KISA 한국인터넷진흥원

개인정보의 안전성 확보조치 기준

(개정 2016.9.1. 행정안전부고시 제2016-35호)

2018. 3

제1조 법적 근거 및 목적

개인정보 보호법 제29조

안전조치의무

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

제73조 벌칙

✓ 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자는 2년 이하의 징역 또는 2천만원 이하의 벌금

제75조 과태료

✓ 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자에게는 3천만원 이하의 과태료

제1조 법적 근거 및 목적

동법 시행령 제30조

개인정보의 안전성 확보 조치

01 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

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

03 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 행정자치부장관이 정하여 고시한다.

개인정보의 안전성 확보조치 기준

제1조 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 기준

(개정 2016. 9. 1. 행정자치부고시 제2016-35호)

제2조 용어 정의

개인정보처리시스템

데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 시스템

바이오정보

지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 가공되거나 생성된 정보를 포함

위험도 분석

개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소 식별·평가하고 해당 위험요소 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위

접속기록

개인정보취급자 등이 개인정보처리시스템에 접속한 사실을 알 수 있는 계정, 접속일시, 접속자 정보, 수행업무 등을 전자적으로 기록한 것

공개된 무선망

불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할수 있는 망

관리용 단말기

개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리 시스템에 직접 접속하는 단말기

제3조 안전조치 기준 적용

- 개인정보처리자는 개인정보처리자 유형 및 개인정보 보유량에 따라 해당하는 유형 유형1(완화) 유형2(표준) 유형3(강화) 의 안전조치를 이행

<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>개 인</td></tr>
<tr><td>단 체</td><td>유형1(완화)</td><td colspan="2">유형2(표준)</td><td>유형3(강화)</td></tr>
</table>

- 개인정보처리자 유형 또는 개인정보 보유량이 변동되는 경우에도 해당하는 유형의 안전조치기준을 적용
- 개인정보처리자가 어느 유형에 해당하는지에 대하여 입증 책임 의무

제4조 내부 관리계획의 수립·시행

- 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음의 사항을 포함하는 **내부 관리계획을 수립·시행**

유형1	유형2	유형3
내부 관리계획을 수립하지 않을 수 있음	12~14까지를 포함하지 않을 수 있음	1~15까지를 포함하여야 함

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

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

- 개인정보 보호책임자는 연 1회 이상으로 **내부 관리계획의 이행 실태를 점검·관리**

제5조 접근 권한의 관리

개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한 범위로 **업무 담당자에 따라 차등 부여** (유형1은 아니할 수 있음)

전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 **지체없이 개인정보처리시스템의 접근 권한 변경 또는 말소**

- 권한 부여, 변경 또는 말소에 대한 내역 기록하고, **그 기록 최소 3년간 보관**

개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 **개인정보취급자별로 사용자계정을 발급**하고 다른 개인정보취급자와 공유되지않도록 조치

개인정보취급자 또는 정보주체가 안전한 비밀번호 설정하여 이행할 수 있도록 **비밀번호 작성규칙을 수립하여 적용**

계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 **개인정보처리시스템에 대한 접근 제한하는 등 필요한 기술적 조치** (유형1은 아니할 수 있음)

제6조 접근 통제

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

- ✓ 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 **인가받지 않은 접근을 제한**
- ✓ 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 **불법적인 개인정보 유출 시도 탐지 및 대응**

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

개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 **안전한 접속수단을 적용하거나 안전한 인증수단을 적용**

(유형1은 아니할 수 있음)

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

제6조 접근 통제

- 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정,공개된 무선망 이용 등 통하여 열람권한이없는 자 공개되거나 유출되지 않도록 **개인정보처리시스템, 업무용 컴퓨터,모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치**

- 인터넷 홈페이지를 통해 고유식별정보를 처리하는 경우 **연 1회 이상 취약점을 점검하고 필요한 보완 조치**

(유형1은 아니할 수 있음)

- 개인정보처리시스템에 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 **자동으로 시스템 접속 차단 조치**

(유형1은 아니할 수 있음)

- 업무용 모바일 기기의 분실.도난 등으로 개인정보가 유출되지 않도록 해당 **모바일 기기에 비밀번호 설정 등의 조치**

제7조 개인정보의 암호화

구 분				암호화 기준
정보통신망, 보조저장매체를 통한 송신 시	비밀번호, 바이오정보, 고유식별정보			암호화 송신
개인정보처리 시스템에 저장 시	비밀번호			일방향(해쉬 함수) 암호화 저장
	바이오정보			암호화 저장
	고유식별 정보	주민등록번호		암호화 저장
		여권번호, 외국인 등록번호, 운전면허번호	인터넷 구간, 인터넷 구간과 내부망의 중간 지점(DMZ)	암호화 저장
			내부망에 저장	암호화 저장 또는 다음 항목에 따라 암호화 적용여부, 적용범위를정하여 시행 가능 ※ 개인정보 영향평가 대상이 되는 공공기관의 경우, 그 개인정보 영향평가의 결과 ※ 암호화 미적용시 위험도 분석에 따른 결과
업무용 컴퓨터, 모바일 기기에 저장시	비밀번호, 바이오정보, 고유식별정보			암호화 저장 ※ 비밀번호는 일방향 암호화 저장 ※ 상용 암호화 소프트웨어 또는 안전한 알고리즘 암호화

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

(유형1 및 유형2는 아니할 수 있음)

제8조 접속기록의 보관 및 점검

- 개인정보취급자가 개인정보처리시스템에 접속한 기록을 **6개월 이상 안전하게 보관·관리**

계 정

개인정보처리 시스템에서 접속자를 식별할 수 있도록 부여된 ID 등 계정 정보

접속일시

접속한 시점 또는 업무를 수행한 시점 (년-월-일, 시:분:초)

접속자 정보

접속한 자의 PC, 모바일기기 등 단말기 정보 또는 서버의 IP주소 등 접속 주소

수행업무

개인정보취급자가 개인정보 처리시스템을 이용하여 개인정보 처리한 내용을 알 수 있는 정보

- 개인정보처리시스템의 **접속기록 등을 반기별로 1회 이상 점검**

제9조 악성프로그램 등 방지

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

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

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

발견된 악성프로그램 등에 대해 삭제 등 **대응 조치**

제10조 관리용 단말기의 안전조치

개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음의 안전조치를 이행

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

인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치

본래 목적 외로 사용되지 않도록 조치

악성프로그램 감염 방지 등 을 위한 보안조치 적용

제11조 물리적 안전조치

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

- 개인정보가 포함된 **서류, 보조저장매체 등을 잠금장치**가 있는 안전한 장소에 보관

- 개인정보가 포함된 **보조저장매체의 반출·입 통제를 위한 보안대책**을 마련
  - 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있음

제12조 재해·재난 대비 안전조치

화재, 홍수, 단전 등 재해·재난 발생 시
개인정보처리시스템 보호를 위한
위기대응 매뉴얼 등 대응절차를
마련하고 정기적으로 점검

재해·재난 발생 시
개인정보처리시스템 백업 및
복구를 위한 계획을 마련
(유형1 및 유형2는 제12조를 아니할 수 있음)

제13조 개인정보의 파기

- 개인정보를 파기할 경우 다음 어느 하나의 조치를 하여야 함

전체 파기

완전파괴
(소각·파쇄 등)

전용 소자장비
이용하여 삭제

데이터가 복원
되지 않게 초기화
또는 덮어쓰기

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

일부 파기

전자적 파일 형태인 경우

개인정보를 삭제한 후 복구 및
재생되지 않도록 관리 및 감독

제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우

해당 부분을 마스킹, 천공 등으로 삭제

감사합니다

KISA 한국인터넷진흥원