개인정보의
안전성 확보조치 기준 해설서

2020. 12.

개인정보보호위원회

KISA 한국인터넷진흥원

본 해설서에서는「개인정보 보호법」(이하 “법”이라 한다.)과 「개인정보의 안전성 확보조치 기준」에 따라 개인정보처리자가 조치하여야 하는 최소한의 보호조치를 안내하고 있습니다.

개인정보처리자는 본 해설서에서 안내하고 있는 보호조치 이외에 개인정보의 유형 및 중요도, 개인정보를 처리하는 방법 및 환경, 보안위험요인 등을 고려하여 필요하다면 추가적인 보호조치를 적용하여 개인정보의 안전성 확보조치를 강화하시기 바랍니다.

목 차

Ⅰ.「개인정보의 안전성 확보조치 기준」 개요 ····· 1

1. 개 요 ····· 1
2. 법적 근거 ····· 2

Ⅱ.「개인정보의 안전성 확보조치 기준」 전문 ····· 4

Ⅲ.「개인정보의 안전성 확보조치 기준」 해설 ····· 12

[제1조] 목적 ····· 13
[제2조] 정의 ····· 16
[제3조] 안전조치 기준 적용 ····· 31
[제4조] 내부 관리계획의 수립·시행 ····· 33
[제5조] 접근 권한의 관리 ····· 46
[제6조] 접근통제 ····· 51
[제7조] 개인정보의 암호화 ····· 60
[제8조] 접속기록의 보관 및 점검 ····· 70
[제9조] 악성프로그램 등 방지 ····· 75
[제10조] 관리용 단말기의 안전조치 ····· 77
[제11조] 물리적 안전조치 ····· 79
[제12조] 재해·재난 대비 안전조치 ····· 81
[제13조] 개인정보의 파기 ····· 84
[제14조] 재검토기한 ····· 87
[부칙] ····· 87
[별표] ····· 88

[붙임] FAQ ····· 89
[참고] 안전조치 기준 적용 유형 ····· 98

Ⅰ 「개인정보의 안전성 확보조치 기준」 개요

1 개 요

구 분	「개인정보의 안전성 확보조치 기준」
법적 근거	o 개인정보보호법 제23조(민감정보의 처리 제한), 제24조(고유식별정보의 처리 제한), 제29조(안전조치의무) o 같은 법 시행령 제21조(고유식별정보의 안전성 확보 조치), 제30조(개인정보의 안전성 확보 조치)
과징금 부과 및 벌칙	o 2년 이하의 징역 또는 2천만원 이하의 벌금(법 제73조제1호) o 3천만원 이하의 과태료(법 제75조제2항제6호)
적용 대상	o 개인정보처리자 o 개인정보처리자로부터 개인정보를 제공받은 자 o 개인정보처리자로부터 개인정보 처리를 위탁받은 자(이하 '수탁자', 준용)
목 적	o 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정함
성 격	o 반드시 준수해야 하는 최소한의 기준
주요 내용	o 내부 관리계획의 수립·시행 o 접근 권한의 관리 o 접근통제 o 개인정보의 암호화 o 접속기록의 보관 및 점검 o 악성프로그램 등 방지 o 관리용 단말기의 안전조치 o 물리적 안전조치 o 재해·재난 대비 안전조치 o 개인정보의 파기

2 법적 근거

o 이 기준은「개인정보보호법」제23조, 제24조, 제29조 및 같은 법 시행령 제21조, 제30조에 근거한다.

o 따라서, 개인정보처리자는 개인정보를 처리할 때 이 기준을 준수하여야 한다.

o 이 기준에 따른 안전성 확보 조치를 하지 아니한 자 등에게는 관련 법률에 따라 벌칙(징역 또는 벌금), 과태료를 부과할 수 있다.

개인정보보호법

제23조(민감정보의 처리 제한) ① 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다.

제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 "고유식별정보"라 한다)를 처리할 수 없다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우

② 삭제

③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

④ 보호위원회는 처리하는 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 제3항에 따라 안전성 확보에 필요한 조치를 하였는지에 관하여 대통령령으로 정하는 바에 따라 정기적으로 조사하여야 한다.

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

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

1. 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자

제75조(과태료) ② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.

6. 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자

개인정보보호법 시행령

제21조(고유식별정보의 안전성 확보 조치) ① 법 제24조제3항에 따른 고유식별정보의 안전성 확보 조치에 관하여는 제30조 또는 제48조의2를 준용한다. 이 경우 "법 제29조"는 "법 제24조제3항"으로, "개인정보"는 "고유식별정보"로 본다.

② 법 제24조제4항에서 "대통령령으로 정하는 기준에 해당하는 개인정보처리자"란 다음 각 호의 어느 하나에 해당하는 개인정보처리자를 말한다.

1. 공공기관
2. 5만명 이상의 정보주체에 관하여 고유식별정보를 처리하는 자

③ 보호위원회는 제2항 각 호의 어느 하나에 해당하는 개인정보처리자에 대하여 법 제24조제4항에 따라 안전성 확보에 필요한 조치를 하였는지를 2년마다 1회 이상 조사해야 한다.

④ 제3항에 따른 조사는 제2항 각 호의 어느 하나에 해당하는 개인정보처리자에게 온라인 또는 서면을 통하여 필요한 자료를 제출하게 하는 방법으로 한다.

⑤ 법 제24조제5항에서 "대통령령으로 정하는 전문기관"이란 다음 각 호의 기관을 말한다.

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원(이하 "한국인터넷진흥원"이라 한다)
2. 법 제24조제4항에 따른 조사를 수행할 수 있는 기술적·재정적 능력과 설비를 보유한 것으로 인정되어 보호위원회가 정하여 고시하는 법인, 단체 또는 기관

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

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

② 보호위원회는 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

Ⅱ 「개인정보의 안전성 확보조치 기준」 전문

제정 2020. 8. 11. 개인정보보호위원회고시 제2020-2호

제1조(목적) 이 기준은 「개인정보 보호법」(이하 “법”이라 한다) 제23조제2항, 제24조제3항 및 제29조와 같은 법 시행령(이하 “영”이라 한다) 제21조 및 제30조에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 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. “대기업”이란 「독점규제 및 공정거래에 관한 법률」 제14조에 따라 공정거래위원회가 지정한 기업집단을 말한다.
5. “중견기업”이란 「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」 제2조에 해당하는 기업을 말한다.
6. “중소기업”이란 「중소기업기본법」 제2조 및 동법 시행령 제3조에 해당하는 기업을 말한다.
7. “소상공인”이란 「소상공인 보호 및 지원에 관한 법률」 제2조에 해당하는 자를 말한다.
8. “개인정보 보호책임자”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.
9. “개인정보취급자”란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
10. “개인정보처리시스템”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
11. “위험도 분석”이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.

12. “비밀번호”란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
13. “정보통신망”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
14. “공개된 무선망”이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
15. “모바일 기기”란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
16. “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
17. “보조저장매체”란 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.
18. “내부망”이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
19. “접속기록”이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
20. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

제3조(안전조치 기준 적용) 개인정보처리자가 개인정보의 안전성 확보에 필요한 조치를 하는 경우에는 [별표] 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준을 적용하여야 한다. 이 경우 개인정보처리자가 어느 유형에 해당하는지에 대한 입증책임은 당해 개인정보처리자가 부담한다.

제4조(내부 관리계획의 수립·시행) 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.

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

② [별표]의 유형1에 해당하는 개인정보처리자는 제1항에 따른 내부 관리계획을 수립하지 아니할 수 있고, [별표]의 유형2에 해당하는 개인정보처리자는 제1항 제12호부터 제14호까지를 내부 관리계획에 포함하지 아니할 수 있다.

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 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연 1회 이상으로 점검·관리 하여야 한다.

제5조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 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 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.

⑥ 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

⑦ [별표]의 유형1에 해당하는 개인정보처리자는 제1항 및 제6항을 아니할 수 있다.

제6조(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 시도 탐지 및 대응

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

③ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.

④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.

⑤ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 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 접근 통제 기능을 이용할 수 있다.

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

⑧ [별표]의 유형1에 해당하는 개인정보처리자는 제2항, 제4항부터 제5항까지의 조치를 아니할 수 있다.

제7조(개인정보의 암호화) ① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 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. 암호화 미적용시 위험도 분석에 따른 결과

⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

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

⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.

제8조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 다만, 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 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 개인정보를 다운로드한 것이 발견되었을 경우에는 내부 관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.

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

제9조(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, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지

2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시
3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

제10조(관리용 단말기의 안전조치) 개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.
1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
2. 본래 목적 외로 사용되지 않도록 조치
3. 악성프로그램 감염 방지 등을 위한 보안조치 적용

제11조(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.

제12조(재해·재난 대비 안전조치) ① 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

② 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

③ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제1항부터 제2항까지 조치를 이행하지 아니할 수 있다.

제13조(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 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, 천공 등으로 삭제

제14조(재검토 기한) 보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2020년 8월 11일을 기준으로 매 3년이 되는 시점(매 3년째의 8월 10일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부칙<제2020-2호, 2020. 8. 11.>

이 고시는 고시한 날부터 시행한다.

[별표]

개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준

유형	적용 대상	안전조치 기준
유형1 (완화)	· 1만명 미만의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인	· 제5조 : 제2항부터 제5항까지 · 제6조 : 제1항, 제3항, 제6항 및 제7항 · 제7조 : 제1항부터 제5항까지, 제7항 · 제8조 · 제9조 · 제10조 · 제11조 · 제13조
유형2 (표준)	· 100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업 · 10만명 미만의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 · 1만명 이상의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인	· 제4조 : 제1항제1호부터 제11호까지 및 제15호, 제3항부터 제4항까지 · 제5조 · 제6조제1항부터 제7항까지 · 제7조:1항부터 제5항까지, 제7항 · 제8조 · 제9조 · 제10조 · 제11조 · 제13조
유형3 (강화)	· 10만명 이상의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 · 100만명 이상의 정보주체에 관한 개인정보를 보유한 중소기업, 단체	· 제4조부터 제13조까지

Ⅱ 「개인정보의 안전성 확보조치 기준」 해설

[제1조] 목적

[제2조] 정의

[제3조] 안전조치 기준 적용

[제4조] 내부 관리계획의 수립·시행

[제5조] 접근 권한의 관리

[제6조] 접근통제

[제7조] 개인정보의 암호화

[제8조] 접속기록의 보관 및 점검

[제9조] 악성프로그램 등 방지

[제10조] 관리용 단말기의 안전조치

[제11조] 물리적 안전조치

[제12조] 재해·재난 대비 안전조치

[제13조] 개인정보의 파기

[부칙]

[별표]

제1조 목적

제1조(목적) 이 기준은 「개인정보 보호법」(이하 "법"이라 한다) 제23조제2항, 제24조제3항 및 제29조와 같은 법 시행령(이하 "영"이라 한다) 제21조 및 제30조에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정하는 것을 목적으로 한다.

해 설

■ 이 기준은 「개인정보 보호법」 제23조(민감정보의 처리 제한)제2항, 제24조(고유식별정보의 처리 제한)제3항 및 제29조(안전조치의무)와 같은 법 시행령 제21조(고유식별정보의 안전성 확보 조치) 및 제30조(개인정보의 안전성 확보 조치)에 근거한다.

「개인정보 보호법」

제23조(민감정보의 처리 제한) ② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다.

제24조(고유식별정보의 처리 제한) ③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

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

「개인정보 보호법 시행령」

제21조(고유식별정보의 안전성 확보 조치) ① 법 제24조제3항에 따른 고유식별정보의 안전성 확보 조치에 관하여는 제30조 또는 제48조의2를 준용한다. 이 경우 "법 제29조"는 "법 제24조제3항"으로, "개인정보"는 "고유식별정보"로 본다.

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

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

② 보호위원회는 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

■ 이 기준은 개인정보처리자에게 적용된다. 개인정보처리자는 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체, 사업자 및 개인 등을 말한다.

■ 개인정보처리자는 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치를 취하여야 한다.

- 가명정보 및 추가 정보를 처리하는 경우, 법 제28조의4 및 같은 법 시행령 제29조의5에 따라 가명정보 및 추가 정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하고 가명정보가 원래의 상태로 복원되지 않도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치를 취하여야 한다.

「개인정보 보호법」 제28조의4 제1항

제28조의4(가명정보에 대한 안전조치의무 등) ① 개인정보처리자는 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

■■■ 「개인정보 보호법 시행령」 제29조의5 제1항 ■■■

제29조의5(가명정보에 대한 안전성 확보 조치) ① 개인정보처리자는 법 제28조의4제1항에 따라 가명정보 및 가명정보를 원래의 상태로 복원하기 위한 추가 정보(이하 이 조에서 “추가 정보”라 한다)에 대하여 다음 각 호의 안전성 확보 조치를 해야 한다.

1. 제30조 또는 제48조의2에 따른 안전성 확보 조치
2. 가명정보와 추가 정보의 분리 보관. 다만, 추가 정보가 불필요한 경우에는 추가 정보를 파기해야 한다.
3. 가명정보와 추가 정보에 대한 접근 권한의 분리. 다만, 「소상공인 보호 및 지원에 관한 법률」 제2조에 따른 소상공인으로서 가명정보를 취급할 자를 추가로 둘 여력이 없는 경우 등 접근 권한의 분리가 어려운 정당한 사유가 있는 경우에는 업무 수행에 필요한 최소한의 접근 권한을 부여하고 접근 권한의 보유 현황을 기록으로 보관하는 등 접근 권한을 관리·통제하는 것을 말한다.

■ 이 기준은 개인정보의 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정한 것이므로 개인정보처리자는 처리하는 개인정보의 종류 및 중요도, 개인정보를 처리하는 방법 및 환경 등을 고려하여 필요하다면 이 기준에서 정한 것 이외에 추가적인 보호조치를 적용하여 개인정보의 안전성 확보조치를 강화하여야 한다.

■ 이 기준을 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자는 3천만원 이하의 과태료를 부과하며, 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

제2조 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. "대기업"이란 「독점규제 및 공정거래에 관한 법률」제14조에 따라 공정거래위원회가 지정한 기업집단을 말한다.
5. "중견기업"이란 「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」제2조에 해당하는 기업을 말한다.
6. "중소기업"이란 「중소기업기본법」제2조 및 동법 시행령 제3조에 해당하는 기업을 말한다.
7. "소상공인"이란 「소상공인 보호 및 지원에 관한 법률」제2조에 해당하는 자를 말한다.
8. "개인정보 보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.
9. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
10. "개인정보처리시스템"이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.
11. "위험도 분석"이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.

12. "비밀번호"란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

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

14. "공개된 무선망"이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

15. "모바일 기기"란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보처리에 이용되는 휴대용 기기를 말한다.

16. "바이오정보"란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.

17. "보조저장매체"란 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결.분리할 수 있는 저장매체를 말한다.

18. "내부망"이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

19. "접속기록"이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.

20. "관리용 단말기"란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

해 설

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

■ 정보주체란 「개인정보 보호법」에 의한 권리의 행사주체라고도 할 수 있다. 이 법의 보호를 받는 정보주체가 되기 위한 사항은 다음과 같다.

- 처리되는 정보에 의하여 알아볼 수 있는 사람
- 법인이나 단체가 아닌 살아있는 사람
- 처리되는 정보의 주체가 되는 자

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

■ 개인정보파일이란 개인의 이름이나 고유식별정보, ID 등을 색인(Index)이나 검색값으로 하여 쉽게 검색할 수 있도록 체계적으로 배열·구성한 집합물을 말한다.

- 개인정보파일은 일반적으로 전자적 형태로 구성된 데이터베이스(DB: DataBase)를 의미하는 경우가 많지만, 그 외에 체계적인 검색·열람을 위한 색인이 되어 있는 컴퓨터 문서 파일, 수기(手記) 문서 자료 등도 포함된다.

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

■ 개인정보처리자는 업무를 목적으로 개인정보를 처리하는 자이다. 순수한 개인적인 활동이나 가사활동을 위해서 개인정보를 수집·이용·제공하는 자는 개인정보처리자가 아니다.

■ 개인정보처리자는 개인정보파일을 운용하기 위하여 개인정보를 처리하는 자이다.

■ 개인정보처리자는 스스로 개인정보를 처리할 수도 있지만 다른 사람을 통해서 개인정보를 처리하는 경우에도 개인정보처리자에 해당한다.

■ 개인정보처리자는 공공기관, 법인, 단체, 개인이 모두 포함된다.

· 처리란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

4. "대기업"이란 「독점규제 및 공정거래에 관한 법률」제14조에 따라 공정거래위원회가 지정한 기업집단을 말한다.

■ 대기업이란 공정거래위원회가 지정한 상호출자제한기업집단 및 채무보증제한기업집단을 말한다.

「독점규제 및 공정거래에 관한 법률」 제14조

제14조(상호출자제한기업집단 등의 지정 등) ① 공정거래위원회는 대통령령으로 정하는 바에 따라 산정한 자산총액이 5조원 이상인 기업집단을 대통령령으로 정하는 바에 따라 공시대상기업집단으로 지정하고, 지정된 공시대상기업집단 중 일정규모 이상의 자산총액 등 대통령령으로 정하는 기준에 해당하는 기업집단을 대통령령으로 정하는 바에 따라 상호출자제한기업집단으로 지정한다. 이 경우 지정된 기업집단에 속하는 회사에 지정 사실을 대통령령으로 정하는 바에 따라 통지하여야 한다.

· 법제처에서 제공하는 국가법령정보센터(https://www.law.go.kr)에서 관련 법률을 검색할 수 있다.

5. "중견기업"이란「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」제2조에 해당하는 기업을 말한다.

■ 중견기업이란 다음의 요건을 모두 갖춘 기업을 말한다.

- 「중소기업기본법」 제2조에 따른 중소기업이 아닐 것

- 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관,「지방공기업법」에 따른 지방공기업 등 「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법 시행령」으로 정하는 기관이 아닐 것

- 그 밖에 지분 소유나 출자관계 등이 「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법 시행령」으로 정하는 기준에 적합한 기업

■■■ 「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」 제2조 ■■■

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1."중견기업"이란 다음 각 목의 요건을 모두 갖춘 기업을 말한다.

가.「중소기업기본법」 제2조에 따른 중소기업이 아닐 것

나.「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관,「지방공기업법」에 따른 지방공기업 등 대통령령으로 정하는 기관이 아닐 것

다. 그 밖에 지분 소유나 출자관계 등이 대통령령으로 정하는 기준에 적합한 기업

■■■ 「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법 시행령」 제2조 ■■■

제2조(중견기업 및 중견기업 후보기업의 범위) ① 「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」(이하 “법”이라 한다) 제2조제1호다목에서 "지분 소유나 출자관계 등이 대통령령으로 정하는 기준에 적합한 기업"이란 다음 각 호의 요건을 모두 갖춘 기업을 말한다.

1. 소유와 경영의 실질적인 독립성이 다음 각 목의 어느 하나에 해당하지 아니하는 기업일 것

가.「독점규제 및 공정거래에 관한 법률」 제14조제1항에 따른 상호출자제한기업집단에 속하는 기업

나.「독점규제 및 공정거래에 관한 법률 시행령」 제21조제2항에 따른 상호출자제한기업집단 지정기준인 자산총액 이상인 기업 또는 법인(외국법인을 포함한다. 이하 같다)이 해당 기업의 주식(「상법」 제344조의3에 따른 의결권 없는 주식은 제외한다) 또는 출자지분(이하 "주식등"이라 한다)의 100분의 30 이상을 직접적 또는 간접적으로 소유하면서 최다출자자인 기업. 이 경우 최다출자자는 해당 기업의 주식등을 소유한 법인 또는 개인으로서 단독으로 또는 다음의 어느 하나에 해당하는 자와 합산하여 해당 기업의 주식등을 가장 많이 소유한 자로 하며, 주식등의 간접소유비율에 관하여는 「국제조세조정에 관한 법률 시행령」 제2조제2항을 준용한다.

1) 주식등을 소유한 자가 법인인 경우: 그 법인의 임원

2) 주식등을 소유한 자가 개인인 경우: 그 개인의 친족

2. 「통계법」 제22조에 따라 통계청장이 고시하는 한국표준산업분류에 따른 다음 각 목의 어느 하나에 해당하는 업종을 영위하는 기업(「독점규제 및 공정거래에 관한 법률」 제8조의2제2항제5호에 따른 일반지주회사는 제외한다)이 아닐 것

가. 금융업

나. 보험 및 연금업

다. 금융 및 보험 관련 서비스업

3.「민법」 제32조에 따라 설립된 비영리법인이 아닐 것

6. "중소기업"이란 「중소기업기본법」제2조 및 동법 시행령 제3조에 해당하는 기업을 말한다.

■ 중소기업이란 다음 어느 하나에 해당하는 기업을 말한다.

- 업종별로 매출액 또는 자산총액 등이 「중소기업기본법 시행령」으로 정하는 기준에 맞을 것
- 지분 소유나 출자 관계 등 소유와 경영의 실질적인 독립성이 「중소기업기본법 시행령」으로 정하는 기준에 맞을 것
- 「사회적기업 육성법」제2조제1호에 따른 사회적기업 중에서 「중소기업기본법 시행령」으로 정하는 사회적기업
- 「협동조합 기본법」제2조에 따른 협동조합, 협동조합연합회, 사회적협동조합, 사회적협동조합연합회 중 「중소기업기본법 시행령」으로 정하는 자
- 「소비자생활협동조합법」 제2조에 따른 조합, 연합회, 전국연합회 중 「중소기업기본법 시행령」으로 정하는 자

「중소기업기본법」제2조

제2조(중소기업자의 범위) ①중소기업을 육성하기 위한 시책(이하 "중소기업시책"이라 한다)의 대상이 되는 중소기업자는 다음 각 호의 어느 하나에 해당하는 기업 또는 조합 등(이하 "중소기업"이라 한다)을 영위하는 자로 한다. 다만, 「독점규제 및 공정거래에 관한 법률」 제14조제1항에 따른 공시대상기업집단에 속하는 회사 또는 같은 법 제14조의3에 따라 공시대상기업집단의 소속회사로 편입·통지된 것으로 보는 회사는 제외한다.

1. 다음 각 목의 요건을 모두 갖추고 영리를 목적으로 사업을 하는 기업
   가. 업종별로 매출액 또는 자산총액 등이 대통령령으로 정하는 기준에 맞을 것
   나. 지분 소유나 출자 관계 등 소유와 경영의 실질적인 독립성이 대통령령으로 정하는 기준에 맞을 것
2. 「사회적기업 육성법」 제2조제1호에 따른 사회적기업 중에서 대통령령으로 정하는 사회적기업
3. 「협동조합 기본법」 제2조에 따른 협동조합, 협동조합연합회, 사회적협동조합, 사회적협동조합연합회 중 대통령령으로 정하는 자
4. 「소비자생활협동조합법」 제2조에 따른 조합, 연합회, 전국연합회 중 대통령령으로 정하는 자

② 중소기업은 대통령령으로 정하는 구분기준에 따라 소기업(小企業)과 중기업(中企業)으로 구분한다.

③ 제1항을 적용할 때 중소기업이 그 규모의 확대 등으로 중소기업에 해당하지 아니하게 된 경우 그 사유가 발생한 연도의 다음 연도부터 3년간은 중소기업으로 본다. 다만, 중

소기업 외의 기업과 합병하거나 그 밖에 대통령령으로 정하는 사유로 중소기업에 해당하지 아니하게 된 경우에는 그러하지 아니하다.

④ 중소기업시책별 특성에 따라 특히 필요하다고 인정하면 「중소기업협동조합법」이나 그 밖의 법률에서 정하는 바에 따라 중소기업협동조합이나 그 밖의 법인·단체 등을 중소기업자로 할 수 있다.

■■■ 「중소기업기본법 시행령」 제3조 ■■■

제3조(중소기업의 범위) ①「중소기업기본법」(이하 "법"이라 한다) 제2조제1항제1호에 따른 중소기업은 다음 각 호의 요건을 모두 갖춘 기업으로 한다.

1. 다음 각 목의 요건을 모두 갖춘 기업일 것
   가. 해당 기업이 영위하는 주된 업종과 해당 기업의 평균매출액 또는 연간매출액(이하 "평균매출액등"이라 한다)이 별표 1의 기준에 맞을 것
   나. 자산총액이 5천억원 미만일 것
2. 소유와 경영의 실질적인 독립성이 다음 각 목의 어느 하나에 해당하지 아니하는 기업일 것
   가. 삭제
   나. 자산총액이 5천억원 이상인 법인(외국법인을 포함하되, 비영리법인 및 제3조의2제3항 각 호의 어느 하나에 해당하는 자는 제외한다)이 주식등의 100분의 30 이상을 직접적 또는 간접적으로 소유한 경우로서 최다출자자인 기업. 이 경우 최다출자자는 해당 기업의 주식등을 소유한 법인 또는 개인으로서 단독으로 또는 다음의 어느 하나에 해당하는 자와 합산하여 해당 기업의 주식등을 가장 많이 소유한 자를 말하며, 주식등의 간접소유 비율에 관하여는 「국제조세조정에 관한 법률 시행령」 제2조제2항을 준용한다.
      1) 주식등을 소유한 자가 법인인 경우: 그 법인의 임원
      2) 주식등을 소유한 자가 1)에 해당하지 아니하는 개인인 경우: 그 개인의 친족
   다. 관계기업에 속하는 기업의 경우에는 제7조의4에 따라 산정한 평균매출액등이 별표 1의 기준에 맞지 아니하는 기업
   라. 삭제

② 법 제2조제1항제2호에서 "대통령령으로 정하는 사회적기업"이란 영리를 주된 목적으로 하지 아니하는 사회적기업으로서 다음 각 호의 요건을 모두 갖춘 기업으로 한다.

1. 제1항제1호 각 목의 요건을 모두 갖출 것
2. 삭제
3. 제1항제2호가목 또는 나목에 해당하지 아니할 것

③ 법 제2조제1항제3호에서 "대통령령으로 정하는 자"란 제2항 각 호의 요건을 모두 갖춘 협동조합, 협동조합연합회, 사회적협동조합 및 사회적협동조합연합회를 말한다.

④ 법 제2조제1항제4호에서 "대통령령으로 정하는 자"란 제2항 각 호의 요건을 모두 갖춘 조합, 연합회 및 전국연합회를 말한다.

7. "소상공인"이란 「소상공인 보호 및 지원에 관한 법률」제2조에 해당하는 자를 말한다.

■ 소상공인이란 다음의 요건을 모두 갖춘 자를 말한다.

- 상시 근로자 수가 10명 미만일 것
- 업종별 상시 근로자 수 등이 「소상공인 보호 및 지원에 관한 법률」 시행령으로 정하는 기준에 해당할 것

■■■ 「소상공인 보호 및 지원에 관한 법률」 제2조 ■■■

제2조(정의) 이 법에서 "소상공인"이란 「중소기업기본법」 제2조제2항에 따른 소기업(小企業) 중 다음 각 호의 요건을 모두 갖춘 자를 말한다.

1. 상시 근로자 수가 10명 미만일 것
2. 업종별 상시 근로자 수 등이 대통령령으로 정하는 기준에 해당할 것

■■■ 「소상공인 보호 및 지원에 관한 법률 시행령」 제2조 ■■■

제2조(소상공인의 범위 등) ① 「소상공인 보호 및 지원에 관한 법률」(이하 "법"이라 한다) 제2조제2호에서 "대통령령으로 정하는 기준"이란 다음 각 호의 구분에 따른 주된 사업에 종사하는 상시 근로자 수를 말한다.

1. 광업·제조업·건설업 및 운수업: 10명 미만
2. 그 밖의 업종: 5명 미만

8. "개인정보 보호책임자"란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.

■ 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정요건에 맞게 지정하고, 법률에 따라 업무를 수행하도록 보장하여야 한다.

· 개인정보 보호책임자의 지정 및 업무 수행에 관한 사항은 이 기준 제4조제1항 해설에서 보다 자세하게 확인할 수 있다.

9. "개인정보취급자"란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.

■ 개인정보취급자란 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 의미한다.

- 개인정보취급자는 개인정보 처리 업무를 담당하고 있는 자라면 정규직, 비정규직, 파견직, 시간제 등 모든 근로형태를 불문한다. 고용관계가 없더라도 실질적으로 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자는 개인정보취급자에 포함된다. (예시: 용역사 상주직원, 자동차·보험 판매 프리랜서 등)

10. "개인정보처리시스템"이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템을 말한다.

■ 개인정보처리시스템이란 일반적으로 데이터베이스(DB) 내의 데이터에 접근할 수 있도록 해주는 응용시스템을 의미하며, 데이터베이스를 구축하거나 운영하는데 필요한 시스템을 말한다.

- 다만, 개인정보처리시스템은 개인정보처리자의 개인정보 처리방법, 시스템 구성 및 운영환경 등에 따라 달라질 수 있다.

■ 업무용 컴퓨터의 경우에도 데이터베이스 응용프로그램이 설치·운영되어 다수의 개인정보취급자가 개인정보를 처리하는 경우에는 개인정보처리시스템에 해당될 수 있다.

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

11. "위험도 분석"이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.

■ 위험도 분석이란 개인정보 처리 시 다양한 위험요소를 사전에 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위하여 종합적으로 분석하는 행위를 의미한다.

- 개인정보 유출에 영향을 미칠 수 있는 위험요소는 내부자의 고의·과실 등 관리적인 측면과 개인정보처리시스템, 관리용 단말기 등의 악성코드 감염으로 인한 해킹 등 기술적인 측면 그리고 비인가자의 전산실 출입 등 물리적인 측면으로 나눌 수 있다.
- 위험요소 식별·평가 및 통제방안으로는 개인정보처리시스템 등 자산식별, 위협확인, 위험확인, 대책마련, 사후관리 등이 해당될 수 있다.

12. "비밀번호"란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

■ 비밀번호란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 계정정보(ID)와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

· 사용자 인증 및 비밀번호의 기능으로 생체인식, 보안카드, 일회용 비밀번호(One Time Password)가 사용되기도 한다.

■ 비밀번호는 알 수 있는 형태로 관리되어서는 아니 된다. 내부직원 또는 비인가자나 공격자 등에 의하여 고의 또는 악의적으로 개인정보처리시스템 등에 접속하여 개인정보를 유출하는 등 불법행위가 가능하기 때문이다.

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

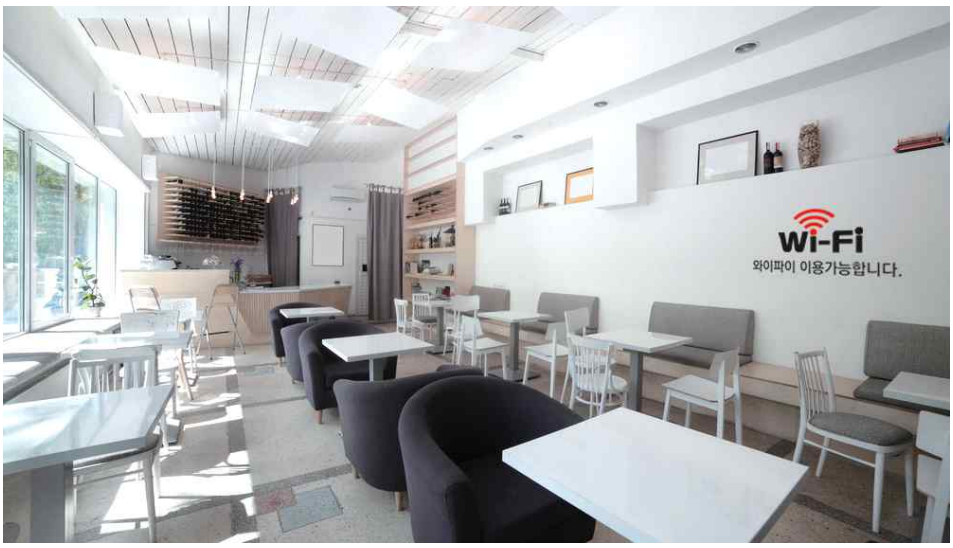
■ 정보통신망은 전기통신을 하기 위한 기계・기구・선로 기타 전기통신에 필요한 설비를 이용하거나 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집・가공・저장・검색・송신 또는 수신하는 정보통신체계를 의미한다.

14. "공개된 무선망"이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.

■ 공개된 무선망은 커피전문점, 도서관, 공항, 철도역, 버스터미널, 대학, 병원, 유통센터, 호텔 등에 설치될 수 있으며 개인정보처리자가 고객이나 방문객용으로 매장, 로비, 대합실, 회의실, 휴게실, 주차장 등의 장소에 설치한 무선접속장치도 이에 해당한다.

※ 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.

■■■ 공개된 무선망(커피전문점) 예시 ■■■



· 개인정보처리자가 직원의 업무처리 목적으로 사무실, 회의실 등에 무선접속장치(AP)를 설치하여 운영하는 경우 “공개된 무선망”에서 제외된다.

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

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

■ 모바일 기기는 이동통신망, 와이파이(Wi-Fi) 등의 무선망을 이용하여 개인정보 처리에 이용되는 휴대용 기기로서, 스마트폰, 태블릿PC, PDA(Personal Digital Assistant) 등이 있다.

■■■ 모바일 기기 예시 ■■■

PDA

스마트폰

태블릿PC

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

- 개인 소유의 휴대용기기라 할지라도 개인정보처리자의 업무 목적으로 개인정보 처리에 이용되는 경우 “모바일 기기”에 포함된다.

· 개인정보처리자의 “업무 목적”으로 “개인정보 처리”에 이용되지 않는 휴대용기기는 “모바일 기기”에서 제외된다.

16. "바이오정보"란 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 갖고 있어 개인을 식별하는 정보로 사용되며, 이러한 바이오정보는 신체적 특징과 행동적 특징을 기반으로 생성된 정보로 구분할 수 있다.

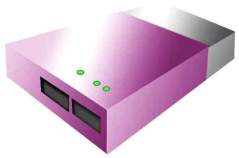
- 신체적 특징 : 지문, 얼굴, 홍채, 정맥, 음성, 망막, 손 모양, 손가락 모양, 열상 등
- 행동적 특징 : 필적, 키보드 타이핑, 입술 움직임, 걸음걸이 등

■ 또한, 바이오정보는 사람의 신체적 또는 행동적 특징을 입력장치를 통해 최초로 수집되어 가공되지 않은 '원본정보'와 그 중 특정 알고리즘을 통해 특징만을 추출하여 생성된 '특징정보'로 구분하기도 한다.

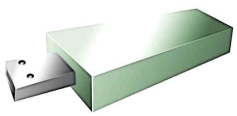
17. "보조저장매체"란 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결.분리할 수 있는 저장매체를 말한다.

■ 보조저장매체에는 이동형 하드디스크, USB메모리, CD, DVD 등이 해당된다. 경우에 따라서는 스마트폰도 보조저장매체가 될 수 있다.

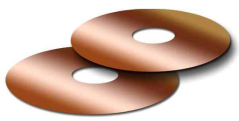
보조저장매체 예시



이동형 하드디스크



USB메모리

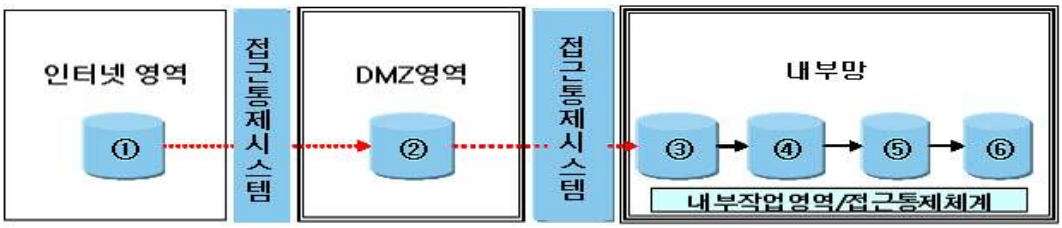


CD

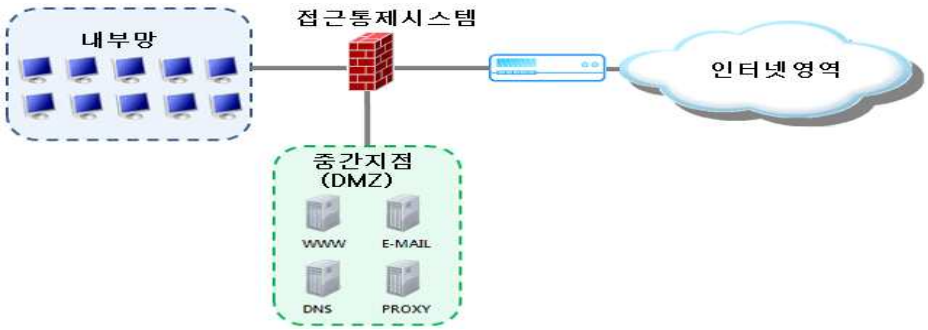
18. "내부망"이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.

■ 내부망이란 인터넷 구간과 물리적으로 망이 분리되어 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 ■■■



19. "접속기록"이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 "접속"이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.

■ 접속기록은 개인정보취급자 등이 개인정보처리시스템에 접속 및 운영 등에 관한 이력정보를 남기는 기록으로서, 접속에 관한 정보와 서비스 이용에 관한 정보 등을 개인정보처리시스템의 로그(Log) 파일 또는 로그관리시스템 등에 전자적으로 기록한 것을 말한다.

■ “개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무”는 개인정보취급자 등의 개인정보처리시스템에 접속한 사실과 접속하여 수행한 업무내역을 확인하는데 필요한 정보를 말한다.

- 계정 : 개인정보처리시스템에서 접속자를 식별할 수 있도록 부여된 ID 등 계정 정보
- 접속일시 : 접속한 시점 또는 업무를 수행한 시점(년-월-일, 시:분:초)
- 접속지 정보 : 개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소 등
- 처리한 정보주체 정보 : 개인정보취급자가 누구의 개인정보를 처리하였는지를 알 수 있는 식별정보(ID, 고객번호, 학번, 사번 등)
- 수행업무 : 개인정보취급자가 개인정보처리시스템을 이용하여 개인정보를 처리한 내용을 알 수 있는 정보(검색, 열람, 조회, 입력, 수정, 삭제, 출력, 다운로드 등)

· "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

20. "관리용 단말기"란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

■ 개인정보처리시스템을 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속할 수 있는 업무용 컴퓨터, 노트북 등이 관리용 단말기에 해당될 수 있다.

■ “직접 접속”이란 물리적 구조와 상관없이 단말기에서 개인정보처리시스템에 대하여 관리, 운영, 개발, 보안 등의 목적으로 활용할 수 있는 명령어 등을 직접 입력하여 처리할 수 있는 상태를 말한다.

제3조 안전조치 기준 적용

제3조(안전조치 기준 적용) 개인정보처리자가 개인정보의 안전성 확보에 필요한 조치를 하는 경우에는 [별표] 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준을 적용하여야 한다. 이 경우 개인정보처리자가 어느 유형에 해당하는지에 대한 입증책임은 당해 개인정보처리자가 부담한다.

해 설

■ 개인정보처리자는 [별표]에 따라 개인정보처리자 유형과 개인정보 보유량을 동시에 적용하여 개인정보처리자가 해당하는 유형의 안전조치 기준을 적용하여야 한다.

[별표] 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준

유형	적용 대상	안전조치 기준
유형1 (완화)	· 1만명 미만의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인	· 제5조 : 제2항부터 제5항까지 · 제6조 : 제1항, 제3항, 제6항 및 제7항 · 제7조 : 제1항부터 제5항까지, 제7항 · 제8조, 제9조, 제10조, 제11조, 제13조
유형2 (표준)	· 100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업 · 10만명 미만의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 · 1만명 이상의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인	· 제4조 : 제1항제1호부터 제11호까지 및 제15호, 제3항부터 제4항까지 · 제5조 · 제6조 : 제1항부터 제7항까지 · 제7조 : 제1항부터 제5항까지, 제7항 · 제8조, 제9조, 제10조, 제11조, 제13조
유형3 (강화)	· 10만명 이상의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 · 100만명 이상의 정보주체에 관한 개인정보를 보유한 중소기업, 단체	· 제4조부터 제13조까지

■■■ 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 적용 유형 ■■■

- 개인정보처리자 유형: 공공기관, 대기업, 중견기업, 중소기업, 소상공인, 개인, 단체
- 개인정보 보유량: 1만명 미만, 1만명~10만명 미만, 10만명~100만명 미만, 100만명 이상

<table>
<tr><th>구 분</th><th>1만명 미만</th><th>1만명~10만명 미만</th><th>10만명~100만명 미만</th><th>100만명 이상</th></tr>
<tr><td>공공기관</td><td colspan="2" rowspan="3">유형2(표준)</td><td colspan="2" rowspan="3">유형3(강화)</td></tr>
<tr><td>대기업</td></tr>
<tr><td>중견기업</td></tr>
<tr><td>중소기업</td><td colspan="3">유형2(표준)</td><td>유형3(강화)</td></tr>
<tr><td>소상공인</td><td rowspan="2">유형1(완화)</td><td colspan="3" rowspan="2">유형2(표준)</td></tr>
<tr><td>개인</td></tr>
<tr><td>단체</td><td>유형1(완화)</td><td colspan="2">유형2(표준)</td><td>유형3(강화)</td></tr>
</table>

※ 예시: 50만명의 개인정보를 보유한 대기업은 ‘유형3(강화)’에 해당하는 안전조치 기준 적용
※ 예시: 5만명의 개인정보를 보유한 중소기업은 ‘유형2(표준)’에 해당하는 안전조치 기준 적용
※ 예시: 5백명의 개인정보를 보유한 소상공인은 ‘유형1(완화)’에 해당하는 안전조치 기준 적용

■ 개인정보처리자는 개인정보 보유량의 변경·변동 가능여부에 대하여 정기적으로 확인하는 등 개인정보처리자 유형 또는 개인정보 보유량이 변동되는 경우에도 해당하는 유형의 안전조치 기준을 적용 하여야 한다. 이 경우 개인정보처리자가 어느 유형에 해당하는지에 대하여 입증할 수 있어야 한다.

제4조 내부 관리계획의 수립·시행

제4조(내부 관리계획의 수립·시행) 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.

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

② [별표]의 유형1에 해당하는 개인정보처리자는 제1항에 따른 내부 관리계획을 수립하지 아니할 수 있고, [별표]의 유형2에 해당하는 개인정보처리자는 제1항제12호부터 제14호까지를 내부 관리계획에 포함하지 아니할 수 있다.

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 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연 1회 이상으로 점검·관리 하여야 한다.

해 설

제4조(내부 관리계획의 수립·시행) 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.

■ 개인정보처리자는 개인정보를 처리함에 있어서 개인정보가 분실・도난・유출・위조・변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적・관리적 및 물리적 안전조치에 관한 내부 관리계획을 수립하고 시행하여야 한다.

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

■ 내부 관리계획은 전사적인 계획 내에서 개인정보가 관리될 수 있도록 최고경영층으로부터 내부결재 등의 승인을 받아 모든 임직원 및 관련자에게 알림으로써 이를 준수할 수 있도록 하여야 한다.

· 내부 관리계획의 문서 제목은 가급적 “내부 관리계획”이라는 용어를 사용하는 것이 바람직하나, 개인정보처리자의 내부 방침에 따라 다른 용어를 사용 할 수 있다.

- 다른 용어를 사용하는 경우에도 이 기준 제4조에 관한 사항을 이행하여야 한다.

■■■ 개인정보 내부 관리계획 목차 예시 ■■■

제1장 총칙
제1조(목적)
제2조(용어정의)
제3조(적용범위)

제2장 내부 관리계획의 수립 및 시행
제4조(내부 관리계획의 수립 및 승인)
제5조(내부 관리계획의 공표)

제3장 개인정보 보호책임자의 역할과 책임
제6조(개인정보 보호책임자의 지정)
제7조(개인정보 보호책임자의 역할 및 책임)
제8조(개인정보취급자의 역할 및 책임)

제4장 개인정보 보호 교육
제9조(개인정보 보호책임자의 교육)
제10조(개인정보취급자의 교육)

제5장 기술적 안전조치
제11조(접근권한의 관리)
제12조(접근통제)
제13조(개인정보의 암호화)
제14조(접속기록의 보관 및 점검)
제15조(악성프로그램 등 방지)

제6장 관리적 안전조치
제16조(개인정보 보호조직 구성 및 운영)
제17조(개인정보 유출사고 대응)
제18조(위험도 분석 및 대응)
제19조(수탁자에 대한 관리 및 감독)

제7장 물리적 안전조치
제20조(물리적 안전조치)
제21조(재해 및 재난 대비 안전조치)

제8장 그 밖에 개인정보 보호를 위하여 필요한 사항

1. 개인정보 보호책임자의 지정에 관한 사항

- 개인정보 보호책임자는 개인정보 처리에 관한 전반적인 사항을 결정하고 이로 인한 제반 결과에 대하여 책임을 지는 자이므로 개인정보보호 법·제도 및 기술 등에 대해 이해와 지식을 보유한 자로 지정하여야 한다.

- 개인정보 보호책임자는 개인정보 수집·이용·제공 등 처리에 대하여 실질적인 권한을 가지고 있어야 하며 조직 내에서 어느 정도 독자적인 의사결정을 할 수 있는 지위에 있는 자이어야 한다.

- 개인정보처리자가 개인정보 보호책임자를 지정하거나 변경하는 경우에는 개인정보처리 방침에 공개하여야 한다.

「개인정보 보호법」 제31조 제1항

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

「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. 공공기관: 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 장. 다만, 개인정보 처리 관련 업무를 담당하는 부서의 장이 2명 이상인 경우에는 해당 공공기관의 장이 지명하는 부서의 장이 된다.
2. 공공기관 외의 개인정보처리자: 다음 각 목의 어느 하나에 해당하는 사람
   가. 사업주 또는 대표자
   나. 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장)

2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항

■ 개인정보처리자는 개인정보 보호책임자가 형식적으로 외부에 보여주기 위한 장치가 아닌 개인정보처리자의 내부 관리체계를 강화하고 자율규제를 활성화하는 등 개인정보 보호책임자에게 실질적인 권한과 의무를 부여하여야 한다.

■■■ 「개인정보 보호법」 제31조 제2~5항 ■■■

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

③ 개인정보 보호책임자는 제2항 각 호의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.

④ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다.

⑤ 개인정보처리자는 개인정보 보호책임자가 제2항 각 호의 업무를 수행함에 있어서 정당한 이유 없이 불이익을 주거나 받게 하여서는 아니 된다.

■■■ 「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

3. 개인정보취급자에 대한 교육에 관한 사항

■ 개인정보처리자는 개인정보의 적정한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다.

■ 교육에 관한 사항에는 교육 목적, 교육 대상, 교육 내용(프로그램 등 포함), 교육 일정 및 방법 등을 포함하도록 한다. 내부 관리계획 등에 규정하거나 "○○년 개인정보보호 교육 계획(안)" 등과 같은 형태로 수립할 수 있다.

■ 교육 내용은 개인정보취급자의 지위·직책, 담당 업무의 내용, 업무 숙련도 등에 따라 각기 다르게 할 필요가 있다. 해당 업무를 수행하기 위한 분야별 전문기술 교육뿐만 아니라 개인정보보호 관련 법률 및 제도, 내부 관리계획 등 필히 알고 있어야 하는 사항을 포함하여 교육을 실시하도록 한다.

■■■ 개인정보 보호 교육내용 예시 ■■■

- 개인정보 보호의 중요성
- 내부 관리계획의 제·개정에 따른 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 보호업무의 절차, 책임, 방법
- 개인정보 처리 절차별 준수사항 및 금지사항
- 개인정보 유·노출 및 침해신고 등에 따른 사실 확인 및 보고, 피해구제 절차 등

■ 교육 방법에는 사내교육, 외부교육, 위탁교육 등 여러 종류가 있을 수 있으며, 조직의 여건 및 환경을 고려하여 집체 교육, 온라인 교육 등 다양한 방법을 활용할 수 있다.

· 보호위원회가 운영하는 개인정보보호 포털(https://www.privacy.go.kr)에서 제공하는 온라인 및 현장 교육 프로그램, 교육 교재 그리고 전문강사 등을 활용할 수 있다.

4. 접근 권한의 관리에 관한 사항

■ 개인정보처리시스템 등에 접근권한이 없는 자의 접근을 방지하기 위하여 이 기준 제5조(접근 권한의 관리)에 관한 사항을 포함하여야 한다.

- 개인정보취급자 등에게 업무수행에 필요한 최소한의 범위로 접근 권한의 부여, 변경 또는 말소에 대한 내역을 기록 및 최소 3년간 보관
- 개인정보취급자 등에 대한 비밀번호 작성규칙 수립 및 적용 등

5. 접근 통제에 관한 사항

■ 정보통신망을 통하여 개인정보처리시스템 등에 불법적인 접근을 차단하고 침해사고를 예방·방지하기 위하여 이 기준 제6조(접근 통제)에 관한 사항을 포함하여야 한다.

- 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 침입차단, 침입탐지 기능을 포함한 조치
- 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하는 경우 안전한 접속수단 또는 안전한 인증수단의 적용
- 개인정보 유·노출 방지를 위한 업무용 컴퓨터 등에 대한 안전조치
- 고유식별정보를 처리하는 인터넷 홈페이지에 대한 취약점 점검 및 개선조치 등

6. 개인정보의 암호화 조치에 관한 사항

■ 고유식별정보, 비밀번호 및 바이오정보가 개인정보처리시스템 등에 저장되거나 정보통신망을 통해 전송되는 경우, 노출 및 위·변조 등을 방지하기 위하여 이 기준 제7조(개인정보의 암호화)에 관한 사항을 포함하여야 한다.

- 고유식별정보, 비밀번호 및 바이오정보는 안전한 알고리즘으로 암호화 저장
- 고유식별정보, 비밀번호 및 바이오정보는 정보통신망을 통해 송신 시 암호화 등

7. 접속기록 보관 및 점검에 관한 사항

■ 개인정보취급자가 개인정보처리시스템에 접속한 정보 등을 확인할 수 있는 중요한 사항으로 이 기준 제8조(접속기록의 보관 및 점검)에 관한 사항을 포함하여야 한다.

- 개인정보취급자가 개인정보처리시스템에 접속한 기록의 보관기간
- 개인정보처리시스템의 접속기록 점검주기(월 1회 이상)
- 개인정보를 다운로드 하였을 경우 사유를 반드시 확인하여야 하는 기준과 사유 확인에 필요한 사항 등

※ 개인정보처리자의 업무 환경을 고려한 다운로드 기준(다운로드 정보주체의 수, 일정기간 내 다운로드 횟수 등)을 정하여 업무 목적 외의 불법행위 등으로 의심 가능한 다운로드에 대해 그 사유를 반드시 확인하여야 한다.

8. 악성프로그램 등 방지에 관한 사항

■ 업무용 컴퓨터 등에 악성프로그램 등의 설치로 인한 개인정보의 유출을 예방하기 위하여 이 기준 제9조(악성프로그램 등 방지)에 관한 사항을 포함하여야 한다.

- 백신소프트웨어 등의 보안 프로그램 설치·운영
- 보안 프로그램은 최신 상태로 유지하고 보안 업데이트 실시 등

9. 물리적 안전조치에 관한 사항

■ 개인정보가 보관되어 있는 물리적 장소나 서류·매체 등을 안전하게 관리하기 위하여 이 기준 제11조(물리적 접근 방지)에 관한 사항을 포함하여야 한다.

- 전산실 등 물리적 보관 장소를 두고 있는 경우에는 출입통제 절차 수립·운영
- 서류, 보조저장매체 등은 잠금장치가 있는 안전한 장소에 보관
- 보조저장매체의 반출·입 통제를 위한 보안대책 마련 등

10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항

■ 개인정보처리자는 개인정보 처리과정 전반에 걸쳐 개인정보를 안전하게 관리하고 보호하기 위하여 개인정보 보호조직을 구성하고 운영하여야 한다.

■ 개인정보 보호조직은 처리하는 개인정보의 종류·중요도 및 보유량, 개인정보를 처리하는 방법 및 환경 등을 고려하여 개인정보처리자 스스로 구성 및 운영하도록 한다.

■ 개인정보 보호조직은 인사명령, 업무분장, 내부 관리계획 등에 명시하도록 하며 인력의 지정에 관한 사항, 역할 및 책임 그리고 역량 및 요건 등 적정성에 관한 사항 등을 포함할 수 있다.

■■■ 개인정보 보호조직 구성도 예시 ■■■

- 개인정보 보호책임자 : 개인정보 처리에 관한 업무를 총괄해서 책임지는 자
- 개인정보 보호담당 : 개인정보 보호책임자의 지휘·감독 하에 개인정보 보호책임자의 업무를 지원하는 자
- 개인정보취급부서 : 개인정보를 처리하는 부서
- 개인정보취급자 : 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자

11. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항

■ 개인정보 유출사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위하여 긴급조치, 유출 신고 및 통지, 피해신고 접수 및 피해 구제 등과 같은 사항을 포함하는 개인정보 유출 사고 대응 계획을 수립·시행하여야 한다.

■■■ 개인정보 유출사고 대응 계획 예시 ■■■

- 개인정보 유출의 정의 및 사례·유형
- 개인정보 유출사고 예방을 위한 안전조치 및 상시 모니터링 수행
- 개인정보 유출사고 대응팀 구성·운영 및 비상연락망
- 개인정보 유출사고시 단계별 대응절차
  - 사고인지 및 긴급조치, 유출통지 및 신고, 피해신고 접수 및 피해구제, 사고 원인 분석 및 안전조치, 재발방지 대책 수립·운영 등

TIP

- "표준 개인정보 유출사고 대응 매뉴얼" 은 개인정보보호 포털(https://www.privacy.go.kr)에서 다운로드 할 수 있다.

12. 위험도 분석 및 대응방안 마련에 관한 사항

■ 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 사전에 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안을 마련하기 위해 종합적으로 분석하는 등 위험도 분석 및 대응방안에 관한 사항을 마련하여야 한다.

- "개인정보 위험도 분석 기준 및 해설서"에 따른 위험도 분석을 수행하고 대응방안을 마련하거나 개인정보처리자가 처리하는 개인정보의 종류 및 중요도, 개인정보를 처리하는 방법 및 환경 등에 따라 국제표준 및 전문기관 권고사항 등을 적용하는 등 개인정보처리자 스스로 이행할 수도 있다.

■■■ 위험도 분석 및 대응방안 예시 ■■■

- (자산식별) 개인정보, 개인정보처리시스템 등 보호대상을 명확하게 확인
- (위협확인) 자산에 손실 또는 해를 끼칠 수 있는 위협요소(취약점 등) 확인
- (위험확인) 위협으로 인하여 자산에 영향을 끼칠 수 있는 위험의 내용과 정도를 확인
- (대책마련) 위험에 대한 적절한 통제 방안 마련
- (사후관리) 위험대책을 적용하고 지속적으로 개선·관리를 위한 안전조치 사항

TIP

- "개인정보 위험도 분석 기준 및 해설서" 는 개인정보보호 포털(https://www.privacy.go.kr)에서 다운로드 할 수 있다.

13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항

■ 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 보호를 통하여 개인정보의 손실, 훼손 등을 방지하기 위하여 이 기준 제12조(재해·재난 대비 안전조치)에 관한 사항을 포함하여야 한다.

- 개인정보처리시스템 보호를 위한 대응절차 마련 및 점검
- 개인정보처리시스템 백업 및 복구를 위한 계획 마련 등

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

■ 개인정보처리자는 개인정보 처리업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

「개인정보 보호법」 제26조

제26조(업무위탁에 따른 개인정보의 처리 제한) ④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

■ 개인정보처리자는 수탁자에 대하여 정기적으로 교육을 실시하고, 수탁자의 개인정보처리 현황 및 실태, 목적 외 이용·제공, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 점검 등 관리·감독하여야 한다.

■ 내부 관리계획에는 수탁자에 대한 교육 및 감독의 시기와 방법, 절차, 점검 항목 등을 포함해야 하며, 이외 수탁자 교육 및 감독에 대한 기록을 남기고 문제점이 발견된 경우 그에 따른 개선 조치를 하여야 한다.

15. 그 밖에 개인정보 보호를 위하여 필요한 사항

■ 개인정보처리자는 처리하는 개인정보의 종류 및 중요도, 보유량 그리고 개인정보를 처리하는 방법 및 환경 등을 고려하여 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전조치를 취하기 위한 사항을 추가적으로 포함하도록 한다.

- 예를 들어, 인증제도·인증마크의 도입, 소프트웨어 보안취약점 점검 및 모의해킹, 내·외부 관리실태 점검 및 평가 등에 관한 사항이 이에 해당될 수 있다.

② [별표]의 유형1에 해당하는 개인정보처리자는 제1항에 따른 내부 관리계획을 수립하지 아니할 수 있고, [별표]의 유형2에 해당하는 개인정보처리자는 제1항제12호부터 제14호까지를 내부 관리계획에 포함하지 아니할 수 있다.

■■■ 안전조치 기준에 따른 적용 유형 ■■■

제4조(내부 관리계획의 수립 · 시행)		유형1 (완화)	유형2 (표준)	유형3 (강화)
항	호			
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.	1. 개인정보 보호책임자의 지정에 관한 사항		○	○
	2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항		○	○
	3. 개인정보취급자에 대한 교육에 관한 사항		○	○
	4. 접근 권한의 관리에 관한 사항		○	○
	5. 접근 통제에 관한 사항		○	○
	6. 개인정보의 암호화 조치에 관한 사항		○	○
	7. 접속기록 보관 및 점검에 관한 사항		○	○
	8. 악성프로그램 등 방지에 관한 사항		○	○
	9. 물리적 안전조치에 관한 사항		○	○
	10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항		○	○
	11.개인정보 유출사고 대응 계획 수립·시행에 관한 사항		○	○
	12. 위험도 분석 및 대응방안 마련에 관한 사항			○
	13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항			○
	14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항			○
	15. 그 밖에 개인정보 보호를 위하여 필요한 사항		○	○
② [별표]의 유형1에 해당하는 개인정보처리자는 제1항에 따른 내부 관리계획을 수립하지 아니할 수 있고, [별표]의 유형2에 해당하는 개인정보처리자는 제1항제12호부터 제14호까지를 내부 관리계획에 포함하지 아니할 수 있다.				
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 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리 하여야 한다.			○	○

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

■ 개인정보처리자는 개인정보 처리 방법, 처리 환경 및 안전조치 사항 등 내부 관리계획에 중요한 변경이 있는 경우에는 변경사항을 즉시 반영하여 내부 관리계획을 수정·변경하여 시행하여야 한다.

■ 내부 관리계획의 수정·변경 시에도 내부 의사결정 절차를 통하여 내부 관리계획을 수정하여 시행하여야 한다.

■ 내부 관리계획을 수정·변경하는 경우에는 그 내용, 수정 및 시행 시기 등 이력을 관리하여야 한다.

■ 또한, 내부 관리계획의 수정·변경 사항을 개인정보취급자 등에게 전파하여 이를 준수할 수 있도록 한다.

④ 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연 1회 이상으로 점검·관리 하여야 한다.

■ 개인정보 보호책임자는 내부 관리계획의 적정성과 실효성을 보장하기 위하여 연 1회 이상 내부 관리계획에 따른 기술적·관리적 및 물리적 안전조치의 이행 여부를 점검·관리하여야 한다.

■ 내부 관리계획의 이행 실태 점검·관리 결과에 따라 적절한 조치를 취하여야 하며, 중대한 영향을 초래하거나 해를 끼칠 수 있는 사안 등에 대해서는 사업주·대표·임원 등에게 보고 후, 의사결정 절차를 통하여 적절한 대책을 마련하여야 한다.

제5조 접근 권한의 관리

제5조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 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 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.

⑥ 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

⑦ [별표]의 유형1에 해당하는 개인정보처리자는 제1항 및 제6항을 아니할 수 있다.

해 설

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

■ 개인정보처리자는 개인정보의 분실・도난・유출・변조 또는 훼손을 방지하기 위하여 개인정보처리시스템에 대한 접근권한을 업무 수행 목적에 따라 필요한 최소한의 범위로 업무 담당자에게 차등 부여하고 접근통제를 위한 안전조치를 취해야 한다.

■ 개인정보처리자가 가명정보를 처리하는 경우, 가명정보에 접근권한이 있는 담당자가 특정 개인을 알아보기 위한 목적으로 가명정보를 처리하는 것을 방지하기 위하여 가명정보에 접근할 수 있는 담당자와 추가 정보에 접근할 수 있는 담당자를 반드시 구분하여야 한다.

- 이 경우, 가명정보에 접근권한이 있는 담당자가 특정 개인을 식별할 수 있는 정보에 접근할 수 없도록 제한하여야 한다.
- 가명정보와 추가 정보에 대한 접근 권한의 분리가 어려운 정당한 사유가 있는 경우(소상공인으로서 가명정보를 취급할 자를 추가로 둘 여력이 없는 경우 등), 업무 수행에 필요한 최소한 접근 권한 부여 및 접근 권한의 보유 현황을 기록으로 보관하는 등 접근권한을 관리 및 통제하여야 한다.

■ 특히, 개인정보처리시스템의 데이터베이스(DB)에 대한 직접적인 접근은 데이터베이스 운영・관리자에 한정하는 등의 안전조치를 적용할 필요성이 있다.

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

■ 조직 내의 임직원 전보 또는 퇴직, 휴직 등 인사이동이 발생하여 사용자계정의 변경・말소 등이 필요한 경우에는 사용자계정 관리절차에 따라 통제하여 인가되지 않는 자의 접근을 차단하여야 한다.

■ 예를 들어, 직원의 퇴직 시 해당 직원의 계정을 지체없이 변경・말소하는 조치 등을 내부 관리계획 등에 반영하여 이행하도록 한다. 또한, 직원의 퇴직 시 계정 말소를 효과적으로 이행하기 위해서는 퇴직 점검표에 사용자계정의 말소 항목을 반영하여, 계정 말소 여부에 대해 확인을 받을 수도 있다.

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

■ 개인정보처리자는 접근권한 부여, 변경, 말소에 대한 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 3년간 보관하여야 한다.

■ 예를 들어, 신청자 정보, 신청일시, 승인자 및 발급자 정보, 신청 및 발급 사유 등 발급 과정과 이력 등을 확인할 수 있도록 필요한 정보를 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.

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

■ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템, 접근통제시스템, 인터넷 홈페이지 등에 적용하여야 한다.

■ 비밀번호는 정당한 접속 권한을 가지지 않는 자가 추측하거나 접속을 시도하기 어렵도록 문자, 숫자 등으로 조합·구성하여야 한다.

※ 비밀번호 이외의 추가적인 인증에 사용되는 휴대폰 인증, 일회용 비밀번호(OTP) 등은 비밀번호 작성규칙을 적용하지 아니할 수 있다.

■ 특히, 개인정보처리시스템의 데이터베이스(DB)에 접속하는 DB관리자의 비밀번호는 복잡하게 구성하고 변경 주기를 짧게 하는 등 강화된 안전조치를 적용할 필요가 있다.

· 안전한 비밀번호 설정을 위해 한국인터넷진흥원(KISA)의 암호이용활성화 홈페이지(https://seed.kisa.or.kr)에서 제공하는 "패스워드 선택 및 이용 안내서"나 비밀번호 안전성 검증 소프트웨어 등을 활용할 수 있다.

■■■ 비밀번호 작성규칙 예시 ■■■

- 비밀번호는 문자, 숫자의 조합·구성에 따라 최소 8자리 또는 10자리 이상의 길이로 구성
  - 최소 8자리 이상 : **두 종류 이상의 문자**를 이용하여 구성한 경우
    ※ 문자 종류 : 알파벳 대문자와 소문자, 특수문자, 숫자
  - 최소 10자리 이상 : **하나의 문자종류**로 구성한 경우
    ※ 단, 숫자로만 구성할 경우 취약할 수 있음
- 비밀번호는 추측하거나 유추하기 어렵도록 설정
  - 동일한 문자 반복(aaabbb, 123123 등), 키보드 상에서 나란히 있는 문자열(qwer 등), 일련번호(12345678 등), 가족이름, 생일, 전화번호 등은 사용하지 않는다.
- 비밀번호가 제3자에게 노출되었을 경우 지체 없이 새로운 비밀번호로 변경해야 함

⑥ 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

■ 개인정보처리자는 개인정보처리시스템에 권한 없는 자의 비정상적인 접근을 방지하기 위하여 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우에는 개인정보처리시스템에 접근을 제한하는 등 기술적 조치를 하여야 한다.

- 계정정보 또는 비밀번호를 일정 횟수(예: 5회) 이상 잘못 입력한 경우 사용자계정 잠금 등의 조치를 취하거나 계정정보·비밀번호 입력과 동시에 추가적인 인증수단(인증서, OTP 등)을 적용하여 정당한 접근 권한 자임을 확인하는 등의 조치를 취하는 것을 말한다.

※ 개인정보취급자에게 개인정보처리시스템에 대한 접근을 재 부여하는 경우에도 반드시 개인정보취급자 여부를 확인 후 계정 잠금 해제 등의 조치가 필요하다.

· 일반적인 비밀번호 공격방법은 사전공격과 무작위 대입공격이 있다.
- 사전공격(Dictionary Attack) : 자주 사용되는 단어를 비밀번호에 대입하는 공격 방법
- 무작위 대입공격(Brute Force) : 가능한 한 모든 값을 비밀번호에 대입해 보는 공격 방법

⑦ [별표]의 유형1에 해당하는 개인정보처리자는 제1항 및 제6항을 아니할 수 있다.

■■■ 안전조치 기준에 따른 적용 유형 ■■■

제5조(접근 권한의 관리)	유형1 (완화)	유형2 (표준)	유형3 (강화)
① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.		○	○
② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 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 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.	○	○	○
⑥ 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.		○	○
⑦ [별표]의 유형1에 해당하는 개인정보처리자는 제1항 및 제6항을 아니할 수 있다.			

제6조 접근통제

제6조(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 시도 탐지 및 대응

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

③ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.

④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.

⑤ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 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 접근 통제 기능을 이용할 수 있다.

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

⑧ [별표]의 유형1에 해당하는 개인정보처리자는 제2항, 제4항부터 제5항까지의 조치를 아니할 수 있다.

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 시도 탐지 및 대응

■ 개인정보처리자는 개인정보처리시스템에서 정보통신망을 통한 불법적인 접근 및 침해사고를 방지하기 위해 아래의 기능을 포함한 안전조치를 하여야 한다.

- 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소, 포트(Port), MAC(Media Access Control) 주소 등으로 제한하여 인가받지 않은 접근을 제한하도록 한다.(침입차단 기능)
- 개인정보처리시스템에 접속한 IP(Internet Protocol)주소, 포트(Port), MAC(Media Access Control) 주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지(침입탐지 기능)하고 접근 제한·차단 등 적절한 대응 조치를 하여야 한다.

■ 불법적인 접근 및 침해사고 방지를 위해서는 침입차단 및 침입탐지 기능을 갖는 장비 설치와 더불어 침입차단 및 침입탐지 정책 설정, 개인정보처리시스템에 접속한 이상행위 대응, 로그 훼손 방지 등 적절한 운영·관리가 필요하다.

■■■ 침입차단 및 침입탐지 기능을 갖춘 장비의 설치 방법 예시 ■■■

- 침입차단시스템, 침입탐지시스템, 침입방지시스템 등 설치·운영
- 웹방화벽, 보안 운영체제(Secure OS) 등 도입
- 스위치 등의 네트워크 장비에서 제공하는 ACL(Access Control List : 접근제어목록) 등 기능을 이용하여 IP 주소 등을 제한함으로써 침입차단 기능을 구현
- 공개용 소프트웨어를 사용하거나, 운영체제(OS)에서 제공하는 기능을 활용하여 해당 기능을 포함한 시스템을 설치·운영
  - 다만, 공개용 소프트웨어를 사용하는 경우에는 적절한 보안이 이루어지는지를 사전에 점검하고 정기적인 업데이트 여부 등 확인 후 적용 필요
- 이외에도, 인터넷데이터센터(IDC), 클라우드 서비스, 보안업체 등에서 제공하는 보안서비스 등도 활용 가능

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

■ 인터넷구간 등 외부로부터 개인정보처리시스템에 대한 접속은 원칙적으로 차단하여야 하나, 개인정보처리자의 업무 특성 또는 필요에 의해 개인정보취급자가 노트북, 업무용 컴퓨터, 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속이 필요한 경우에는 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

- 접속수단 예시: 가상사설망(VPN : Virtual Private Network) 또는 전용선 등

※ 가상사설망(VPN : Virtual Private Network) : 개인정보취급자가 사업장 내의 개인정보처리시스템에 대해 원격으로 접속할 때 IPsec이나 SSL 기반의 암호 프로토콜을 사용한 터널링 기술을 통해 안전한 암호통신을 할 수 있도록 해주는 보안 시스템을 의미

※ 전용선 : 물리적으로 독립된 회선으로서 두 지점간에 독점적으로 사용하는 회선으로 개인정보처리자와 개인정보취급자, 또는 본점과 지점간 직통으로 연결하는 회선 등을 의미

■■■ 가상사설망 및 전용선 구성 예시 ■■■

TIP

· IPsec(IP Security Protocol)은 인터넷 프로토콜(IP) 통신 보안을 위해 패킷에 암호화 기술이 적용된 프로토콜 집합

· SSL(Secure Socket Layer)은 웹 브라우저(클라이언트)와 웹 서버(서버)간에 데이터를 안전하게 주고받기 위해 암호화 기술이 적용된 보안 프로토콜

- IPsec, SSL 등의 기술이 사용된 가상사설망을 안전하게 사용하기 위해서는, 잘 알려진 취약점(예시: Open SSL의 HeartBleed 취약점)들을 조치하고 사용 할 필요가 있다.

- 인증수단 예시: 인증서(PKI), 보안토큰, 일회용 비밀번호(OTP) 등

※ 인증서(PKI, Public Key Infrastructure) : 전자상거래 등에서 상대방과의 신원확인, 거래사실 증명, 문서의 위·변조 여부 검증 등을 위해 사용하는 전자서명으로서 해당 전자서명을 생성한 자의 신원을 확인하는 수단

※ 보안토큰 : 암호 연산장치 등으로 내부에 저장된 정보가 외부로 복사, 재생성되지 않도록 공인인증서 등을 안전하게 보호할 수 있는 수단으로 스마트 카드, USB 토큰 등이 해당

※ 일회용 비밀번호(OTP, One Time Password) : 무작위로 생성되는 난수를 일회용 비밀번호로 한 번 생성하고, 그 인증값이 한 번만 사용가능하도록 하는 방식

· 인증수단만을 적용하는 경우에는 통신 보안을 위한 암호화 기술의 추가 적용이 필요할 수 있으므로, 보안성 강화를 위하여 안전한 접속수단을 권고한다.

③ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.

■ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지 등을 통해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 안전조치를 하여야 한다.

- 인터넷 홈페이지 중 서비스 제공에 사용되지 않거나 관리되지 않는 사이트 또는 URL(Uniform Resource Locator)에 대한 삭제 또는 차단 조치를 한다.

- 인터넷 홈페이지의 설계·개발 오류 또는 개인정보취급자의 업무상 부주의 등으로 인터넷 서비스 검색엔진(구글링 등) 등을 통해 관리자 페이지와 취급중인 개인정보가 노출되지 않도록 필요한 조치를 한다.

■ 인터넷 홈페이지를 통하여 개인정보가 유출될 수 있는 위험성을 줄이기 위하여 정기적으로 웹 취약점 점검을 권고한다.

■ 개인정보처리자는 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 P2P, 공유설정은 기본적으로 사용하지 않는 것이 원칙이나, 업무상 반드시 필요한 경우에는 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 안전조치를 하여야 한다.

- 업무상 꼭 필요한 경우라도 드라이브 전체 또는 불필요한 폴더가 공유되지 않도록 조치하고, 공유폴더에 개인정보 파일이 포함되지 않도록 정기적으로 점검이 필요하다.

- 이외에도 상용 웹메일, 웹하드, 메신저, SNS 서비스 등을 통하여 고의 혹은 부주의로 인한 개인정보 유·노출 방지 조치 등이 해당될 수 있다.

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

■ 개인정보처리자는 공개된 무선망을 이용하여 개인정보를 처리하는 경우 취급중인 개인정보가 신뢰되지 않은 무선접속장치(AP), 무선 전송 구간 및 무선접속장치의 취약점 등에 의해 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 안전조치를 하여야 하며, 다음과 같은 방식들을 활용 할 수 있다.

- 비밀번호 등 송신 시 SSL, VPN 등의 보안기술이 적용된 전용 프로그램을 사용하거나 암호화하여 송신한다.

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

- 고유식별정보 등이 포함된 파일 송신 시 파일을 암호화하여 저장 후 송신한다.

※ 예시: 모바일 기기, 노트북에서 개인정보처리시스템에 고유식별정보가 포함된 파일 송신 시, 암호화 저장한 후 송신

- 개인정보 유출 방지 조치가 적용된 공개된 무선망을 이용한다.

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

④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.

■ 인터넷 홈페이지를 통해 고유식별정보(주민등록번호, 운전면허번호, 외국인등록번호, 여권번호)를 처리하는 개인정보처리자는 고유식별정보가 유출·변조·훼손되지 않도록 해당 인터넷 홈페이지에 대해 연 1회 이상 취약점을 점검하여야 하며, 그 결과에 따른 개선 조치를 하여야 한다.

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

· 잘 알려진 웹 취약점 점검 항목은 행정안전부, 국가사이버안전센터(NCSC), 한국인터넷진흥원(KrCERT), OWASP(오픈소스웹보안프로젝트) 등에서 발표하는 항목 참조

· 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.

■ 인터넷 홈페이지의 취약점 점검 시에는 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.

· 취약점 점검 및 조치에 활용할 수 있는 기술문서는 아래와 같이 다양한 자료가 있다.
- 공개SW를 활용한 소프트웨어 개발보안 진단 가이드(행정안전부, 2019.6.)
- 소프트웨어 보안약점 진단가이드(행정안전부, 2019.6.)
- 소프트웨어 개발보안 가이드(행정안전부, 2019.11.)
- 시큐어코딩가이드(C, Java)(행정안전부, 2012.9.) 등

■ 기술과 서비스 발전에 따라 시스템 등에 대한 신규 취약점은 계속적으로 발생하고 있으며, 정기적인 취약점 점검 및 개선조치를 통하여 개인정보 유출을 예방하는 등 적극적인 보호활동을 권장한다.

⑤ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.

■ 개인정보처리시스템에 접속하는 업무용 컴퓨터 등에서 해당 개인정보처리시스템에 대한 접속의 차단을 의미하며, 업무용 컴퓨터의 화면보호기 등은 접속차단에 해당하지 않는다.

■ 개인정보취급자가 일정시간 이상 업무처리를 하지 않아 개인정보처리시스템에 접속이 차단된 이후, 다시 접속하고자 할 때에도 최초의 로그인과 동일한 방법으로 접속하여야 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 접근 통제 기능을 이용할 수 있다.

■ PC, 노트북 등의 업무용 컴퓨터의 운영체제(OS)에서 제공하는 접근 통제 기능 설정 방법은 아래와 같으며, 별도의 보안프로그램을 사용하여 접근 통제 기능을 설정하고 이용 할 수 있다.

■■■ 업무용 컴퓨터(윈도우의 경우) 방화벽 설정 방법 ■■■

・업무용 컴퓨터 : 제어판 >> Windows 방화벽 >> Windows 방화벽 설정 또는 해제

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

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

- 모바일 기기에서는 네트워크 및 소프트웨어 통제, 인입 포트 차단 등의 접근 통제 기능을 제공하는 운영체제를 사용할 수 있으며, 접근 통제 기능을 제공하는 방화벽 등 어플리케이션(App)을 설치・운영을 할 수 있다.

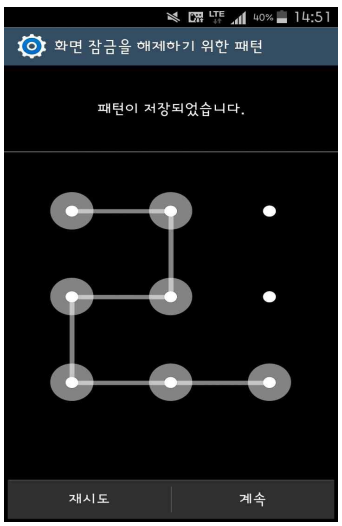
⑦ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

■ 업무용 모바일 기기는 성능 및 처리 속도가 향상되어 대량의 개인정보 처리에 활용되고 있으나, 이동성·휴대성 등으로 인하여 기기가 분실·도난 되는 경우에는 해당 기기를 통하여 개인정보처리시스템에 접속하지 못하도록 조치하거나 기기에 저장된 개인정보가 유출되지 않도록 비밀번호 설정 등의 안전조치를 하여야 한다.

- 비밀번호, 패턴, PIN, 지문, 홍채 등을 사용하여 화면 잠금 설정

화면 잠금 설정 예시

비밀번호



패턴입력

- 디바이스 암호화 기능을 사용하여 애플리케이션, 데이터 등 암호화
- USIM 카드에 저장된 개인정보 보호를 위한 USIM 카드 잠금 설정
- 모바일 기기 제조사 및 이동통신사가 제공하는 기능을 이용한 원격 잠금, 원격 데이터 삭제
- 중요한 개인정보를 처리하는 모바일 기기는 MDM(Mobile Device Management) 등 모바일 단말 관리 프로그램을 설치하여 원격 잠금, 원격 데이터 삭제, 접속 통제 등

※ MDM은 무선망을 이용해 원격으로 스마트폰 등의 모바일 기기를 제어하는 솔루션으로서, 분실된 모바일 기기의 위치 추적, 잠금 설정, 정보 삭제, 특정 사이트 접속 제한 등의 기능 제공

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.

⑧ [별표]의 유형1에 해당하는 개인정보처리자는 제2항, 제4항부터 제5항까지의 조치를 아니할 수 있다.

■■■ 안전조치 기준에 따른 적용 유형 ■■■

제6조(접근 통제)		유형1 (완화)	유형2 (표준)	유형3 (강화)
항	호			
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 시도 탐지 및 대응	○	○	○
② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.			○	○
③ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.		○	○	○
④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.			○	○
⑤ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 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 접근 통제 기능을 이용할 수 있다.		○	○	○
⑦ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.		○	○	○
⑧ [별표]의 유형1에 해당하는 개인정보처리자는 제2항, 제4항부터 제5항까지의 조치를 아니할 수 있다.				

제7조 개인정보의 암호화

제7조(개인정보의 암호화) ① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 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. 암호화 미적용시 위험도 분석에 따른 결과

⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

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

⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.

해설

① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

■ 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

- 고유식별정보는 개인을 고유하게 구별하기 위하여 부여된 식별정보를 말하며 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호를 말한다.
- 비밀번호란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
- 바이오정보란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
- 정보통신망이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.

TIP

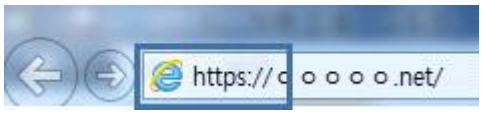
· 개인정보처리자는 자신이 제공하는 인터넷 홈페이지에서 이용자가 입력하는 고유식별정보, 비밀번호, 바이오정보를 암호화하여 송신하거나 전달하여야 한다.

■ 정보통신망을 통하여 비밀번호를 송신하는 경우에는 SSL 등의 통신 암호 프로토콜이 탑재된 기술을 활용하여야 한다.

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

■■■ SSL 적용 예시 ■■■

일반 웹주소



SSL 적용 웹주소

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

■ 보조저장매체를 통해 고유식별정보, 비밀번호, 바이오정보를 전달하는 경우에도 암호화 하여야 하며, 이를 위해 다음과 같은 방법 등이 사용 될 수 있다.

- 암호화 기능을 제공하는 보안 USB 등의 보조저장매체에 저장하여 전달
- 해당 개인정보를 암호화 저장 한 후 보조저장매체에 저장하여 전달

■ 고유식별정보, 비밀번호, 바이오정보를 제외한 개인정보(성명, 연락처 등)는 암호화 조치가 필수는 아니나, 개인정보의 위·변조 및 유·노출 등을 고려하여 가급적 암호화 조치를 권장한다.

② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

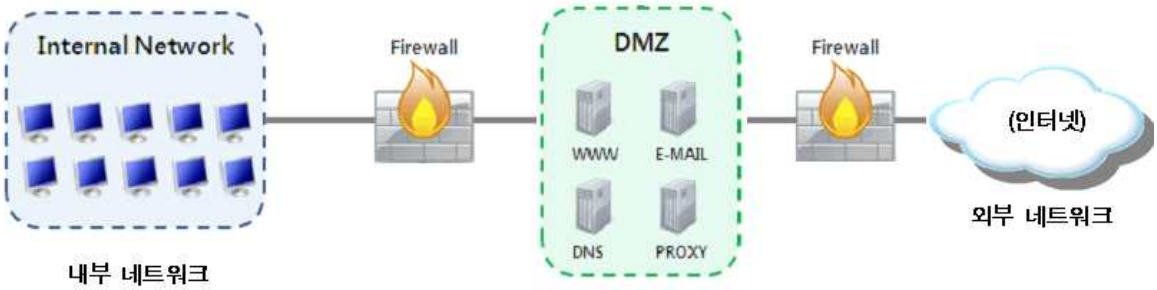
■ 개인정보처리자는 비밀번호, 바이오정보를 DB 또는 파일 등으로 저장하는 경우에는 노출 또는 위·변조되지 않도록 암호화하여 저장하여야 한다.

- 비밀번호의 경우에는 복호화 되지 않도록 일방향(해쉬 함수) 암호화 하여야 한다. 일방향 암호화는 저장된 값으로 원본 값을 유추하거나 복호화 할 수 없도록 한 암호화 방법으로서, 인증검사 시에는 사용자가 입력한 비밀번호를 일방향 함수에 적용하여 얻은 결과 값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 확인한다.
- 바이오정보를 식별 및 인증 등의 업무에 활용하기 위하여 수집·이용하는 경우에는 암호화 조치를 하여야 하며 복호화가 가능한 양방향 암호화 저장을 할 수 있다.

③ 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 구간을 의미하고, DMZ 구간은 인터넷과 내부망 사이에 위치한 중간 지점 또는 인터넷 구간 사이에 위치한 중간 지점으로서 인터넷 구간에서 직접 접근이 가능한 영역을 말한다.(침입차단시스템 등으로 접근 제한 등을 수행하는 경우에도 해당) 또한, 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.

④ 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. 암호화 미적용시 위험도 분석에 따른 결과

■ 내부망에 주민등록번호를 저장하는 경우, 법 제24조의2, 같은 법 시행령 제21조의2에 따라 "개인정보 영향평가"나 암호화 미적용시 "위험도 분석"의 결과에 관계없이 암호화 하여야 한다.

「개인정보 보호법」 제24조의2 제2항

제24조의2(주민등록번호 처리의 제한) ② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.

「개인정보 보호법 시행령」 제21조의2

제21조의2(주민등록번호 암호화 적용 대상 등) ① 법 제24조의2제2항에 따라 암호화 조치를 하여야 하는 암호화 적용 대상은 주민등록번호를 전자적인 방법으로 보관하는 개인정보처리자로 한다.

② 제1항의 개인정보처리자에 대한 암호화 적용 시기는 다음 각 호와 같다.

1. 100만명 미만의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2017년 1월 1일
2. 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자: 2018년 1월 1일

③ 보호위원회는 기술적·경제적 타당성 등을 고려하여 제1항에 따른 암호화 조치의 세부적인 사항을 정하여 고시할 수 있다.

■ 내부망에 주민등록번호를 제외한 고유식별정보를 저장하는 경우에는 다음에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

- 「개인정보 보호법」 제33조 및 시행령 제35조에 따라 영향평가의 대상이 되는 개인정보 파일을 운용하는 공공기관은 해당 "개인정보 영향평가"의 결과

「개인정보 보호법」 제33조 제1항

제33조(개인정보 영향평가) ① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보 파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 "영향평가"라 한다)를 하고 그 결과를 보호위원회에 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 보호위원회가 지정하는 기관(이하 "평가기관"이라 한다) 중에서 의뢰하여야 한다.

「개인정보 보호법 시행령」 제35조

제35조(개인정보 영향평가의 대상) 법 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다.

1. 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 법 제23조에 따른 민감정보(이하 "민감정보"라 한다) 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
4. 법 제33조제1항에 따른 개인정보 영향평가(이하 "영향평가"라 한다)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.

- 공공기관 이외의 개인정보처리자는 암호화 미적용시 "위험도 분석"에 따른 결과

· "개인정보 영향평가 수행 안내서" 및 "개인정보 위험도 분석 기준 및 해설서"는 개인정보보호 포털(https://www.privacy.go.kr)에서 다운로드 할 수 있다.

⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

■ 고유식별정보, 비밀번호, 바이오정보를 암호화 하는 경우에는 국내 및 미국, 일본, 유럽 등의 국외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

국내·외 암호 연구 관련 기관의 권고 암호 알고리즘 예시

분류	미국(NIST)	일본(CRYPTREC)	유럽(ECRYPT)	국내
대칭키 암호 알고리즘	AES-128/192/256 3TDEA	AES-128/192/256 Camellia-128/192/256	AES-128/192/256 Camellia-128/192/256 Serpent-128/192/256	SEED HIGHT ARIA-128/192/256 LEA-128/192/256
공개키 암호 알고리즘 (메시지 암·복호화)	RSA (사용 권고하는 키길이 확인 필요)	RSAS-OAEP	RSA-OAEP	RSAES
일방향 암호 알고리즘	SHA-224/256/ 384/512	SHA-256/384/512	SHA-224/256/384/512 Whirlpool	SHA-224/256/ 384/512

· 국내·외 암호 연구 관련 기관에서 대표적으로 다루어지는 권고 암호 알고리즘만 표시('18.12월 기준)
· 권고 암호 알고리즘은 달라질 수 있으므로, 암호화 적용시 국내·외 암호 관련 연구기관에서 제시하는 최신 정보 확인 필요

TIP

· 안전한 암호알고리즘, 암호화 방식 등은 "개인정보의 암호화 조치 안내서"를 참조하고, 해당 자료는 개인정보보호 포털(https://www.privacy.go.kr)에서 다운로드 할 수 있다.
· 국내외 암호 연구 관련 기관은 한국인터넷진흥원(KISA)의 암호이용활성화 홈페이지(https://seed.kisa.or.kr)의 "암호 표준화 및 유관기관"에서도 확인 가능하다.
· 국가정보원 검증대상 암호 알고리즘 목록은 국가정보원 홈페이지에서 확인할 수 있다.

⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

■ 암호 키는 암호화된 데이터를 복호화 할 수 있는 정보이므로 암호 키의 안전한 사용과 관리는 매우 중요하며, 라이프사이클 단계별 암호 키 관리 절차를 수립·시행하여야 한다.

암호 키 관리 예시

1. 준비 단계: 암호 키가 사용되기 이전의 단계
 - 암호 키 생성
  · 암호 키 생성에 필요한 난수는 안전한 난수발생기(RNG)를 이용하여 생성
  · 비대칭키 알고리즘 키 생성 방식: 디지털 서명을 위한 키 쌍 생성, 키 설정을 위한 키 쌍 생성
  · 대칭키 알고리즘 방식: 미리 공유된 키, 패스워드, 다수의 암호 키를 이용한 키 생성 등
 - 암호 키 분배
  · 대칭키 알고리즘 키 분배 방식: 수동적 키 분배, 자동화된 키 전송 등
  · 비대칭키 알고리즘의 키 분배 방식
  · 기타 키 자료 생성 및 분배 방식: 영역 파라미터, 초기값, 공유된 비밀, RNG 시드, 다른 공개 및 비밀정보, 중간 값, 난수, 패스워드 등

2. 운영 단계: 암호 키가 암호 알고리즘 및 연산에 사용되는 단계
 - 암호 키의 유효기간동안 사용되는 키 자료들은 필요에 따라 장비 모듈에 보관되거나 별도의 저장 매체에 보관 등으로 저장해야 함
 - 암호 키는 하드웨어 손상 또는 소프트웨어 오류 등의 사유로 손상될 가능성이 있으므로 가용성 보장을 위해서는 키 백업 및 키 복구 등이 가능해야 함
 - 암호 키가 노출되거나 노출의 위협이 있는 경우 그리고 암호키 유효기간의 만료가 가까워지는 경우에는 암호 키를 다른 암호키로 안전하게 변경해야 함

3. 정지 단계: 암호 키가 더 이상 사용되지 않지만, 암호 키에 대한 접근은 가능한 단계
 - 암호 키 보관 및 복구
  · 암호 키는 수정이 불가한 상태이거나 새로운 보관 키를 이용하여 주기적으로 암호화
  · 운영 데이터와 분리되어 보관하며, 암호 정보의 사본들은 물리적으로 분리된 곳에 보관
  · 암호 키는 응용프로그램의 소스 프로그램 내에 평문으로 저장 금지
  · 암호화되는 중요한 정보에 대한 보관키는 백업되어야 하며, 사본은 다른 곳에 보관 등
 - 모든 개인키나 대칭키의 복사본이 더 이상 필요하지 않다면 즉시 파기하여야 함
 - 암호 키 손상시 유효기간 내에 키 자료를 제거하고, 보안 도메인에 속해있는 실체의 권한을 삭제하여 말소된 실체의 키 자료의 사용을 방지해야 함

4. 폐기 단계: 암호 키가 더 이상 사용될 수 없는 단계(폐기 또는 사고 상태)
 - 일반적으로 폐기 단계의 키 자료에 대한 모든 기록은 삭제(다만, 일부기관에서는 감사를 목적으로 특정 키 속성 유지가 필요할 수도 있음)
 - 폐기 상태의 암호 키와 사고 상태의 암호 키들의 특성에 대한 기록 유지 등

TIP
· 개인정보보호 포털(https://www.privacy.go.kr)에서 제공하는 “개인정보의 암호화 조치 안내서” 그리고 암호이용활성화(https://seed.kisa.or.kr)에서 제공하는 “암호 키 관리 안내서” 등을 참고할 수 있다.

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

■ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하거나, 개인정보처리시스템으로부터 개인정보취급자의 업무용 컴퓨터, 모바일 기기에 내려 받아 저장하는 경우에는 안전한 암호화 알고리즘이 탑재된 암호화 소프트웨어 등을 이용하여 해당 파일을 암호화하여 불법적인 유·노출 및 접근 등으로부터 보호하여야 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

■■■ 암호화 적용 기준 요약표 ■■■

<table>
<tr><th colspan="4">구 분</th><th>암호화 기준</th></tr>
<tr><td>정보통신망, 보조저장매체를 통한 송신 시</td><td colspan="3">비밀번호, 바이오정보
고유식별정보</td><td>암호화 송신</td></tr>
<tr><td rowspan="5">개인정보처리 시스템에 저장 시</td><td colspan="3">비밀번호</td><td>일방향(해쉬 함수) 암호화 저장</td></tr>
<tr><td colspan="3">바이오정보</td><td>암호화 저장</td></tr>
<tr><td rowspan="3">고유식별정보</td><td colspan="2">주민등록번호</td><td>암호화 저장</td></tr>
<tr><td rowspan="2">여권번호, 외국인 등록번호, 운전면허 번호</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 시행
① 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과
② 암호화 미적용시 위험도 분석에 따른 결과</td></tr>
<tr><td>업무용 컴퓨터, 모바일 기기에 저장시</td><td colspan="3">비밀번호,
바이오정보,
고유식별정보</td><td>암호화 저장
※ 비밀번호는 일방향 암호화 저장</td></tr>
</table>

⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.

■■■ 안전조치 기준에 따른 적용 유형 ■■■

제7조(개인정보의 암호화)		유형1 (완화)	유형2 (표준)	유형3 (강화)
항	호			
① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.		○	○	○
② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.		○	○	○
③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.		○	○	○
④ 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. 암호화 미적용시 위험도 분석에 따른 결과	○	○	○
부칙 제2조(적용례) 영 제21조의2제2항에 따른 주민등록번호의 암호화 적용시기 이후에는 고유식별정보 중 주민등록번호는 제7조제4항을 적용하지 아니한다.				
⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.		○	○	○
⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.				○
⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.		○	○	○
⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.				

제8조 접속기록의 보관 및 점검

제8조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 다만, 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 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 개인정보를 다운로드한 것이 발견되었을 경우에는 내부 관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.

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

해 설

① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 다만, 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.

■ 접속기록에는 개인정보취급자가 개인정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 아래의 항목들을 기록하여야 한다.

- 계정 : 개인정보처리시스템에서 접속자를 식별할 수 있도록 부여된 ID 등 계정 정보
- 접속일시 : 접속한 시간 또는 업무를 수행한 시간(년-월-일, 시:분:초)
- 접속지 정보 : 개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소 등
- 처리한 정보주체 정보 : 개인정보취급자가 누구의 개인정보를 처리하였는지를 알 수 있는 식별정보(ID, 고객번호, 학번, 사번 등)

※ 기록하는 정보주체 정보의 경우 민감하거나 과도한 개인정보가 저장되지 않도록 하여야 한다.

※ 가명정보를 처리하는 경우 추가 정보의 사용 없이는 정보주체를 식별 할 수 없으므로 정보주체를 구별할 수 있는 정보(가명정보ID, 일련번호 등)가 있다면 '처리한 정보주체 정보' 항목으로 해당 정보를 기록하여야 하며, 정보주체를 구별할 수 있는 정보가 없는 경우는 '처리한 정보주체 정보' 항목을 남기지 아니할 수 있다.

※ 검색조건문(쿼리)을 통해 대량의 개인정보를 처리했을 경우 해당 검색조건문을 정보주체 정보로 기록할 수 있으나, 이 경우 DB테이블 변경 등으로 책임추적성 확보가 어려울 수 있으므로 해당시점의 DB를 백업하는 등 책임추적성 확보를 위해 필요한 조치를 취하여야 한다.

■■■ 검색조건문(쿼리) 예시 ■■■

· '김'씨 성을 가진 회원을 조회하는 경우
- 정보주체의 정보 : SELECT * FROM student WHERE name LIKE '김%';
※ name: 학생이름(컬럼), student: 학생정보(테이블)

· 영화를 연간 50회 이상 관람한 고객에게 VIP 등급부여
- 정보주체의 정보 : UPDATE member SET membership='VIP' WHERE movie_count_per_year>=50;
※ member: 회원정보(테이블), membership: 고객정보(컬럼), movie_count_per_year: 연간 영화관람 건수(컬럼)

- 수행업무 : 개인정보취급자가 개인정보처리시스템을 이용하여 개인정보를 처리한 내용을 알 수 있는 정보

※ 개인정보에 대한 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄) 등이 수행업무에 해당될 수 있다.

■■■ 접속기록 항목 예시 ■■■

· 계정 : A0001(개인정보취급자 계정)
· 접속일시 : 2019-02-25, 17:00:00
· 접속지 정보 : 192.168.100.1(접속한 자의 IP주소)
· 처리한 정보주체 정보 : CLI060719(정보주체를 특정하여 처리한 경우 정보주체의 식별정보)
· 수행업무 : 회원목록 조회, 수정, 삭제, 다운로드 등
※ 위 정보는 반드시 기록하여야 하며 개인정보처리자의 업무환경에 따라 책임추적성 확보에 필요한 항목은 추가로 기록해야 한다.

■ 개인정보처리자는 접속기록을 최소 1년 이상 보관·관리하여야 한다.

■ 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 개인정보 유출 등으로 인한 피해 가능성이 매우 높은 특수성 등으로 인하여 해당 개인정보처리시스템에 대한 접속기록을 최소 2년 이상 보관·관리하여야 한다.

· 민감정보란 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 유전자검사 등의 결과로 얻어진 유전정보, 범죄경력자료, 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보, 인종이나 민족에 관한 정보에 해당하는 정보를 말한다.
· 고유식별정보란 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 주민등록번호, 여권번호, 운전면허의 면허번호, 외국인등록번호를 말한다.

■ 개인정보처리자는 접속기록을 최소 보관기간 이후에도 즉시 삭제하지 않고 책임추적성을 확보하기에 충분한 기간 동안 보관·관리할 수 있도록 개인정보처리시스템에 저장된 개인정보의 중요도 및 민감도 등을 고려하여 내부 관리계획에 보관기간을 정하고 이를 이행하여야 한다.

■ 비인가자의 개인정보처리시스템에 대한 접속 시도 기록 및 정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독 등을 통하여 개인정보처리시스템에 대한 불법적인 접근 및 비정상 행위 등에 대한 안전조치를 강화할 수 있다.

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

■ 개인정보처리자는 개인정보처리시스템의 접속기록을 월 1회 이상 정기적으로 점검하여야 하며, 이를 통해 비인가된 개인정보 처리, 대량의 개인정보에 대한 조회, 정정, 다운로드, 삭제, 출력 등의 비정상 행위를 탐지하고 적절한 대응조치를 할 필요가 있다.

■ 개인정보처리자는 접속기록 점검을 개인정보처리시스템 운영 부서가 자체적으로 하도록 하거나 특정부서가 여러 개의 개인정보 처리시스템을 통합하여 점검할 수 있다.

■■■ 접속기록 내 비정상 행위 예시 ■■■

- 계정 : 접근권한이 부여되지 않은 계정으로 접속한 행위 등
- 접속일시 : 출근시간 전, 퇴근시간 후, 새벽시간, 휴무일 등 업무시간 외에 접속한 행위 등
- 접속지 정보 : 인가되지 않은 단말기 또는 지역(IP)에서 접속한 행위 등
- 처리한 정보주체 정보 : 특정 정보주체에 대하여 과도하게 조회, 다운로드 등의 행위 등
- 수행업무 : 대량의 개인정보에 대한 조회, 정정, 다운로드, 삭제 등의 행위 등
- 그 밖에 짧은 시간에 하나의 계정으로 여러 지역(IP)에서 접속한 행위 등

■ 특히, 개인정보처리시스템에 접근하여 개인정보를 다운로드 한 경우에는 내부 관리계획으로 정하는 바에 따라 그 사유를 확인하고, 개인정보취급자가 개인정보의 오·남용이나 유출을 목적으로 다운로드 한 것이 확인되었다면 지체없이 개인정보취급자가 다운로드 한 개인정보를 회수하여 파기하는 등 필요한 조치를 하여야 한다.

※ 고시 제4조(내부 관리계획의 수립·시행) 제1항 제7호의 “접속기록 보관 및 점검에 관한 사항”에 개인정보처리자의 업무 현황을 고려하여 다운로드한 사유를 확인하여야 하는 다운로드 기준을 책정하여야 한다.

■■■ 다운로드 사유확인이 필요한 기준 책정 예시 ■■■

- **(다운로드 정보주체의 수)** 통상적으로 개인정보 처리 건수가 일평균 20건 미만인 소규모 기업에서 개인정보취급자가 100명 이상의 정보주체에 대한 개인정보를 다운로드 한 경우 사유 확인
- **(일정기간 내 다운로드 횟수)** 개인정보취급자가 1시간 내 다운로드한 횟수가 20건 이상일 경우 단시간에 수차례에 걸쳐 개인정보를 다운로드 한 행위에 대한 사유 확인
- **(업무시간 외 다운로드 수행)** 새벽시간, 휴무일 등 업무시간 외 개인정보를 다운로드 한 경우 사유 확인

- 다운로드란 개인정보처리시스템에 접속하여 개인정보취급자의 컴퓨터 등에 개인정보를 엑셀, 워드, 텍스트, 이미지 등의 파일형태로 저장하는 것을 말한다.

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

■ 개인정보처리자는 아래와 같은 방법 등으로서 개인정보취급자의 접속기록을 안전하게 보관·관리하여야 한다.

- 상시적으로 접속기록 백업을 수행하여 개인정보처리시스템 이외의 별도의 보조저장매체나 별도의 저장장치에 보관

- 접속기록에 대한 위·변조를 방지하기 위해서는 CD-ROM, DVD-R, WORM(Write Once Read Many) 등과 같은 덮어쓰기 방지 매체를 사용

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

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

■ 특히, 개인정보처리시스템의 접속기록은 임의적인 수정·삭제 등이 불가능하도록 접근권한을 제한하는 등의 안전조치를 하여야 한다.

제9조 악성프로그램 등 방지

제9조(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, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시
3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

해 설

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 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 업데이트를 실시하여 최신의 상태로 유지해야 한다.

- 실시간으로 신종·변종 악성 프로그램이 유포됨에 따라 백신 상태를 최신의 업데이트 상태로 적용하여 유지해야 한다.
- 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. 악성프로그램 관련 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 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우에는 감염을 예방하고 감염된 경우 피해를 최소화하기 위해 즉시 업데이트를 실시하여야 한다.

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

  ※ 한컴 오피스, MS 오피스 등 개인정보처리에 자주 이용되는 응용프로그램은 자동업데이트 설정 시, 보안 업데이트 공지에 따른 즉시 업데이트가 용이하다.

- 개인정보처리시스템 등에 대한 보안 업데이트 적용 사항, 적용 일자 등 설치·변경·제거 사항을 기록하는 등 형상관리를 통해 관리체계를 강화할 수 있다.

3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

■ 개인정보처리자는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여 발견된 바이러스, 웜, 트로이목마, 스파이웨어 등의 악성프로그램 등에 대해 삭제, 치료 등의 대응 조치를 하여야 한다.

■ 발견된 악성프로그램에 대해 백신 소프트웨어에서의 삭제, 치료 등의 기능을 지원하지 않는 경우에는 개인정보처리시스템, 업무용 컴퓨터 등을 분리하는 등 악성프로그램의 확산 방지를 위한 적절한 안전조치를 취하여야 한다.

TIP

· 불법 또는 비인가된 보안 프로그램을 사용 시 신규 취약점 등을 삭제하기 위한 업데이트 지원을 받지 못하거나, 악성코드 침투 경로로 이용되어 개인정보 유출이 가능함에 따라 정품 S/W만을 사용하도록 한다.

제10조 관리용 단말기의 안전조치

제10조(관리용 단말기의 안전조치) 개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.

1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
2. 본래 목적 외로 사용되지 않도록 조치
3. 악성프로그램 감염 방지 등을 위한 보안조치 적용

해 설

1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치

■ 개인정보처리자는 관리용 단말기에 대해 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 업무 처리를 하는 특정 직원 등에 한하여 접근을 허용하는 등 업무관련자 이외의 인가 받지 않는 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 접근통제 등의 안전조치를 하여야 한다.

2. 본래 목적 외로 사용되지 않도록 조치

■ 개인정보처리자는 관리용 단말기를 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 사용하여야 하며, 관리용 단말기를 통한 개인정보의 공유 등 다른 목적으로 사용하지 않아야 한다.

3. 악성프로그램 감염 방지 등을 위한 보안조치 적용

■ 개인정보처리자는 악성프로그램 감염 방지를 위한 보안 프로그램의 최신상태 유지, 보안 업데이트 실시, 발견된 악성프로그램의 삭제 등 대응 조치 등을 적용하여야 한다.

· 관리용 단말기의 안전조치 시 고려사항
- 관리용 단말기의 종류에 따른 특성, 중요도
- 관리용 단말기가 개인정보처리시스템에 접속하는 빈도 및 수행업무
- 관리용 단말기를 통한 개인정보의 유출 가능성 및 개인정보처리시스템에 악성코드 전파 등 직·간접적으로 영향을 끼칠 수 있는 요소 등

관리용 단말기의 안전조치 예시

· 관리용 단말기 현황 관리(IP주소, 용도, 담당자, 설치 위치 등)
· 중요 관리용 단말기를 지정하여 외부 반출, 인터넷 접속, 그룹웨어 접속의 금지
· 관리용 단말기에 주요 정보 보관 및 공유 금지
· 비인가자 접근을 방지하기 위한 부팅암호, 로그인 암호, 화면보호기 암호 설정
· 보조기억매체 및 휴대용 전산장비 등에 대한 접근 통제
· 정당한 사용자인가의 여부를 확인할 수 있는 기록을 유지
· 악성코드 감염 방지를 위한 보안 프로그램의 최신상태 유지, 보안 업데이트 적용, 악성프로그램 삭제 등 대응 조치
· 보안 상태 및 사용현황에 대한 정기 점검 등

제11조 물리적 안전조치

제11조(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.

해 설

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

■ 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 비인가자의 출입 등으로 인한 개인정보의 유출 등의 방지를 위한 출입통제 절차를 수립・운영하여야 한다.

■ 출입을 통제하는 방법으로는 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 출입 통제장치, 지문 등 바이오정보 기반 출입통제 장치 등

※ 전산실은 다량의 정보시스템을 운영하기 위한 별도의 물리적인 공간으로 전기시설(UPS, 발전기 등), 공조시설(항온항습기 등), 소방시설(소화설비 등)등을 갖춘 시설을 의미한다.

※ 자료보관실은 가입신청서 등의 문서나 DAT(Digital Audio Tape), LTO(Linear Tape Open), DLT(Digital Linear Tape), 하드디스크 등이 보관된 물리적 저장장소를 의미한다.

- 수기문서 대장 기록 방법(예시) : 출입자, 출입일시, 출입목적, 소속 등

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

■ 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체(이동형 하드디스크, USB메모리, SSD 등) 등은 금고, 잠금장치가 있는 캐비넷 등 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.

■ 개인정보처리시스템을 운영하는 개인정보처리자는 USB메모리, 이동형 하드디스크 등의 보조저장매체를 통해 개인정보가 유출되지 않도록 개인정보가 저장·전송되는 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다.

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

· 보조저장매체의 반출·입 통제를 위한 보안대책 마련 시 고려사항
- 보조저장매체 보유 현황 파악 및 반출·입 관리 계획
- 개인정보취급자 및 수탁자 등에 의한 개인정보 유출 가능성
- 보조저장매체의 안전한 사용 방법 및 비인가된 사용에 대한 대응
- USB를 PC에 연결시 바이러스 점검 디폴트로 설정 등 기술적 안전조치 방안 등

제12조 재해·재난 대비 안전조치

제12조(재해·재난 대비 안전조치) ① 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

② 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

③ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제1항부터 제2항까지 조치를 이행하지 아니할 수 있다.

해 설

① 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

■ 재난이란 국민의 생명·신체·재산과 국가에 피해를 주거나 줄 수 있는 것을 말하며, 재해란 재난으로 인하여 발생하는 피해를 말한다.

「재난 및 안전관리 기본법」 제3조

제3조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. "재난"이란 국민의 생명·신체·재산과 국가에 피해를 주거나 줄 수 있는 것으로서 다음 각 목의 것을 말한다.

가. 자연재난: 태풍, 홍수, 호우(豪雨), 강풍, 풍랑, 해일(海溢), 대설, 한파, 낙뢰, 가뭄, 폭염, 지진, 황사(黃砂), 조류(藻類) 대발생, 조수(潮水), 화산활동, 소행성·유성체 등 자연우주물체의 추락·충돌, 그 밖에 이에 준하는 자연현상으로 인하여 발생하는 재해

나. 사회재난: 화재·붕괴·폭발·교통사고(항공사고 및 해상사고를 포함한다)·화생방사고·환경오염사고 등으로 인하여 발생하는 대통령령으로 정하는 규모 이상의 피해와 국가핵심기반의 마비, 「감염병의 예방 및 관리에 관한 법률」에 따른 감염병 또는 「가축전염병예방법」에 따른 가축전염병의 확산, 「미세먼지 저감 및 관리에 관한 특별법」에 따른 미세먼지 등으로 인한 피해

「자연재해대책법」 제2조

제2조(정의) 이 법에서 사용하는 뜻과 정의는 다음과 같다.

1. "재해"란 「재난 및 안전관리 기본법」(이하 "기본법"이라 한다) 제3조제1호에 따른 재난으로 인하여 발생하는 피해를 말한다.

■ 개인정보처리자는 재해·재난 발생 시 개인정보의 손실 및 훼손 등을 방지하고 개인정보 유출사고 등을 예방하기 위하여 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 문서화하여 마련하고 이에 따라 대처하여야 한다.

■ 또한, 개인정보처리자는 대응절차의 적정성과 실효성을 보장하기 위하여 정기적으로 점검하여야 한다.

- 대응절차를 정기적으로 점검하여 대응절차에 변경이 있는 경우에는 변경사항을 반영하는 등 적절한 조치를 취하여야 하며, 중대한 영향을 초래하거나 해를 끼칠 수 있는 사안 등에 대해서는 사업주·대표·임원 등에게 보고 후, 의사결정 절차를 통하여 적절한 대책을 마련하여야 한다.

② 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

■ 개인정보처리자는 재해·재난 발생 시 혼란을 완화시키고 신속한 의사결정을 위한 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

- 백업 및 복구를 위한 계획에는 개인정보처리시스템 등 백업 및 복구 대상, 방법 및 절차 등을 포함하도록 한다.

TIP · 개인정보처리시스템 백업 및 복구 계획은 위기대응 매뉴얼 등에 포함할 수 있다.

■■■ 개인정보처리시스템 위기대응 메뉴얼 및 백업·복구 계획 예시 ■■■

- 개인정보처리시스템 구성 요소(개인정보 보유량, 종류·중요도, 시스템 연계 장비·설비 등)
- 재해·재난 등에 따른 파급효과(개인정보 유출, 손실, 훼손 등) 및 초기대응 방안
- 개인정보처리시스템 백업 및 복구 우선순위, 목표시점·시간
- 개인정보처리시스템 백업 및 복구 방안(복구센터 마련, 백업계약 체결, 비상가동 등)
- 업무분장, 책임 및 역할
- 실제 발생 가능한 사고에 대한 정기적 점검, 사후처리 및 지속관리 등

③ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제1항부터 제2항까지 조치를 이행하지 아니할 수 있다.

■■■ 안전조치 기준에 따른 적용 유형 ■■■

제12조(재해·재난 대비 안전조치)	유형1 (완화)	유형2 (표준)	유형3 (강화)
① 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.			○
② 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.			○
③ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제1항부터 제2항까지 조치를 이행하지 아니할 수 있다.			

제13조 개인정보의 파기

제13조(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 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, 천공 등으로 삭제

해 설

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 보유 기간의 경과, 개인정보의 처리 목적 달성 등 개인정보가 불필요하게 되었을 때는 지체 없이 그 개인정보를 파기하여야 한다. 개인정보를 파기할 때에는 복구 또는 재생되지 않도록 조치하여야 한다.

■ 개인정보처리자는 개인정보를 파기할 때에는 복구 또는 재생되지 않도록 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 등)으로 덮어쓰기(3회 이상 권고), 해당 드라이브를 안전한 알고리즘 및 키 길이로 암호화 저장 후 삭제하고 암호화에 사용된 키 완전 폐기 및 무작위 값 덮어쓰기 등

· 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 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, 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 비인가 된 복구에 대해 조치

- 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록 매체인 경우: 해당 부분을 마스킹, 천공 등으로 삭제

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

제14조 재검토 기한

제14조(재검토기한) 개인정보보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2020년 8월 11일을 기준으로 매 3년이 되는 시점(매 3년째의 8월 10일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

해 설

■ 개인정보보호위원회는 신규 침해위협 및 기술·서비스 발전 등을 고려하여 이 기준에 대하여 정기적으로 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

[부칙] <제2020-2호, 2020. 8. 11.>

이 고시는 고시한 날부터 시행한다.

[별표]

개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준

유형	적용 대상	안전조치 기준
유형1 (완화)	· 1만명 미만의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인	· 제5조 : 제2항부터 제5항까지 · 제6조 : 제1항, 제3항, 제6항 및 제7항 · 제7조 : 제1항부터 제5항까지, 제7항 · 제8조 · 제9조 · 제10조 · 제11조 · 제13조
유형2 (표준)	· 100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업 · 10만명 미만의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 · 1만명 이상의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인	· 제4조 : 제1항제1호부터 제11호까지 및 제15호, 제3항부터 제4항까지 · 제5조 · 제6조 : 제1항부터 제7항까지 · 제7조 : 제1항부터 제5항까지, 제7항 · 제8조 · 제9조 · 제10조 · 제11조 · 제13조
유형3 (강화)	· 10만명 이상의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관 · 100만명 이상의 정보주체에 관한 개인정보를 보유한 중소기업, 단체	· 제4조부터 제13조까지

붙임 FAQ

문1. 개인정보의 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준이란 무엇을 의미하는지?

⇒ 이 기준은 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준입니다.

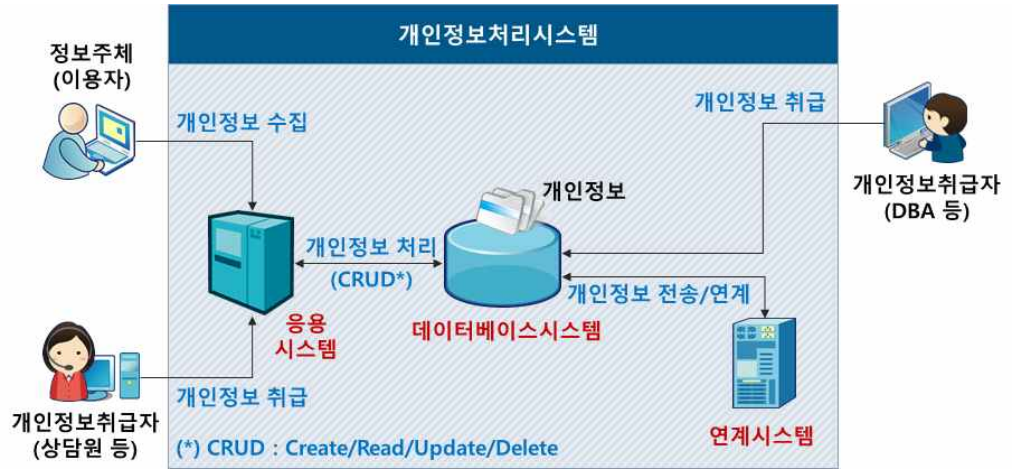
개인정보처리자는 처리하는 개인정보의 종류 및 중요도, 개인정보를 처리하는 방법 및 환경 등을 고려하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 하기 위하여 필요하다면 본 고시에서 정한 사항 이외의 추가적인 보호조치를 적용하여 개인정보의 안전성 확보조치를 강화하시기 바랍니다.

문2. 개인정보처리시스템의 범위는 어디까지를 말하는지?

⇒ 개인정보처리시스템이란 일반적으로 데이터베이스(DB) 내의 데이터에 접근할 수 있도록 해주는 응용시스템을 의미하며, 데이터베이스를 구축하거나 운영하는데 필요한 시스템을 말합니다. 다만, 개인정보처리시스템은 개인정보처리자의 개인정보 처리방법, 시스템 구성 및 운영환경 등에 따라 달라질 수 있습니다.

예를 들어, 온라인 서비스 제공을 위한 데이터베이스를 구축·운영하면서 회원 관리, 민원처리 등 개인정보 처리가 수반되는 서비스 제공을 위하여 웹서버, 어플리케이션 서버, 중계 서버로 시스템을 구성했다면 데이터베이스시스템을 포함하여 웹서버, 어플리케이션 서버, 중계 서버도 개인정보처리시스템에 해당할 수 있습니다.

업무용 컴퓨터에 데이터베이스 응용프로그램이 설치·운영되어 다수의 개인정보 취급자가 사용할 경우에도 개인정보처리시스템에 해당될 수 있으나, 데이터베이스 응용프로그램이 설치·운영되지 않는 PC, 노트북과 같은 업무용 컴퓨터는 개인정보처리시스템에서 제외됩니다.



문3. 관리용 단말기의 범위는 어디까지를 말하는지?

⇒ 개인정보처리시스템을 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속할 수 있는 업무용 컴퓨터, 노트북 등이 관리용 단말기에 해당될 수 있습니다.

여기에서 "직접 접속"이란 물리적 구조와 상관없이 단말기에서 개인정보처리시스템에 대하여 관리, 운영, 개발, 보안 등의 목적으로 활용할 수 있는 명령어 등을 직접 입력하여 처리할 수 있는 상태를 말합니다.

문4. 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.

문5. 전용선의 범위는 어디까지인지?

⇒ 물리적으로 독립된 회선으로서 두 지점간에 독점적으로 사용하는 회선으로 개인정보처리자와 개인정보취급자, 또는 본점과 지점 간 직통으로 연결하는 회선 등을 의미합니다.

문6. 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)

수탁자도 개인정보의 안전성 확보조치에 관한 개인정보 보호법 제24조제3항, 제29조가 준용되어 적용됩니다.(법 제26조제7항)

따라서 수탁자는 이 기준에 따라 개인정보의 안전성 확보에 필요한 조치를 이행하여야 합니다.

문7. 안전조치 기준 적용은 어떻게 되나요?

⇒ 이 기준 [별표]에 따라 개인정보처리자 유형과 개인정보 보유량을 동시에 적용하여 개인정보처리자가 해당하는 유형에 안전조치 기준을 적용하여야 합니다.

■■■ 안전조치 기준 적용 분류 ■■■

- 개인정보처리자 유형: 공공기관, 대기업, 중견기업, 중소기업, 소상공인, 개인, 단체
- 개인정보 보유량: 1만명 미만, 1만명~10만명 미만, 10만명~100만명 미만, 100만명 이상

<table>
<tr><th>구 분</th><th>1만명 미만</th><th>1만명~10만명 미만</th><th>10만명~100만명 미만</th><th>100만명 이상</th></tr>
<tr><td>공공기관</td><td colspan="2" rowspan="3">유형2(표준)</td><td colspan="2" rowspan="3">유형3(강화)</td></tr>
<tr><td>대기업</td></tr>
<tr><td>중견기업</td></tr>
<tr><td>중소기업</td><td colspan="3">유형2(표준)</td><td>유형3(강화)</td></tr>
<tr><td>소상공인</td><td rowspan="2">유형1(완화)</td><td colspan="3" rowspan="2">유형2(표준)</td></tr>
<tr><td>개인</td></tr>
<tr><td>단체</td><td>유형1(완화)</td><td colspan="2">유형2(표준)</td><td>유형3(강화)</td></tr>
</table>

문8. 중소기업입니다. 안전조치 기준이 어떻게 적용되나요?

⇒ “중소기업”이란 「중소기업기본법」 제2조 및 동법 시행령 제3조에 해당하는 기업을 의미합니다.

100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업은 유형2(표준)에 해당하며, 100만명 이상의 정보주체에 관한 개인정보를 보유한 중소기업은 유형3(강화)에 해당합니다. 회사가 해당하는 유형에 따른 조치를 이행하여야 합니다.

이 경우 어느 유형에 해당하는지에 대한 입증책임 의무는 해당 기업에 있습니다. 중소기업 여부 그리고 개인정보 보유량에 대하여 스스로 증명할 수 있어야 합니다.

문9. 개인정보 보유량이 변동되는 경우 안전조치 기준이 어떻게 적용되나요?

⇒ 개인정보 보유량이 변동되는 시점(日)에 개인정보처리자가 해당하는 유형의 안전조치가 되어 있어야 합니다.

개인정보처리자는 개인정보 보유량의 변경·변동 가능여부에 대하여 정기적으로 확인하는 등 개인정보처리자 유형 또는 개인정보 보유량이 변동되는 경우에도 해당하는 유형의 안전조치 기준을 적용하여야 합니다.

문10. 내부 관리계획 수립 시, 문서 제목을 반드시 "내부 관리계획"으로 하여야 하나요?

⇒ 내부 관리계획의 문서 제목은 가급적 "내부 관리계획"이라는 용어를 사용하는 것이 바람직하나, 개인정보처리자의 내부 방침에 따라 다른 용어를 사용할 수도 있습니다. 다른 용어를 사용하는 경우에도 이 기준 제4조(내부 관리계획의 수립·시행)에 관한 사항을 이행하여야 합니다.

문11. 부동산 중개업을 운영하는 소상공인입니다. 현재 500명의 고객관리를 위해 업무용 컴퓨터를 운영하고 있습니다. "개인정보의 안전성 확보조치 기준"에 따라 어떠한 조치를 수행해야 하는지?

⇒ 안전조치 기준 유형1(완화)에 해당하는 소상공인이 업무용 컴퓨터로 고객정보를 관리하는 경우 업무용 컴퓨터에 비밀번호를 설정하고 업무용 컴퓨터에서 제공되는 침입차단 기능을 설정하고 악성프로그램을 차단하도록 백신 소프트웨어를 설치하는 등 이 기준에 따른 안전조치를 하여야 합니다.

문12. 공공기관에서 암호화를 수행하는 경우, 이 기준에서 규정하는 사항과 다른 기관에서 규정하는 지침 등이 있는 경우에는 어느 규정을 준수해야 하는지?

⇒ 이 기준의 제7조(개인정보의 암호화)에서 규정하는 사항을 이행하면 "개인정보 보호법"상 암호화 의무는 준수한 것으로 볼 수 있습니다.

다만, 해당 분야에 관련된 다른 암호화 지침 등이 있는 경우에는 해당 규정도 준수하여야 할 것입니다.

문13. 공공기관입니다. 고객정보 데이터베이스를 운영하고 있습니다. 개인정보 보호법에서 규정하는 암호화 대상이 무엇이며 어떻게 해야 하는지?

⇒ "개인정보 보호법" 상에서 요구되는 암호화 대상은 비밀번호, 바이오정보, 고유식별정보(주민등록번호, 외국인등록번호, 운전면허번호, 여권번호)입니다. 개인정보처리자는 비밀번호, 바이오정보, 고유식별정보를 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 주민등록번호를 제외한 고유식별정보를 저장하는 경우 영향평가의 결과에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있습니다.

■■■ 암호화 적용 기준 요약표 ■■■

<table>
<tr><th colspan="4">구 분</th><th>암호화 기준</th></tr>
<tr><td>정보통신망, 보조저장매체를 통한 송신 시</td><td colspan="3">비밀번호, 바이오정보, 고유식별정보</td><td>암호화 송신</td></tr>
<tr><td rowspan="5">개인정보처리 시스템에 저장 시</td><td colspan="3">비밀번호</td><td>일방향(해쉬 함수) 암호화 저장</td></tr>
<tr><td colspan="3">바이오정보</td><td>암호화 저장</td></tr>
<tr><td rowspan="3">고유식별정보</td><td colspan="2">주민등록번호</td><td>암호화 저장</td></tr>
<tr><td rowspan="2">여권번호, 외국인 등록번호, 운전면허 번호</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 시행
① 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과
② 암호화 미적용시 위험도 분석에 따른 결과</td></tr>
<tr><td>업무용 컴퓨터, 모바일 기기에 저장시</td><td colspan="3">비밀번호, 바이오정보, 고유식별정보</td><td>암호화 저장
※ 비밀번호는 일방향 암호화 저장</td></tr>
</table>

문14. 내부망에 저장하는 주민등록번호는 영향평가나 위험도 분석을 통해 암호화하지 않고 보유할 수 있는지?

⇒ 내부망에 주민등록번호를 저장하더라도, 법 제24조의2, 동법 시행령 제21조의2에 따라 "개인정보 영향평가"나 "암호화 미적용시 위험도 분석"의 결과에 관계없이 암호화 하여야 합니다.

문15. 암호화해야 하는 바이오 정보의 대상은 어디까지인지?

⇒ 바이오 정보를 식별 및 인증 등의 업무에 활용하기 위하여 수집·이용하는 경우에는 암호화 조치를 하여야 하며 복호화가 가능한 양방향 암호화 저장을 할 수 있습니다.

문16. 업무용 PC에서 고유식별정보나 바이오정보를 처리하는 경우 개인정보 암호화는 어떻게 해야 하는지?

⇒ PC에 저장된 개인정보의 경우 상용프로그램(한글, 엑셀 등)에서 제공하는 비밀번호 설정 기능을 사용하여 암호화를 적용하거나, 안전한 암호화 알고리즘을 이용하는 소프트웨어를 사용하여 암호화해야 합니다.

암호화에 관한 세부사항은 "개인정보의 암호화 조치 안내서"를 참고할 수 있습니다.

문17. 전산실 또는 자료보관실이 없는 중소기업입니다. "개인정보의 안전성 확보조치 기준" 제11조(물리적 안전조치)조항을 준수해야 하는지?

⇒ 개인정보가 포함된 서류나 보조저장매체 등을 운영하는 경우에는 잠금장치가 있는 캐비넷 등 안전한 장소에 보관하여야 하며, 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여 운영해야 합니다.

다만, 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관장소를 별도로 두고 있지 않은 경우에는 이에 대한 출입통제 절차를 수립·운영하지 않을 수 있습니다.

문18. 접속기록에는 어떠한 정보를 보관·관리하여야 하는지?

⇒ 접속기록에는 계정(개인정보처리시스템에서 접속자를 식별할 수 있도록 부여된 ID 등 계정정보), 접속일시(접속한 시간 또는 업무를 수행한 시간), 접속지 정보(개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소), 정보주체의 정보(개인정보취급자가 누구의 개인정보를 처리하였는지를 알 수 있는 식별정보), 수행업무(개인정보취급자가 개인정보처리시스템을 이용하여 개인정보를 처리한 내용을 알 수 있는 정보)가 포함됩니다.

문19. 접속기록에 기록하는 "처리한 정보주체 정보"의 범위는 어디까지를 말하는지?

⇒ 접속기록에 기록하는 "처리한 정보주체의 정보"는 개인정보취급자가 처리한 정보주체를 확인할 수 있는 식별정보(ID, 고객번호, 학번, 사번 등)를 기록하여야 하며, 민감하거나 과도한 개인정보가 저장되지 않도록 하여야 합니다. 또한, 다량의 정보주체의 정보를 처리한 경우 검색조건문을 정보주체의 정보로 기록할 수 있습니다. 다만, 변경이 빈번하게 발생하거나 임시적으로 활용하는 테이블에 저장된 개인정보를 처리하는 경우, 검색조건문을 정보주체의 정보로 기록하면 책임추적성 확보가 어려울 수 있으므로 해당시점의 DB를 백업하는 등 필요한 조치를 하여야 합니다.

문20. 월 1회 이상 접속기록을 점검할 때 보관하고 있는 모든 접속기록에 대하여 점검해야 하는지?

⇒ 월 1회 이상 접속기록 점검을 할 때 보관하고 있는 모든 접속기록을 점검할 필요는 없습니다. 개인정보처리자가 기존에 점검을 완료한 접속기록임을 확인하였을 경우, 해당 접속기록에 대하여 별도의 점검을 하지 않을 수 있습니다. 또한, 내부 관리계획에서 정하는 점검 기준 및 점검 범위는 실질적인 개인정보 유출 및 오·남용을 확인할 수 있도록 타당하고 합리적으로 수립·이행하여야 합니다.

문21. 재해·재난 대비 안전조치는 반드시 필요한가요?

⇒ 재해・재난 발생 시 개인정보처리시스템에 보관된 개인정보의 손실, 훼손 등을 방지하고 개인정보 유출 사고 등을 예방하기 위한 안전조치는 필요합니다.

개인정보처리자는 재해・재난 발생 시 혼란을 완화시키고 신속한 의사결정을 위하여 대응절차 마련 및 점검, 백업 및 복구 계획 수립 등을 하여야 합니다.

참고 안전조치 기준 적용 유형

■■■ [별표]에 따른 안전조치 기준 적용 유형 ■■■

조	항	호	유형1 (완화)	유형2 (표준)	유형3 (강화)
제1조(목적)					
제2조(정의)					
제3조(안전조치 기준 적용)					
제4조 (내부관리계획의 수립·시행)	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.	1. 개인정보 보호책임자의 지정에 관한 사항		○	○
		2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항		○	○
		3. 개인정보취급자에 대한 교육에 관한 사항		○	○
		4. 접근 권한의 관리에 관한 사항		○	○
		5. 접근 통제에 관한 사항		○	○
		6. 개인정보의 암호화 조치에 관한 사항		○	○
		7. 접속기록 보관 및 점검에 관한 사항		○	○
		8. 악성프로그램 등 방지에 관한 사항		○	○
		9. 물리적 안전조치에 관한 사항		○	○
		10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항		○	○
		11. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항		○	○
		12. 위험도 분석 및 대응방안 마련에 관한 사항			○
		13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항			○
		14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항			○
		15. 그 밖에 개인정보 보호를 위하여 필요한 사항		○	○
	② [별표]의 유형1에 해당하는 개인정보처리자는 제1항에 따른 내부 관리계획을 수립하지 아니할 수 있고, [별표]의 유형2에 해당하는 개인정보처리자는 제1항제12호부터 제14호까지를 내부 관리계획에 포함하지 아니할 수 있다.				
	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 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리 하여야 한다.			○	○

조	항	호	유형1 (완화)	유형2 (표준)	유형3 (강화)
제5조 (접근 권한의 관리)	① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.			○	○
	② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 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 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.		○	○	○
	⑥ 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.			○	○
	⑦ [별표]의 유형1에 해당하는 개인정보처리자는 제1항 및 제6항을 아니할 수 있다.				

조	항	호	유형1 (완화)	유형2 (표준)	유형3 (강화)
제6조 (접근 통제)	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 시도 탐지 및 대응	○	○	○
	② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.			○	○
	③ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.		○	○	○
	④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.			○	○
	⑤ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 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 접근 통제 기능을 이용할 수 있다.		○	○	○
	⑦ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.		○	○	○
	⑧ [별표]의 유형1에 해당하는 개인정보처리자는 제2항, 제4항부터 제5항까지의 조치를 아니할 수 있다.				

조	항	호	유형1 (완화)	유형2 (표준)	유형3 (강화)
제7조 (개인정보의 암호화)	① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.		○	○	○
	② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.		○	○	○
	③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.		○	○	○
	④ 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. 암호화 미적용시 위험도 분석에 따른 결과	○	○	○
	부칙 제2조(적용례) 영 제21조의2제2항에 따른 주민등록번호의 암호화 적용시기 이후에는 고유식별정보 중 주민등록번호는 제7조제4항을 적용하지 아니한다.				
	⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.		○	○	○
	⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.				○
	⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.		○	○	○
	⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.				

조	항	호	유형1 (완화)	유형2 (표준)	유형3 (강화)
제8조 (접속기록의 보관 및 점검)	① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 다만, 5만 명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 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 개인정보를 다운로드한 것이 발견되었을 경우에는 내부 관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.		○	○	○
	③ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.		○	○	○
제9조 (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, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지	○	○	○
		2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시	○	○	○
		3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치	○	○	○
제10조 (관리용 단말기의 안전조치)	개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.	1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치	○	○	○
		2. 본래 목적 외로 사용되지 않도록 조치	○	○	○
		3. 악성프로그램 감염 방지 등을 위한 보안조치 적용	○	○	○

조	항	호	유형1 (완화)	유형2 (표준)	유형3 (강화)
제11조 (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.		○	○	○
제12조 (재해·재난 대비 안전조치)	① 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.				○
	② 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.				○
	③ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제1항부터 제2항까지 조치를 이행하지 아니할 수 있다.				
제13조 (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 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, 천공 등으로 삭제1	○	○	○
제14조(재검토 기한)					