의 조치를 하여야 한다.

– 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독

※ 개인정보를 삭제하는 방법 예시: 운영체제, 응용프로그램, 상용 도구 등에서 제공하는 삭제 기능을 사용하여 삭제, 백업시 파기 대상 정보주체의 개인정보를 제외한 백업 등 (운영체제, 응용프로그램, 상용 도구 등에서 제공하는 삭제 기능을 사용하는 경우에도 가능한 복구 불가능한 방법을 사용해야 복구 및 재생의 위험을 줄일 수 있다)

※ 복구 및 재생되지 않도록 관리 및 감독하는 방법 예시: 복구 관련 기록 · 활동에 대해 모니터링하거나 주기적 점검을 통해 비인가된 복구에 대해 조치

– 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

※ 예시: 회원가입 신청서에 기재된 주민등록번호 삭제시, 해당 신청서에서 주민등록번호가 제거되도록 절삭, 천공 또는 펜 등으로 마스킹

부칙 <제2011-43호, 2011. 9. 30.>

제1조 이 기준은 고시한 날부터 시행한다.

취지

- 이 고시의 시행일에 대한 정의를 하고 있다. 시행되는 일시는 고시한 날부터이다.

제2조(영상정보처리기기에 대한 안전성 확보조치의 적용 제외) 영상정보처리기기에 대한 안전성 확보조치에 대해서는 「표준 개인정보 보호지침」중에서 영상정보처리기기 설치 · 운영 기준이 정하는 바에 따른다.

취지

- 영상정보처리기기에 대한 안전성 확보조치 기준은 「표준 개인정보 보호지침」의 영상정보처리기기 설치 · 운영 기준에서 언급된 안전성 확보조치 기준이 정하는 바에 따른다.

제3조(전산센터, 클라우드컴퓨팅센터 등의 운영환경에서의 안전조치) 개인정보처리자가 전산센터(IDC : Internet Data Center), 클라우드컴퓨팅센터(Cloud Computing Center) 등에 계약을 통해 하드웨어, 소프트웨어 등을 임차 또는 임대하여 개인정보를 처리하는 경우에는 계약서 또는 서비스수준협약서(SLA : Service Level Agreement)에 이 기준에 준하는 수준의 안전조치 내용이 포함되어 있으면 이 기준을 이행한 것으로 본다.

부칙<제2014-7호, 2014. 12. 30.>

이 기준은 고시한 날부터 시행한다.

개인정보의 안전성 확보조치 기준 해설서

[붙임] FAQ

03 [붙임] FAQ

문1. 개인정보처리시스템의 범위는 어디까지를 말하는지?

개인정보처리시스템은 DBMS(database management system)로서, 다수의 사용자들이 데이터베이스(DB) 내의 데이터에 접근할 수 있도록 해주는 응용프로그램의 집합을 말합니다.

여기에는 DB자체 뿐 아니라, DB에 연결되어 DB를 관리하거나 DB의 개인정보를 처리할 수 있는 응용 프로그램(예: 웹 서버)까지 포함될 수 있습니다.

문2. 개인용 스마트폰에서 회사 e-mail 서버로부터 자료를 주고받아 개인정보 처리 업무를 수행하는 경우에, 모바일 기기에 포함되는지?

모바일 기기에 포함됩니다.

개인용 스마트폰이나 태블릿PC에 회사의 업무용 앱(App)을 설치하여 업무목적의 개인정보를 처리하는 경우나, 개인용 스마트폰이나 태블릿PC에 설치된 메일 읽기 프로그램을 사용하여 회사 메일서버에 접속하여 업무목적의 개인정보를 처리하는 경우에는 모바일 기기에 해당됩니다.

다만, 개인용 스마트폰이 회사 e-mail 서버로부터 자료를 주고 받더라도 개인정보가 포함되지 않거나, 회사 업무목적 아닌 경우는 모바일 기기에서 제외됩니다.

문3. 전용선의 범위는 어디까지 인지?

두 지점간에 독점적으로 사용하는 회선으로 개인정보처리자와 개인정보취급자, 또는 본점과 지점간을 직통으로 연결하는 회선 등을 말합니다.

문4. 개인정보처리자로부터 업무를 위탁받아 처리하는 수탁자도 이 기준을 준수하여야 합니까?

그렇습니다.

"수탁자"는 개인정보처리자로부터 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위 등의 업무를 위탁받아 처리하는 자를 말합니다(법 제26조). 그런데 수탁자에 관하여는 개인정보의 안전성 확보조치에 관한 개인정보 보호법 제24조제3항, 제29조가 준용되어 적용됩니다 (법 제26조제7항). 따라서 수탁자는 이 기준에 따라 개인정보의 안전성 확보에 필요한 조치를 이행하여야 합니다.

문5. 「소기업 및 소상공인 지원을 위한 특별조치법」에 따른 소상공인입니다. 내부관리계획을 수립하지 않아도 되는지?

소상공인은 "개인정보의 안전성 확보조치 기준" 제3조제2항에 의거 내부관리계획을 수립하지 않아도 됩니다.

문6. 개인정보 보호에 관한 사항을 회사규칙으로 마련한 경우에도 「개인정보 보호법」에 따른 내부관리계획을 별도로 마련해야 하는지?

회사규칙에 내부관리계획에 포함되어야 하는 내용(개인정보 보호책임자의 지정에 관한 사항, 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항, 개인정보의 안전성 확보에 필요한 조치에 관한 사항, 개인정보취급자 교육에 관한 사항, 수탁자에 대한 관리 및 감독에 관한 사항, 그 밖에 개인정보 보호를 위하여 필요한 사항)이 모두 포함되어 있다면 별도의 내부관리계획을 마련하지 않아도 됩니다.

문7. 비디오 대여점을 운영하는 소상공인입니다. 현재 고객관리를 위해 업무용 컴퓨터를 운영하고 있습니다. "개인정보의 안전성 확보조치 기준"에 따라 어떠한 조치를 수행해야 하는지?

업무용 컴퓨터로 고객정보를 관리하는 경우 제4조(접근 권한의 관리)제5항에 따라 업무용 컴퓨터에 비밀번호를 설정하고 업무용 컴퓨터에서 제공되는 침입차단 기능을 설정하고 악성프로그램을 차단하도록 백신 소프트웨어를 설치하여야 합니다. 또한, 업무용 컴퓨터에 주민등록번호 등 고유식별정보가 저장된 경우에는 암호화 등의 보안조치를 수행하여야 합니다.

문8. 백화점입니다. 고객정보 데이터베이스를 운영하고 있습니다. 개인정보 암호화 대상이 무엇이며 어떻게 해야 하는지?

"개인정보 보호법" 상에서 요구되는 암호화 대상은 고유식별정보(주민등록번호, 외국인등록번호, 운전면허번호, 여권번호), 비밀번호, 바이오정보입니다. 개인정보처리자는 고유식별정보 등을 정보통신망 또는 보조저장매체 등을 통해 전달하는 경우 암호화하여 전송해야 합니다. 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 고유식별정보를 저장하는 경우에도 반드시 암호화하여야 합니다. 또한, 내부망에 고유식별정보를 저장하는 경우 위험도 분석 또는 영향평가 후에 암호화 적용범위 및 적용범위를 정하여 시행할 수 있습니다.

[암호화 적용 기준 요약표]

<table>
<tr><th colspan="3">구 분</th><th>암호화 기준</th></tr>
<tr><td>정보통신망, 보조저장매체를 통한 송 · 수신 시</td><td colspan="2">비밀번호, 바이오정보, 고유식별정보</td><td>암호화 송 · 수신
※ 내부망에서 전송시 해설 내용 참조</td></tr>
<tr><td rowspan="4">개인정보처리시스템에 저장 시</td><td colspan="2">비밀번호</td><td>일방향 암호화 저장</td></tr>
<tr><td colspan="2">바이오정보</td><td>암호화 저장</td></tr>
<tr><td rowspan="2">고유식별정보</td><td>인터넷 구간, 인터넷 구간과 내부망의 중간 지점(DMZ)</td><td>암호화 저장</td></tr>
<tr><td>내부망에 저장</td><td>암호화 저장 또는 다음 항목에 따라 암호화 적용여부 · 적용범위를 정하여 저장
① 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과
② 위험도 분석에 따른 결과</td></tr>
<tr><td>업무용 컴퓨터, 모바일 기기에 저장시</td><td colspan="2">비밀번호, 바이오정보, 고유식별정보</td><td>암호화 저장(비밀번호는 일방향 암호화 저장)</td></tr>
</table>

다만, 주민등록번호의 경우에는 2016년 1월 1일부터는 내부망에 저장하는 경우라도 개인정보 영향평가나 위험도 분석의 결과에 관계없이 암호화 하여야 하며, 암호화 적용 대상 및 대상별 적용 시기 등은 “개인정보 보호법” 시행령에 따릅니다.

문9. 내부망에 저장하는 주민등록번호는 영향평가나 위험도 분석을 통해 암호화하지 않고 보유할 수 있는지?

2016년 1월 1일 이전까지는 가능하나, 2016년 1월 1일부터 내부망에 저장하는 경우라도 개인정보 영향평가나 위험도 분석의 결과에 관계없이 암호화 하여야 하며, 암호화 적용 대상 및 대상별 적용 시기 등은 “개인정보 보호법” 시행령에 따릅니다.

문10. 암호화해야 하는 바이오정보의 대상은 어디까지 인지?

암호화 하여야 하는 바이오정보는 식별 및 인증 등의 고유기능에 사용되는 경우로 한정되며 콜센터 등 일반 민원 상담시 저장되는 음성기록이나 일반 사진 정보는 암호화 대상에서 제외됩니다.

바이오정보인 경우에 원본 데이터와 가공되거나 생성된 특징정보 모두 암호화 대상입니다.

문11. 특정기관에서 암호화 관련 준수해야 하는 지침과 본 고시에서 규정한 암호화 요구사항 중 어느 것을 적용해야 하는지?

“개인정보 보호법” 측면에서는 본 고시에서 규정한 암호화 요구사항을 준수하면 “개인정보 보호법”상 암호화 의무는 준수한 것입니다. 본 고시 준수로 인하여 다른 지침을 준수하기 어렵게 된다면 “개인정보 보호법” 은 준수하였으나 해당 지침은 위배한 것이 될 수 있습니다. 따라서, 최선의 방법은 본 고시에서 규정한 암호화 요구사항과 다른 암호화 관련 지침의 요구사항 모두를 준수하는 것이라 할 수 있습니다.

문12. 업무용 PC에서 고유식별정보나 바이오정보를 처리하는 경우 개인정보 암호화는 어떻게 해야 하는지?

PC에 저장된 개인정보의 경우 상용프로그램(한글, 엑셀 등)에서 제공하는 비밀번호 설정기능을

사용하여 암호화를 적용하거나, 안전한 암호화 알고리즘을 이용하는 소프트웨어를 사용하여 암호화해야 합니다.

암호화에 관한 세부 질문사항은 '개인정보 암호화 조치 안내서'를 참고 할 수 있습니다.

문13. 전산실 또는 자료보관실이 없는 중소기업입니다. "개인정보의 안전성 확보조치 기준" 제9조 (물리적 접근 방지)조항을 준수해야 하는지?

기업의 규모에 상관없이 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관장소를 별도로 운영하고 있지 않으면 출입통제 절차를 수립 · 운영하지 않아도 됩니다.

다만 서류나, 보조저장매체 등을 운영하는 경우에는 잠금장치가 있는 캐비넷 등에 안전하게 보관하여야 하며, 보조저장매체의 반출 · 입 통제를 위한 보안대책을 마련해서 운영해야 합니다.

문14. 접속기록 중, 수행업무에 남겨야 하는 내용은 무엇인지?

접속기록에는 식별자, 접속일시, 접속지를 알 수 있는 정보와 수행업무가 포함됩니다.

수행업무는 정보주체의 개인정보에 대한 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄) 등의 내역을 말합니다.

특히, 개인정보취급자가 특정 정보주체의 개인정보를 처리 한 경우, '수행업무'에는 해당 정보주체에 대한 식별정보도 포함됩니다.

행정자치부

KISA 한국인터넷진흥원
Korea Internet & Security Agency