개인정보의 기술적·관리적
보호조치 기준 해설서

2012. 9

방송통신위원회
KOREA COMMUNICATIONS COMMISSION

KISA 한국인터넷진흥원
Korea Internet & Security Agency

o 본 해설서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) 제28조제1항과 같은 법 시행령 제15조제6항에 따른 〃개인정보의 기술적·관리적 보호조치 기준〃 고시가 개정(2012. 8. 23)됨에 따라,

- 각 조항별로 주안점과 가급적 구체적인 사례를 제시하여 해석상 오해의 소지를 없애고, 올바른 이해를 통해 사업자의 개인정보 보호조치 이행을 돕기 위한 목적으로 발간되었습니다.

o 따라서, 본 해설서에서 안내하고 있는 제품이나 사례 등은 각 기업의 고유한 특성에 따라 실제 환경에서 그대로 적용되지 않을 수 있습니다.

- 본 기준을 이행하는데 필요한 제품이나 보안 방법을 도입하기 전에 각 기업의 환경에 적합한 제품을 찾아 확인하여 적용하는 것이 필요합니다.

o 본 해설서는 지속적으로 보완되어 KISA 홈페이지 [www.kisa.or.kr - 자료실 - 주요사업 자료실]와 개인정보보호 포털 [www.i-privacy.kr - 자료실 - 가이드라인]에 게시될 예정입니다.

o 해설서의 내용 중 오류가 있거나 의견이 있을 경우에는 KISA 홈페이지 [www.kisa.or.kr - 고객광장 - 118 상담서비스 - 3.개인정보민원신청] 또는 전자메일 118@kisa.or.kr로 문의하여 주시기 바랍니다.

목 차

개인정보의 기술적·관리적 보호조치 기준 해설서

Ⅰ. 개요

1. 제·개정 배경
2. 기준의 법적 성격

Ⅰ. 개요

1. 제・개정의 배경

o 과거의 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서는 개인정보의 분실・도난・누출・변조・훼손을 방지하기 위한 조치를 강구하도록 원칙만 규정하고 있었으나,

- 이후 이용자의 개인정보를 취급하는 사업자가 안전한 개인정보 취급・관리 조치를 취하지 않아 개인정보가 유출 또는 오・남용되는 사례가 빈번하게 발생하여 심각한 사회문제로 대두되면서 보다 세부적인 규정 마련이 필요하게 되었다.

o 즉, 개인정보의 취급을 위한 구체적이고 명확한 기술적・관리적 세부 기준이 없어 개인정보를 취급하는 사업자들이 보호조치를 이행하는데 어려움이 있어,

- 법 개정(2004.1.29)과 시행규칙 개정(2004.7.30)을 통해 개인정보의 안전성 확보에 필요한 최소한의 기술적・관리적 보호조치 기준을 정하여 고시할 수 있도록 법적 근거를 마련하게 되었다.

o 보호조치 기준 제정(2005.3.24) 이후에도 해킹 등 외부 공격에 의한 개인정보 유출과 유출 정보를 활용한 2차 피해 확산 문제 등이 발생함에 따라,

- 개인정보의 보호조치 강화를 위해 법률(2008.6.13) 및 시행령(2009.1.28)을 개정하였고, 「개인정보의 기술적・관리적 보호조치 기준」 고시도 아래의 사항을 추가(2009.8.7) 하였다.
  ・개인정보처리시스템에 접근하는 개인정보취급자 접근통제규칙의 상세화
  ・침해대응을 위해 개인정보취급자 접속기록의 관리・감독의 강화
  ・민감한 개인정보의 불법사용을 방지하기 위한 개인정보의 암호화 강화 등

o 이와 같은 조치에도 불구하고 대량의 개인정보 유출사고가 지속됨에 따라, 보다 높은 수준의 보안조치를 위해 「개인정보의 기술적・관리적 보호조치 기준」을 개정(2012. 8. 23.)하여 외부망과의 망분리를 의무화 하였다.
  ・개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등에 대한 외부 인터넷망 차단

2. 개인정보의 보호조치 기준의 법적 성격

o 본 기준은 가이드라인이나 지침과 같은 권고가 아니며 법률에 의하여 반드시 준수하여야 하는 의무사항을 구체화한 것으로, 동 기준을 위반할 경우 법률에 따른 형사처벌이나 행정처분이 부과될 수 있다.

- 법 제28조제1항제2호부터 제5호까지의 조치(개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치 설치·운영, 접속기록의 위조·변조 방지조치, 개인정보의 암호화 저장·전송, 컴퓨터바이러스 침해 방지조치)를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조·훼손한 경우 2년 이하의 징역 또는 1천만원 이하의 벌금과 1억원 이하의 과징금 부과(법 제28조제1항, 제73조제1호, 제64조의3제6호)

- 제28조제1항에 따른 기술적·관리적 조치를 하지 않은 경우 3천만원 이하의 과태료 부과(법 제28조제1항, 제76조제1항제3호)

o 본 해설서는 보호조치 기준에 대한 구체적인 사례 등을 제시하여 정보통신서비스 제공자등이 관련 기준을 해석·적용함에 있어 오해의 소지를 없애고 자발적으로 준수할 수 있도록 지원하기 위한 것으로 행정지도의 성격을 갖는다고 볼 수 있다. 다만, 해설서에서 소개된 기준 이행방법은 사업자의 이해제고를 위해 영세사업자를 고려한 최소한의 기준을 제시한 것으로 사업자의 규모나 서비스의 특징을 모두 반영한 것은 아니다.

[개인정보의 기술적 · 관리적 보호조치 기준 관련 법 및 시행령]

정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17, 일부개정)	정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2012. 8. 17, 일부개정)
제28조 (개인정보의 보호조치) ① 정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실・도난・누출・변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적・관리적 조치를 하여야 한다. 1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립・시행 2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치・운영 3. 접속기록의 위조・변조 방지를 위한 조치 4. 개인정보를 안전하게 저장・전송할 수 있는 암호화기술 등을 이용한 보안조치 5. 백신 소프트웨어의 설치・운영 등 컴퓨터 바이러스에 의한 침해 방지조치 6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치 ② 정보통신서비스 제공자등은 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여야 한다.	**제15조 (개인정보의 보호조치)** ① 법 제28조제1항제1호에 따라 정보통신서비스 제공자등은 개인정보의 안전한 취급을 위하여 다음 각 호의 내용을 포함하는 내부관리계획을 수립·시행하여야 한다. 1. 개인정보 관리책임자의 지정 등 개인정보보호 조직의 구성·운영에 관한 사항 2. 개인정보취급자의 교육에 관한 사항 3. 제2항부터 제5항까지의 규정에 따른 보호조치를 이행하기 위하여 필요한 세부 사항 ② 법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 다음 각 호의 조치를 하여야 한다. 다만, 제3호의 조치는 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등만 해당한다. 1. 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템(이하 "개인정보처리시스템"이라 한다)에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행 2. 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영 3. 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단 4. 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영 5. 그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치

정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17, 일부개정)	정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2012. 8. 17, 일부개정)
제64조의3(과징금의 부과 등) ① 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 1 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 다만, 제6호에 해당하는 행위가 있는 경우에는 1억원 이하의 과징금을 부과할 수 있다. 1. ~ 5. (생략) 6. 제28조제1항제2호부터 제5호까지의 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손한 경우 7. (생략) ② ~ ⑦ (생략) **제73조 (벌칙)** 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다. 1. 제28조제1항제2호부터 제5호까지(제67조에 따라 준용되는 경우를 포함한다)의 규정에 따른 기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손한 자 2. ~ 8. (생략) **제76조 (과태료)** ① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다. 1. ~ 2의2. (생략) 3. 제28조제1항(제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 아니한 자 4. ~ 12. (생략) ② ~ ⑦ (생략)	③ 법 제28조제1항제3호에 따라 정보통신서비스 제공자등은 접속기록의 위조·변조 방지를 위하여 다음 각 호의 조치를 하여야 한다. 1. 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독 2. 개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관 ④ 법 제28조제1항제4호에 따라 정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 다음 각 호의 보안조치를 하여야 한다. 1. 비밀번호 및 바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다)의 일방향 암호화 저장 2. 주민등록번호 및 계좌정보 등 금융정보의 암호화 저장 3. 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안서버 구축 등의 조치 4. 그 밖에 암호화 기술을 이용한 보안조치 ⑤ 법 제28조제1항제5호에 따라 정보통신서비스 제공자등은 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치하여야 하며, 이를 주기적으로 갱신·점검하여야 한다. ⑥ 방송통신위원회는 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조제1항제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다.

[개인정보의 기술적·관리적 보호조치 기준 개요]

구 분	개인정보의 기술적・관리적 보호조치 기준
목 적	o 정보통신서비스 제공자등이 이용자의 개인정보를 취급함에 있어서 개인정보가 분실・도난・누출・변조・훼손 등이 되지 아니하도록 안전성을 확보하기 위함
관련 근거	o 법 제28조(개인정보의 보호조치) o 법 시행령 제15조(개인정보의 보호조치)
주요 내용	o 이용자의 개인정보가 안전하게 취급되기 위해 내부관리계획의 수립・시행에 관한 조치 o 접근통제 규칙 설정, 침입차단시스템 및 침입탐지시스템의 설치・운영, 외부 인터넷망 차단 등 이용자의 개인정보에 대한 불법적인 접근을 차단하기 위한 보호조치 o 개인정보처리시스템에 대한 접속기록의 위조・변조를 방지하기 위한 보호조치 o 이용자의 개인정보를 안전하게 저장・전송하기 위한 조치 o 백신소프트웨어의 설치・운영 등 악성 프로그램의 침투 여부를 항시 점검・치료하기 위한 보호조치 o 기타 개인정보의 안전성 확보를 위해 필요한 보호조치
대상 사업자	o 정보통신서비스 제공자 o 정보통신서비스 제공자로부터 개인정보를 제공받은 자 o 개인정보 수집・취급 등을 위탁받은 자(준용) o 방송사업자(준용)
성 격	o 반드시 준수해야 하는 최소한의 기준
행정처분 및 벌칙	o 3천만원 이하의 과태료(법 제76조제1항제3호) o 1억원 이하의 과징금(법 제64조의3제1항제6호) o 2년 이하의 징역 또는 1천만원 이하의 벌금(법 제73조제1호)

개인정보의 기술적·관리적 보호조치 기준 해설서

II. 개인정보 기술적·관리적 보호조치 기준

Ⅱ. 개인정보의 기술적·관리적 보호조치 기준

방송통신위원회 고시 제2012-50호(2012. 8. 23.)

제1조(목적) 이 기준은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) 제28조제1항 및 같은 법 시행령 제15조제6항에 따라 정보통신서비스 제공자등이 이용자의 개인정보를 취급함에 있어서 개인정보가 분실·도난·누출·변조·훼손 등이 되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 기술적·관리적 보호조치의 구체적인 기준을 정하는 것을 목적으로 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보관리책임자"라 함은 정보통신서비스 제공자의 사업장 내에서 이용자의 개인정보보호 업무를 총괄하거나 업무처리를 최종 결정하는 임직원을 말한다.
2. "개인정보취급자"라 함은 정보통신서비스 제공자의 사업장 내에서 이용자의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.
3. "내부관리계획"이라 함은 정보통신서비스 제공자등이 개인정보의 안전한 취급을 위하여 개인정보보호 조직의 구성, 개인정보취급자의 교육, 개인정보 보호조치 등을 규정한 계획을 말한다.
4. "개인정보처리시스템"이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.
5. "망분리"라 함은 외부 인터넷망을 통한 불법적인 접근과 내부정보 유출을 차단하기 위해 업무망과 외부 인터넷망을 분리하는 망 차단조치를 말한다.
6. "비밀번호"라 함은 이용자 및 개인정보취급자 등이 시스템 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
7. "접속기록"이라 함은 이용자 또는 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
8. "바이오정보"라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
9. "P2P(Peer to Peer)"라 함은 정보통신망을 통해 서버의 도움 없이 개인과 개인이

직접 연결되어 파일을 공유하는 것을 말한다.

10. “공유설정”이라 함은 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것을 말한다.
11. “보안서버”라 함은 정보통신망에서 송・수신하는 정보를 암호화하여 전송하는 웹서버를 말한다.
12. “인증정보”라 함은 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등이 요구한 식별자의 신원을 검증하는데 사용되는 정보를 말한다.

제3조(내부관리계획의 수립・시행) ① 정보통신서비스 제공자등은 다음 각 호의 사항을 정하여 개인정보 보호 조직을 구성・운영하여야 한다.

1. 개인정보관리책임자의 자격요건 및 지정에 관한 사항
2. 개인정보관리책임자와 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보 내부관리계획의 수립 및 승인에 관한 사항
4. 개인정보의 기술적・관리적 보호조치 이행 여부의 내부 점검에 관한 사항
5. 그 밖에 개인정보보호를 위해 필요한 사항

② 정보통신서비스 제공자등은 다음 각 호의 사항을 정하여 개인정보관리책임자 및 개인정보취급자를 대상으로 매년 2회 이상 교육을 실시하여야 한다.

1. 교육목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

③ 정보통신서비스 제공자등은 제1항 및 제2항에 대한 세부 계획, 제4조부터 제8조까지의 보호조치 이행을 위한 세부적인 추진방안을 포함한 내부관리계획을 수립・시행하여야 한다.

제4조(접근통제) ① 정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여한다.

② 정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.

③ 정보통신서비스 제공자등은 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다.

④ 정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 공인인증서 등 안전한 인증 수단을 적용하여야 한다.

⑤ 정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

⑥ 정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 한다.

⑦ 정보통신서비스 제공자등은 이용자가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성규칙을 수립하고, 이행한다.

⑧ 정보통신서비스 제공자등은 개인정보취급자를 대상으로 다음 각 호의 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 한다.

1. 다음 각 목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성
   가. 영문 대문자(26개)
   나. 영문 소문자(26개)
   다. 숫자(10개)
   라. 특수문자(32개)
2. 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고
3. 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경

⑨ 정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 한다.

제5조(접속기록의 위·변조방지) ① 정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리하여야 한다.

② 단, 제1항의 규정에도 불구하고 「전기통신사업법」 제5조의 규정에 따른 기간통신사업자의 경우에는 보존·관리해야할 최소 기간을 2년으로 한다.

③ 정보통신서비스 제공자등은 개인정보취급자의 접속기록이 위·변조되지 않도록 별도의 물리적인 저장 장치에 보관하여야 하며 정기적인 백업을 수행하여야 한다.

제6조(개인정보의 암호화) ① 정보통신서비스 제공자등은 비밀번호 및 바이오정보는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.

② 정보통신서비스 제공자등은 주민등록번호, 신용카드번호 및 계좌번호에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다.

③ 정보통신서비스 제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호 중 하나의 기능을 갖추어야 한다.

1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능
2. 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능

④ 정보통신서비스 제공자등은 이용자의 개인정보를 개인용컴퓨터(PC)에 저장할 때에는 이를 암호화해야 한다.

제7조(악성프로그램 방지) 정보통신서비스 제공자등은 백신 소프트웨어를 월 1회 이상 주기적으로 갱신·점검하고, 악성 프로그램관련 경보가 발령된 경우 및 백신소프트웨어 또는 운영체제 제작업체에서 업데이트 공지가 있는 경우에는 응용프로그램과 정합성을 고려하여 최신 소프트웨어로 갱신·점검하여야 한다.

제8조(출력·복사시 보호조치) ① 정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화 한다.

② 정보통신서비스 제공자등은 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등 필요한 보호조치를 갖추어야 한다.

제9조(개인정보 표시 제한 보호조치) 정보통신서비스 제공자 등은 개인정보 업무처리를 목적으로 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보보호를 위하여 개인정보를 마스킹하여 표시제한 조치를 취하는 경우에는 다음의 원칙으로 적용할 수 있다.

1. 성명 중 이름의 첫 번째 글자 이상
2. 생년월일
3. 전화번호 또는 휴대폰 전화번호의 국번
4. 주소의 읍·면·동
5. 인터넷주소는 버전 4의 경우 17~24비트 영역, 버전 6의 경우 113~128비트 영역

제10조(재검토기한)「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 고시 발령 후의 법령이나 현실여건의 변화 등을 검토하여 이 고시의 폐지, 개정 등의 조치를 하여야 하는 기한은 2012년 8월 6일까지로 한다.

부칙<제2012-50호, 2012.8.23.>

이 고시는 2013년 2월 18일부터 시행한다.

개인정보의 기술적·관리적 보호조치 기준 해설서

Ⅲ. 조문별 기준 해설

1. 목적
2. 정의
3. 내부관리계획의 수립・시행
4. 접근통제
5. 접속기록의 위・변조 방지
6. 개인정보의 암호화
7. 악성프로그램 방지
8. 출력・복사시 보호조치
9. 개인정보 표시 제한 보호조치

Ⅲ. 조문별 기준 해설

1. 목적

제1조(목적) 이 기준은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) 제28조제1항 및 같은 법 시행령 제15조제6항에 따라 정보통신서비스 제공자등이 이용자의 개인정보를 취급함에 있어서 개인정보가 분실·도난·누출·변조·훼손 등이 되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 기술적·관리적 보호조치의 구체적인 기준을 정하는 것을 목적으로 한다.

【취 지】

▶ 기준의 근거가 되는 법률·시행령과 목적을 밝히고 있다. 법 제28조 및 같은 법 시행령 제15조제6항에 근거한 기준은 법률과 시행령의 규정을 구체화하여 개인정보가 분실·도난·누출·변조·훼손 등이 되지 아니하도록 안전성을 확보하기 위함임을 밝히고 있다.

【해 설】

▶ 이 기준을 준수하여야 하는 자는 ① 정보통신서비스 제공자, ② 정보통신서비스 제공자로부터 이용자의 개인정보를 제공받은 자, ③ 개인정보의 취급 업무를 위탁받은 자(준용), ④ 방송사업자(준용), ⑤ 다른 법률에서 정보통신망법의 준용을 명시 한 경우이다. 다만, 위의 자에 해당하더라도 이용자의 개인정보를 전혀 수집·이용하지 않는다면 이 기준의 적용대상에서 제외된다.

▶ "정보통신서비스 제공자"는 ① 전기통신사업법에 의한 전기통신사업자(기간·별정·부가통신사업자) 및 ② 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공·매개하는 자를 말한다.

※ "영리를 목적으로 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자"는 인터넷 홈페이지 등을 이용하여 정보 및 서비스를 제공하는 자를 의미하며, 보통 영업행위를 하는 주체가 홈페이지를 개설하고 회원가입을 받는 경우에는 모두 적용 대상이 된다.

- 특히 '영리 목적'은 자기 또는 제3자의 재산적 이익을 얻기 위한 목적을 말하는 것으로 해석하고 있으며 여기서의 이익은 계속적, 반복적일 필요는 없다.

▶ “정보통신서비스 제공자로부터 이용자의 개인정보를 제공받은 자”는 법 제24조의2제1항에 따라 사전에 이용자로부터 제3자 제공에 대한 동의를 받고 정보통신서비스 제공자로부터 개인정보를 제공받은 자를 의미한다.

- 정보통신서비스 제공자와 그로부터 이용자의 개인정보를 제공받은 자를 합하여 “정보통신서비스 제공자등”이라 칭하고 있다(법 제25조제1항).

▶ “방송사업자”는 법 제67조제1항에 따라, 준용사업자로 지정되어 정보통신망법 제22조에서 제32조까지 준용된다.

[보호조치 기준 적용 대상자 일람]

<table>
<tr><td rowspan="7">기준
적용
대상자</td><td rowspan="5">정보통신서비스 제공자등</td><td rowspan="4">정보통신서비스 제공자</td><td rowspan="3">전기통신사업자</td><td>기간통신사업자
(전기통신사업법 제5조제1항)</td><td>음성·데이터 등의 송·수신, 주파수 할당·제공, 전기통신회선설비임대역무 등</td></tr>
<tr><td>별정통신사업자
(전기통신사업법 제19조)</td><td>기간통신사업자의 전기통신회선설비 등을 이용한 기간통신역무제공, 구내전기통신역무 제공 등</td></tr>
<tr><td>부가통신사업자
(전기통신사업법 제21조)</td><td>기간통신사업자의 전기통신회선설비를 임차하여 기간통신역무 외의 전기통신역무 제공</td></tr>
<tr><td colspan="2">영리를 목적으로 전기통신사업자의 전기통신역무를 이용해 정보를 제공하거나 매개하는 자</td><td>인터넷 홈페이지 등을 운영하는 영리를 목적으로 하는 개인사업자</td></tr>
<tr><td colspan="3">정보통신서비스 제공자로부터 법 제24조의2제1항에 따라 이용자의 동의를 얻어 개인정보를 제공받은 자</td><td>업무제휴 등을 위해 이용자의 동의를 얻어 개인정보를 제공받은 자 등</td></tr>
<tr><td colspan="3">방송사업자
(정보통신망법 제67조제1항)</td><td>시청자의 개인정보를 수집·이용 또는 제공하는 자</td></tr>
<tr><td colspan="3">개인정보의 취급업무를 위탁받은 자
(정보통신망법 제25조제1항, 제67조제2항)</td><td>수탁자에 대하여는 법 제28조의 기술적·관리적 보호조치 규정을 준용 적용</td></tr>
<tr><td colspan="3">다른 법률에서 이 법 적용을 받은 자</td><td>다른 법률에서 특별히 규정된 경우
(제7장의 통신과금서비스에 관하여 이 법 우선 적용)</td></tr>
</table>

▶ “수탁자”는 정보통신서비스 제공자등으로부터 ③개인정보의 수집·보관·처리·이용·제공·관리·파기 등의 업무를 위탁받은 자를 말한다(법 제25조제1항).

- 개인정보의 기술적·관리적 보호조치는 정보통신서비스 제공자등 외에도 수탁자에 대해서도 보호조치 내용을 준용하여 적용된다(법 제67조제2항).

▶ 정보통신망법 외의 다른 법률에서 정보통신망법 상의 개인정보보호 의무를 준용할 것을 명시하거나, 정보통신망법의 기준에 따라 공정하게 수집·이용할 것을 규정한 경우가 있다. 이 중에서 “정보통신망법의 준용”이 명시된 경우에는 보호조치 기준 역시 적용되며, 그 외의 경우에도 최대한 정보통신망법의 기준에 따라 보호조치를 이행할 의무가 있다고 해석하여야 할 것이다.

▶ 해당 기준의 적용대상이 되는 정보통신서비스 제공자등, 준용사업자(방송사업자, 수탁자) 등이 해당 기준을 준수하지 않은 경우, 정보통신망법에 따라 처벌받을 수 있다. (동 해설서 p3 참조)

[보호조치 기준 적용 대상 관련 법률]

법률명	주요 내용	보호조치 기준 적용여부
인터넷주소자원에 관한 법률	인터넷주소관리기관 및 인터넷주소관리대행자가 인터넷주소 사용자의 개인정보를 보호하는 경우에는 정보통신망법을 준용(제15조)	○
장애인차별금지 및 권리구제 등에 관한 법률	장애인의 개인정보 수집 및 관리시 개인정보보호법 및 정보통신망법을 준용(제22조)	○
전자문서 및 전자거래기본법	전자거래사업자가 전자거래이용자의 개인정보를 수집·이용·관리하는 경우 정보통신망법을 준수(제12조)	○
전자상거래 등에서의 소비자보호에 관한 법률	사업자가 전자상거래·통신판매를 위해 소비자의 정보를 수집·이용하는 경우 정보통신망법에 따라 공정하게 수집·이용(제11조)	○
방문판매 등에 관한 법률	특수판매업자가 소비자에 관한 정보를 수집·이용하는 경우 정보통신망법에 따라 공정하게 수집·이용(제55조)	○

【FAQ】

[문1] 부가통신사업자로 신고를 하였지만 부가통신사업 중에 특별히 개인정보를 수집하고 있지는 않습니다. 대신 오프라인으로 컴퓨터를 판매하는 과정에서 고객의 정보를 수집하고 있습니다. 이런 경우에도 보호조치 기준을 이행하여야 합니까?

▶ 부가통신사업자로 신고하여 "정보통신서비스 제공자등"의 범위에 속하는 전기통신사업자에 해당한다면 오프라인으로 수집·운용되는 개인정보라 하더라도 이 보호조치 기준 적용 대상이 됩니다.

[문2] 홈페이지를 운영하고 있지 않는 여행사입니다. 그렇지만 여행상품 계약 등을 위해 고객의 개인정보를 수집하고 있습니다. 오프라인으로 개인정보를 수집하고 있기 때문에 이 보호조치 기준을 이행하지 않아도 된다고 생각되는데요.

▶ 정보통신망을 이용하여 서비스를 제공하고 있지 않은 사업자의 경우 본 고시 및 해설서의 적용대상이 되지는 않으나, 「개인정보보호법」에 따라 행정안전부장관이 정한 '개인정보의 안전성 확보조치 기준'에 따른 보호조치를 하여야 합니다.

[문3] 회사 내부에서 직원의 관리 등을 위해서만 사용하는 시스템의 경우도 보호조치 기준의 적용대상에 해당 됩니까?

▶ 전기통신사업자의 전기통신역무를 이용하여 고객에게 정보를 제공하거나 정보의 제공을 매개하지 않고 내부에서만 직원관리 용도 등으로 사용하는 경우에는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 적용대상에 해당되지 않습니다. 이 경우는 「개인정보보호법」 적용 대상이 됩니다. 「개인정보보호법」은 개인정보를 수집, 이용 제공 등 처리하는 모든 자(공공기관, 법인, 단체, 개인 등)에 적용되는 일반법입니다.

[문4] 금융업종에서 개인정보보호와 관련하여 준수하여야 하는 법 규정 범위가 어디까지인지, 법에 있는 내용을 준수하여야 하는지요? (정보통신서비스 제공자등에 포함되는지 여부)

▶ 금융업종에 속하는 사업자의 경우 우선적으로 「신용정보의 이용 및 보호에 관한 법률」의 적용을 받습니다. 다만, 해당 사업자가 인터넷 홈페이지 등을 이용하여 정보 및 서비스를 제공하는 경우에는 영리를 목적으로 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자에 해당하므로 「신용정보의 이용 및 보호에 관한 법률」에서 규정하지 않은 사항에 한해서 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 적용 대상이 됩니다.

[문5] 당사는 자동차판매회사로서 고객정보가 취득되는 경로를 보면 당사 차량 구입고객정보, 오토카드, 정비고객, 영업사원 취득정보, 홈페이지 회원 정보, 이벤트 참여고객 등으로 나누어지는데 금번 보호조치 기준을 이행하여야 하는 고객정보는 홈페이지 회원 정보만 해당되는 건가요?

▶ 자동차 판매회사는 「개인정보보호법」에 따라 행정안전부장관이 정한 '개인정보의 안전성 확보조치 기준'을 적용받습니다. 다만, 인터넷 홈페이지를 통해 서비스를 제공하는 부분에 대해서는 "영리를 목적으로 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자(정보통신서비스 제공자 등)"로 보아 본 고시 및 해설서의 적용대상에 해당됩니다.

2. 정의

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. “개인정보관리책임자”라 함은 정보통신서비스 제공자의 사업장 내에서 이용자의 개인정보보호 업무를 총괄하거나 업무처리를 최종 결정하는 임직원을 말한다.
2. “개인정보취급자”라 함은 정보통신서비스 제공자의 사업장 내에서 이용자의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.
3. “내부관리계획”이라 함은 정보통신서비스 제공자등이 개인정보의 안전한 취급을 위하여 개인정보보호 조직의 구성, 개인정보취급자의 교육, 개인정보 보호조치 등을 규정한 계획을 말한다.
4. “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.
5. “망분리”라 함은 외부 인터넷망을 통한 불법적인 접근과 내부정보 유출을 차단하기 위해 업무망과 외부 인터넷망을 분리하는 망 차단조치를 말한다.
6. “비밀번호”라 함은 이용자 및 개인정보취급자 등이 시스템 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
7. “접속기록”이라 함은 이용자 또는 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
8. “바이오정보”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
9. “P2P(Peer to Peer)”라 함은 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.
10. “공유설정”이라 함은 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것을 말한다.
11. “보안서버”라 함은 정보통신망에서 송・수신하는 정보를 암호화하여 전송하는 웹서버를 말한다.
12. “인증정보”라 함은 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등이 요구한 식별자의 신원을 검증하는데 사용되는 정보를 말한다.

【취 지】

▶ 기준에서 정의 조항을 별로로 두는 이유는 법 제2조(정의)에서 정의한 용어 이외에 같은 법 시행령과 「개인정보의 기술적·관리적 보호조치 기준」의 신규 용어에 대한 해석상의 혼란을 방지하기 위함이다.

【해 설】

1. "개인정보관리책임자"라 함은 정보통신서비스 제공자의 사업장 내에서 이용자의 개인정보보호 업무를 총괄하거나 업무처리를 최종 결정하는 임직원을 말한다.

▶ 법 제27조와 시행령 제13조에 따라 개인정보관리책임자의 지정범위는 임원, 개인정보와 관련하여 이용자의 고충처리를 담당하는 부서의 장 또는 대표자(개인정보관리책임자를 지정하지 않아도 되는 소규모 사업자) 로 제한된다. 이와 같은 지위를 갖는 자가 개인정보보호 업무를 총괄하거나 업무처리를 최종 결정하도록 정하고 있는 것은 사내의 중요 의사결정을 수행하는 중역으로서 개인정보보호 요구사항을 적극적으로 반영할 수 있도록 하기 위함이다.

2. "개인정보취급자"라 함은 정보통신서비스 제공자의 사업장 내에서 이용자의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.

▶ 업무를 하는 자가 서비스 제공을 위해 개인정보처리시스템에 접속하여 이용자의 개인정보를 조회할 수 있는 권한만을 갖고 있다고 하더라도 개인정보취급자에 포함된다.

▶ 시스템(데이터베이스 포함) 운영자와 정보보호담당자 등이 업무 수행을 위해 개인정보를 취급할 경우 개인정보취급자에 포함시켜야 한다. 또한, 서비스 개발 또는 개선과 관련한 테스트 시 우선적으로 가상 데이터를 활용하는 것이 바람직하나, 반드시 실제 데이터가 필요하여 이용자의 개인정보를 식별할 수 없는 형태로 변환하여 사용하는 경우가 발생할 수 있다. 이 경우, 변환된 정보를 제공받아 테스트하는 개발자는 개인정보취급자에 포함되지 않으나, 개인정보를 변환하여 개발자에게 제공하는 자는 개인정보취급자에 포함된다.

▶ 개인정보취급자의 지정과 함께 중요하게 고려할 사항은 지정된 개인정보취급자가 개인정보보호 의무를 다하도록 하는 것이다.

3. “내부관리계획”이라 함은 정보통신서비스 제공자등이 개인정보의 안전한 취급을 위하여 개인정보보호 조직의 구성, 개인정보취급자의 교육, 개인정보 보호조치 등을 규정한 계획을 말한다.

▶ 정보통신서비스 제공자등은 개인정보취급자의 개인정보의 분실・도난・누출・변조 또는 훼손을 방지하기 위해 내부관리계획을 수립하여야 한다. 내부관리계획에는 개인정보보호 조직의 구성, 개인정보취급자의 교육, 개인정보 보호조치 등에 대한 내용을 포함하여야 한다.

4. “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 말한다.

▶ 개인정보처리시스템은 법 시행령 제15조제2항제1호에 따라 개인정보를 보관・처리하기 위한 시스템이다. 일반적으로 체계적인 데이터 처리를 위해 DBMS (Database Management System)를 사용하고 있으나, 이용자의 개인정보 보관・처리를 위해 파일처리시스템 등으로 구성한 경우 개인정보처리시스템에 포함시키는 것이 타당하다.

5. “망분리”라 함은 외부 인터넷망을 통한 불법적인 접근과 내부정보 유출을 차단하기 위해 업무망과 외부 인터넷망을 분리하는 망 차단조치를 말한다.

▶ ‘불법적인 접근’이라 함은 인가되지 않은 자가 계정탈취, 자료유출 등의 목적으로 개인정보취급자의 컴퓨터 등에 접근하는 것을 뜻한다.

▶ ‘업무망과 외부 인터넷망을 분리하는 망 차단조치’라 함은 업무망과 외부 인터넷망을 분리하여 두 영역이 서로 접근할 수 없도록 차단하는 것을 의미한다.

▶ 망분리 방법에는 물리적 망분리와 논리적 망분리가 있다. 물리적 망분리는 통신망, 장비 등을 이원화하여 업무망과 외부 인터넷망의 접근 경로를 단절시키는 것을 말한다. 논리적 망분리는 물리적으로 하나의 통신망, 장비 등을 사용하지만 가상화 등의 방법으로 서로 접근할 수 없도록 분리하는 것이다.

6. “비밀번호”라 함은 이용자 및 개인정보취급자 등이 시스템 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

▶ 이용자 및 개인정보취급자 등이 시스템 또는 정보통신망에 접속할 때 사용하는 식별자는 소유자 식별을 위한 목적의 ID, 사용자이름, 사용자 계정명 등을 말한다. ‘시스템에 전달해야 하는 고유의 문자열’은 영문 대문자(A~Z), 소문자(a~z), 숫자(0~9), 특수문자(~ · ! @ # $ % ^ & * ( ) _ - + = { } [ ] | \ ; : ‘ “ < > , . ? /) 중 2가지 이상을 조합하여 구성한 문자열을 의미한다.

▶ ‘타인에게 공개되지 않는 정보’의 의미는 개인정보취급자 중 계정관리자라 할지라도 이용자 및 개인정보취급자의 비밀번호를 알 수 있는 형태로 관리되어서는 안 된다는 것이다. 비밀번호가 알 수 있는 형태로 관리되는 경우 해당 정보에 접근할 수 있는 관리 담당자에 의한 도용이 가능하기 때문이다. 이와 관련하여 제6조제1항은 비밀번호를 복호화되지 않게 일방향 암호화하도록 규정하고 있다.

▶ 비밀번호의 안전성은 컴퓨터의 성능 향상, 해킹 기술 발달 등에 따라 주기적으로 검토되어야 하고, 비밀번호의 길이는 시간이 지남에 따라 길어지고, 변경 주기는 짧아지게 된다.

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

▶ ‘접속하여 수행한 업무 내역’이라 함은 이용자 또는 개인정보취급자가 개인정보처리시스템을 이용하여 수행한 업무를 알 수 있는 정보이다. 이용자 측면에서는 자신의 개인정보 조회, 수정, 탈퇴 등의 업무를 의미한다. 개인정보취급자 측면에서는 이용자의 개인정보를 서비스 제공을 위해 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 의미한다.

▶ ‘식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등’은 접속한 사실을

확인하는데 사용되는 정보이다. 식별자는 접근자의 ID 또는 계정명이 해당되며, 접속일시는 접속한 시점 또는 업무를 수행한 시점의 "xxxx년 xx월 xx일 xx시 xx분 xx초"에 대한 정보이다. 접속지를 알 수 있는 정보는 개인정보처리시스템에 접속한 자의 PC 또는 서버의 IP 주소를 의미한다. 수행업무는 개인정보에 대한 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등을 확인할 수 있도록 기호로 표기한 정보이다.

▶ '전자적으로 기록한 것'의 의미는 개인정보취급자가 수기로 작성한 문서가 아니라 시스템 로그와 같이 자동적으로 기록된 정보를 의미한다.

▶ 접속기록은 최근 해킹에 의한 침해 또는 개인정보취급자의 권한 남용 등이 발생한 경우 신속하게 대응하기 위해 활용되는 가장 중요한 정보이다. 따라서 정보통신서비스 제공자등은 접속기록이 위·변조되지 않도록 관리 및 보관하는 절차를 마련하여야 한다.

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

▶ 지문, 얼굴, 홍채, 정맥, 음성, 필적은 개인을 식별할 수 있는 신체적 특징과 행동적 특징의 예를 든 것으로 이에 한정되지는 않는다.
- 신체적 특징 : 지문, 얼굴, 홍채, 정맥, 음성, 망막, 손 모양, 손가락 모양, 열상 등
- 행동적 특징 : 필적, 키보드 타이핑, 입술 움직임, 걸음걸이 등

※ 유전자(DNA)를 이용한 개인식별에 대해서는 「생명윤리 및 안전에 관한 법률」이 적용됨

▶ '개인을 식별할 수 있는'의 의미는 특정 개인을 다른 사람과 구별할 수 있다는 것(Identification)이다. 또한, 바이오정보는 개인에 따라 고유의 특성을 가지므로 개인을 특정지어 본인임을 인증(Authentication)하는 수단으로 활용되고 있다.

▶ 바이오정보는 사람의 신체적 또는 행동적 특징을 입력장치를 통해 최초로 수집되어 가공되지 않은 '원본정보'와 그 중 특정 알고리듬을 통해 특징만이 추출, 생성된 '특징정보'로 구분된다.

9. “P2P(Peer to Peer)”라 함은 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.

▶ ‘정보통신망을 통해 서버의 도움 없이’는 기존의 서비스가 공급자와 소비자, 서버와 클라이언트 등의 주종관계나 상하관계를 벗어나 참여자 모두가 참여하는 동등한 관계를 의미한다.

▶ ‘개인이 직접 연결되어’는 파일을 보유하고 있는 참여자와 파일을 갖고자 하는 참여자가 직접 연결된 상태를 의미한다.

10. “공유설정”이라 함은 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것을 말한다.

▶ ‘컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록’의 의미는 컴퓨터 소유자가 파일을 사용하는 시간이 다르므로 타인이 해당 파일을 조회, 변경, 복사 등을 할 수 있도록 설정하는 것이다.

11. “보안서버”라 함은 정보통신망에서 송·수신하는 정보를 암호화하여 전송하는 웹서버를 말한다.

▶ 보안서버는 인터넷상에서 사용자 PC와 웹서버 사이에 송·수신되는 개인정보를 암호화하여 전송하는 서버를 의미한다. 또한, 보안서버는 해당 전자거래업체의 실존을 증명하여 사용자와 웹서버간의 신뢰를 형성하고, 웹브라우저와 웹서버 간에 전송되는 데이터의 암·복호화를 통하여 보안채널을 형성한다.

12. “인증정보”라 함은 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등이 요구한 식별자의 신원을 검증하는데 사용되는 정보를 말한다.

▶ ‘시스템 등이 요구한 식별자’는 해당 시스템에 접속하여 업무를 수행하기 위해서 시스템에게 알려주어야 하는 계정 또는 ID 등의 정보로서, 시스템에 등록 시 이용자가 선택하거나 또는 계정(또는 권한) 관리자가 부여한 고유한 문자열이다.

▶ ‘신원을 검증하는데 사용되는 정보’는 해당 시스템에서 업무를 수행할 수 있는 권한을 갖고 있음을 시스템에게 증명하기 위하여 식별자와 연계된 정보로서 비밀번호, 바이오정보, 전자서명값 등이 있다.

3. 내부관리계획의 수립・시행

제3조(내부관리계획의 수립・시행) ① 정보통신서비스 제공자등은 다음 각 호의 사항을 정하여 개인정보 보호 조직을 구성・운영하여야 한다.

1. 개인정보관리책임자의 자격요건 및 지정에 관한 사항
2. 개인정보관리책임자와 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보 내부관리계획의 수립 및 승인에 관한 사항
4. 개인정보의 기술적・관리적 보호조치 이행 여부의 내부 점검에 관한 사항
5. 그 밖에 개인정보보호를 위해 필요한 사항

② 정보통신서비스 제공자등은 다음 각 호의 사항을 정하여 개인정보관리책임자 및 개인정보취급자를 대상으로 매년 2회 이상 교육을 실시하여야 한다.

1. 교육목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

③ 정보통신서비스 제공자등은 제1항 및 제2항에 대한 세부 계획, 제4조부터 제8조까지의 보호조치 이행을 위한 세부적인 추진방안을 마련하여야 한다.

【취 지】

▶ 이용자의 개인정보를 보호하기 위한 조치를 적절히 시행하기 위해서는 회사 전체에 통용되는 내부규정이 필요하다. 이를 기초로 세부 지침이나 안내서를 마련하여 사원 전원이 동일한 행동을 취할 수 있도록 할 필요가 있다.

▶ 정보통신서비스 제공자등은 취급하는 개인정보가 분실・도난・누출・변조 또는 훼손되지 아니하도록 안전성을 확보하기 위하여 개인정보보호 활동에 대한 조직 내부의 개인정보 관리계획을 수립하고 모든 임직원 및 관련자에게 알림으로써 이를 준수할 수 있도록 하여야 한다.

- 이와 같이 내부관리계획을 수립하도록 하는 이유는 개인정보보호 활동이 임기응변식이 아니라 체계적이고 전사적인 계획 내에서 수행될 수 있도록 하는데 목적이 있으며, 이를 위해서는 전사차원의 방향제시와 지원이 필수적이다.

【해 설】

① 정보통신서비스 제공자등은 다음 각 호의 사항을 정하여 개인정보 보호 조직을 구성·운영하여야 한다.

▶ 내부관리계획에는 개인정보 보호 조직의 구성 및 운영에 관한 다음과 같은 사항을 포함하여야 한다.

- 개인정보관리책임자의 자격요건 및 지정에 관한 사항
- 개인정보관리책임자와 개인정보취급자의 역할 및 책임에 관한 사항
- 개인정보 내부관리계획의 수립 및 승인에 관한 사항
- 개인정보의 기술적·관리적 보호조치 이행 여부의 내부 점검에 관한 사항
- 그 밖에 개인정보보호를 위해 필요한 사항

1. 개인정보관리책임자의 자격요건 및 지정에 관한 사항

▶ 개인정보관리책임자의 자격요건

- 원칙적으로 시행령 제13조에 따라 임원의 지위에 해당하는 개인정보관리책임자(CPO: Chief Privacy Officer) 직제를 신설하거나, 이용자의 개인정보 보호 업무를 위해 조직된 부서의 장 등을 지정할 수 있다.

- 또는, 정보통신서비스 제공자등의 사업 환경에 따라 이용자의 개인정보를 주로 활용하는 업무를 수행하는 부서(고객 응대, 마케팅, 경영지원 등)나 정보보호 업무를 수행하는 부서에서 본연의 업무와 동시에 개인정보와 관련된 이용자의 고충처리를 담당하게 되는 경우 해당 부서의 장이 개인정보관리책임자로 지정될 수 있다. 만약 본연의 사업(마케팅 등) 업무와 개인정보보호 업무 간에 충돌이 발생할 경우 개인정보관리책임자는 우선적으로 개인정보보호에 무게를 두는 것이 바람직하다.

- 조직 내에 정보보호(Security) 업무를 총괄하는 정보보호책임자(CSO : Chief Security Officer)가 별도로 있는 경우에는 기술적 조치에 관하여 상호간의 업무를 분명하게 분장하여야 한다. 정보통신서비스 제공자등은 개인정보관리책임자와 정보보호책임자로 동일인을 지정할 수 있으나, 개인정보관리책임자의 효과적인 업무수행을 위해 가급적 별도로 지정하는 것을 권장한다.

- 개인정보관리책임자는 정보보안 관련 지식뿐만 아니라 개인정보 취급에 관한 법·제도적인 측면 등의 다양한 지식을 습득할 필요가 있다.

※ 관련 법규 : 법 시행령 제13조

(개인정보관리책임자의 자격요건 등) ① 정보통신서비스 제공자와 그로부터 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)가 법 제27조제1항 본문에 따라 지정하는 개인정보관리책임자는 다음 각 호의 어느 하나에 해당하는 지위에 있는 자로 하여야 한다. <개정 2009.1.28>

1. 임원
2. 개인정보와 관련하여 이용자의 고충처리를 담당하는 부서의 장

② 법 제27조제1항 단서에서 "대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자등"이란 상시 종업원 수가 5명 미만인 정보통신서비스 제공자등을 말한다. 다만, 인터넷으로 정보통신서비스를 제공하는 것을 주된 업으로 하는 정보통신서비스 제공자등의 경우에는 상시 종업원 수가 5명 미만으로서 전년도 말 기준으로 직전 3개월간의 일일평균이용자가 1천명 이하인 자를 말한다. <개정 2009.1.28>

▶ 개인정보관리책임자의 지정

- 정보통신서비스 제공자등은 임원 또는 담당부서의 장 중 최소 1인을 개인정보관리책임자로 지정하여야 한다. 개인정보관리책임자의 지정 시에는 인사발령 등을 통해 공식적으로 책임과 역할을 부여하는 것이 바람직하다.

- 다만, ①인터넷으로 정보통신서비스를 제공하는 것을 주된 업으로 하지 않는 경우 상시종업원 수가 5명 미만이거나 ②인터넷으로 정보통신서비스를 제공하는 것이 주된 업으로써 상시종업원 수가 5명 미만이고 전년도 말 기준으로 직전 3개월간의 일일평균이용자가 1천명 이하인 자의 경우에는 개인정보관리책임자를 지정하지 않을 수 있는데, 이 경우에는 사업주 또는 대표자가 개인정보관리책임자가 된다.

※ 관련 법규 : 법 제27조

(개인정보 관리책임자의 지정) ① 정보통신서비스 제공자등은 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보 관리책임자를 지정하여야 한다. 다만, 종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자등의 경우에는 지정하지 아니할 수 있다.

② 제1항 단서에 따른 정보통신서비스 제공자등이 개인정보 관리책임자를 지정하지 아니하는 경우에는 그 사업주 또는 대표자가 개인정보 관리책임자가 된다.

③ 개인정보 관리책임자의 자격요건과 그 밖의 지정에 필요한 사항은 대통령령으로 정한다.[전문개정 2008.6.13]

※ 미이행 시 법 제76조제2항제3호에 따라 2천만원 이하의 과태료가 부과됨

2. 개인정보관리책임자와 개인정보취급자의 역할 및 책임에 관한 사항

▶ 개인정보관리책임자의 역할 및 책임

- 개인정보관리책임자는 사내의 개인정보보호에 관한 업무를 총괄하는 역할을 한다.
- 개인정보관리책임자는 개인정보와 관련된 내부지침을 준수하도록 충분한 기술적·관리적 보호조치를 실시하여야 한다. 개인정보관리책임자는 내부규정의 정비, 기술적·관리적 보호조치의 실시 등의 업무를 수행하게 된다.
- 또한, 이용자의 불만사항 접수 및 처리에 대한 책임을 지게 되며, 개인정보를 취급하는 직원에 대해 충분한 교육훈련을 실시하여야 한다. 개인정보를 취급하는 업무를 외부에 위탁하는 경우, 개인정보관리책임자는 해당 업무를 위탁받은 자의 개인정보 관리상황을 지속적으로 확인해야 한다.

[개인정보관리책임자의 역할 및 책임]

- 개인정보보호조직 구성·운영의 총괄
- 내부관리계획의 수립 및 승인
- 개인정보의 기술적·관리적 보호조치 기준 이행 총괄
- 소속 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검
- 정보주체로부터 제기되는 개인정보에 관한 고충이나 의견의 처리 및 감독
- 임직원, 개인정보취급자 및 수탁자, 대리점 등에 대한 교육 등 인식제고
- 그 밖에 정보주체의 개인정보보호에 필요한 사항

▶ 개인정보취급자의 역할 및 책임

- 개인정보취급자는 업무 상 또는 서비스 제공을 위해 이용자의 개인정보를 취급(수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등)하는 역할을 한다.

[개인정보취급자의 역할 및 책임]

- 개인정보보호 활동 참여
- 내부관리계획의 준수 및 이행
- 개인정보의 기술적·관리적 보호조치 기준 이행
- 소속 직원 또는 제3자에 의한 위법·부당한 개인정보 침해행위에 대한 점검 등

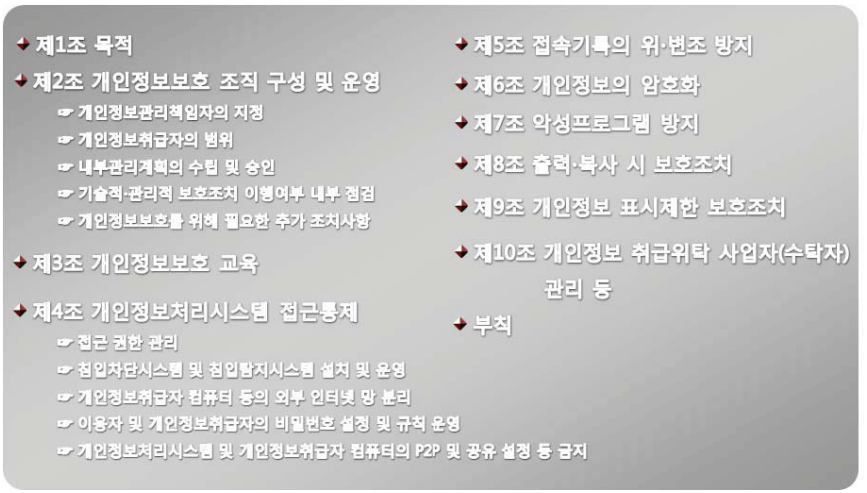
- 개인정보취급자는 고객정보를 이용한 마케팅, 고객상담, 개인정보처리시스템의 관리 등 개인정보를 취급하는 모든 자가 해당되며, 개인정보에 대한 제한적인 권한만을 가지고 있더라도 개인정보취급자에 해당된다. 이는 정규직 이외에 임시직·계약직원 등도 동일하게 적용된다.

3. 개인정보 내부관리계획의 수립 및 승인에 관한 사항

▶ 내부관리계획의 수립 및 승인

- 개인정보 내부관리계획의 수립은 개인정보취급자와 개인정보관리책임자가 이용자의 개인정보를 어떻게 관리할 것인지에 관한 규정 문서를 작성하는 과정이라 할 수 있다.

[개인정보 내부관리계획 목차(예시)]



- 내부관리계획은 법률에서 규정한 사항을 그대로 반영하는 것이 아니라, 해당 기업의 개인정보 정책의 수립·운용되는 사항을 명시하는 것이 타당하다. 또한, 수탁업체도 수탁하는 개인정보의 내부관리계획을 수립하여야 한다.

- 내부관리계획의 승인에 관한 내용과 이에 대한 주기적인 검토 방법에 관한 내용이 포함되어야 한다. 예를 들면 내부관리계획의 승인에 관한 내용은 '내

부관리계획은 ○○회사 개인정보관리책임자의 승인을 거쳐 ○○회사 전 임직원에게 공표한다'와 같이 규정하고, 내부관리계획의 주기적인 검토는 '연 1회 이상 타당성 등을 검토하여 수정·보완한다'와 같은 명시적 내용을 포함하여 주기적으로 관리한다.

4. 개인정보의 기술적·관리적 보호조치 이행 여부의 내부 점검에 관한 사항

▶ **기술적·관리적 보호조치 이행 여부의 내부 점검**

- 개인정보취급자가 "내부관리계획" 등에 따라 적절하게 개인정보 보호조치를 이행하고 있는 지를 파악할 수 있도록 정기적(최소 연 1회 권고)으로 점검한다. 그리고 "내부관리계획"을 위반한 사항을 발견한 때에는 곧바로 필요한 조치를 취하고 이러한 사실을 문서화하여 보관하는 것이 바람직하다.
- 정보통신서비스 제공자등은 개인정보의 기술적·관리적 보호조치 이행 여부의 내부 점검 방법에 관하여 내부관리계획에 '점검방법, 점검반 구성, 점검절차 및 결과 자료 관리 등'의 내용을 포함하도록 한다.
- 점검방법에는 점검시기, 대상, 내용 등을 포함하고, 점검반에는 정보통신서비스 제공자등의 사업장 내에 개인정보보호 관련 부서의 감사자 또는 유관 부서의 전문가로 구성할 수 있고, 점검절차에는 범위, 대상, 기간, 점검수행자 등의 내용과 점검결과를 어떻게 처리할 것인지의 내용을 포함하여야 한다.
- 점검결과 자료의 관리는 시스템 점검결과 요약, 화면 덤프 내역, 시스템 로그 및 수집한 증거자료 등 점검 시 생성된 모든 자료와 결과보고서를 관리하는 것을 의미한다. 점검결과 자료에 대한 접근은 점검반으로 제한하여 자료의 무결성을 보장하여야 한다.

5. 그 밖에 개인정보보호를 위해 필요한 사항

▶ 기타 개인정보보호를 위하여 필요한 사항으로는 보안서약서 작성, 개인정보보호 정책의 수립, 중고 PC 하드디스크 복구로 인한 개인정보 노출 대책 등이 있을 수 있다.

▶ 보안서약서 작성

- 조직에서 임직원들의 기밀정보 유출 위험을 최소화하고, 임직원에게 개인정보 보호에 대한 책임을 명확히 주지시키기 위해 문서화한 보안서약서에 서명하도록 한다.
- 보안서약서의 서명은 개인정보보호를 위한 기본적인 절차 중 하나로 인식되고 이행될 필요가 있다. 이러한 절차는 일반적으로 신규 인력 채용 시 인력관리 부서에 의해 수행될 수 있다.
- 보안서약서에는 일반적으로 '고객 개인정보 보호, 회사 영업비밀 보호 등의 의무'에 관한 내용과 서명날짜, 서명자 정보 및 서명을 포함하여야 한다.

▶ 임직원 개인정보보호 인식제고

- 임직원들의 개인정보보호 인식제고를 위해 개인정보보호 관련 정보, 개인정보 보호 실천수칙 등과 같은 관련 지침 및 규정을 배포하고 알림으로써 이를 준수할 수 있도록 한다.
- 개인정보보호 관련 지침 및 규정에 대한 수정·보완이 필요한 경우에는 정해진 절차에 따라 변경관리가 이루어질 수 있도록 하며, 개정된 내용을 임직원들이 즉시 주지할 수 있도록 한다.

▶ 중고 PC 하드디스크 복구로 인한 개인정보 누출 대책

- 파일을 삭제하거나 하드디스크를 포맷한 후 중고 PC로 매매하는 경우가 종종 있으나, 파일 삭제 또는 하드디스크 포맷만으로는 데이터 영역이 완전하게 삭제되지 않고 복구될 수 있다. 만약 중고 PC에 전 이용자의 신용카드 번호, 주민등록번호 등 민감한 개인정보가 남아있을 경우, 중고 PC 이용자에 의한 개인정보 오·남용의 위험성이 있으므로 이를 방지하기 위한 조치가 필요하다.
- 일반적으로 데이터를 삭제하는 경우, 사용자 환경에서 데이터가 없는 것으로 보이지만 실제로 저장되었던 공간에 데이터가 그대로 남아 있다. 따라서, 저장매체에 저장된 개인정보가 복구되지 않도록 영구삭제 하기 위한 조치를 하여야 한다. 데이터의 영구삭제 방법에는 완전파괴, 전용 소자장비 이용, 완전포맷 3회 수행 등이 있다.

  · 완전파괴(소각, 파쇄, 용해) : 물리적으로 저장매체를 파괴
  · 전용 소자장비 이용 : 소자장비의 자기력을 이용하여 저장매체의 자성 소거
  · 완전포맷 3회 : 저장매체 전체에 난수, 0, 1 덧쓰기 수행

- 또한, 이를 지원해 주는 다수의 제품에 대해 검증을 실시하여 검증필 제품 정보를 제공하고 있다.

※ 국가정보원 IT보안인증사무국 홈페이지(service1.nis.go.kr - IT 보안인증 사무국 - 보안적합성 검증 - 검증필 제품 목록 - 데이터 영구삭제(제품유형))에서 확인 가능하다.

▶ 개인정보 취급 위탁업체의 관리

- 개인정보 위탁시 계약서에 취급목적, 업무범위, 보안필요사항 등을 명시하여 개인정보 보호대책을 마련하는 것이 좋으며, 수탁자가 개인정보보호 관련 의무를 위반하지 않도록 관리·감독할 책임이 있다.

※ 관련 법규 : 법 제25조(개인정보의 취급위탁)

제25조(개인정보의 취급위탁) ① 정보통신서비스 제공자와 그로부터 제24조의2제1항에 따라 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)는 제3자에게 이용자의 개인정보를 수집·보관·처리·이용·제공·관리·파기 등(이하 "취급"이라 한다)을 할 수 있도록 업무를 위탁(이하 "개인정보 취급위탁"이라 한다)하는 경우에는 다음 각 호의 사항 모두를 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

1. 개인정보 취급위탁을 받는 자(이하 "수탁자"라 한다)
2. 개인정보 취급위탁을 하는 업무의 내용

② 정보통신서비스 제공자등은 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 경우로서 제1항 각 호의 사항 모두를 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 취급위탁에 따른 제1항의 고지절차와 동의절차를 거치지 아니할 수 있다. 제1항 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

③ 정보통신서비스 제공자등은 개인정보 취급위탁을 하는 경우에는 수탁자가 이용자의 개인정보를 취급할 수 있는 목적을 미리 정하여야 하며, 수탁자는 이 목적을 벗어나서 이용자의 개인정보를 취급하여서는 아니 된다.

④ 정보통신서비스 제공자등은 수탁자가 이 장의 규정을 위반하지 아니하도록 관리·감독하여야 한다.

⑤ 수탁자가 개인정보 취급위탁을 받은 업무와 관련하여 이 장의 규정을 위반하여 이용자에게 손해를 발생시키면 그 수탁자를 손해배상책임에 있어서 정보통신서비스 제공자등의 소속 직원으로 본다.[전문개정 2008.6.13]

② 정보통신서비스 제공자등은 다음 각 호의 사항을 정하여 개인정보관리책임자 및 개인정보취급자를 대상으로 매년 2회 이상 교육을 실시하여야 한다.

▶ 개인정보보호 교육의 목적은 정보통신서비스 제공자등의 사업장 내의 개인정보 취급자에게 개인정보보호에 대한 인식을 제고시키고 개인정보보호 대책의 필요성을 이해시키는 것이다. 구현된 기술적·관리적 보호조치 기준에 대한 정확한 교육 및 훈련 프로그램을 수립하여 이행하여야 한다.

▶ 개인정보관리책임자 및 개인정보취급자를 대상으로 매년 정기적으로 2회 이상의 개인정보보호 교육을 실시하여야 한다. 특히, 개인정보취급자가 고객의 개인정보를 훼손·침해·누설할 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해지므로, 교육 시 이러한 점을 개인정보취급자에게 인식시키기 위해 노력해야 한다.

※ 관련 법규 : 법 제28조2(개인정보의 누설금지) 및 제71조(벌칙)제5호 및 6호

(개인정보의 누설금지) ① 이용자의 개인정보를 취급하고 있거나 취급하였던 자는 직무상 알게 된 개인정보를 훼손·침해 또는 누설하여서는 아니 된다.
② 누구든지 그 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받아서는 아니 된다.[전문개정 2008.6.13]

(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
1. ~ 4. (생략)
5. 제28조의2제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 개인정보를 훼손·침해 또는 누설한 자
6. 제28조의2제2항을 위반하여 그 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
7. ~ 11. (생략)[전문개정 2008.6.13]

▶ 개인정보보호 교육의 구체적인 사항에는 교육 목적, 대상, 내용(프로그램 등 포함), 일정 및 방법 등을 포함하는 내부관리계획 또는 임직원의 결재를 얻은 "○○년 개인정보보호 교육 계획(안)"과 같이 관리하여야 한다.

▶ 교육 방법은 집체교육 뿐만 아니라 조직의 환경을 고려하여 인터넷 교육, 그룹웨어 교육 등 다양한 방법을 활용하여 실시하도록 하고, 필요한 경우 외부 전문기관이나 전문요원에 위탁하여 교육을 실시할 수 있다.

▶ 특히, 개인정보 침해 위험성이 높은 분야인 위탁받은 자와 대리점 등에 대한 교육은 더욱 필요하다.

- 개인정보의 임의 사용 등 사례가 위탁받은 자에게서 가장 많이 나타나고 있으며, 법에서도 위탁받은 자에 대한 관리·감독 의무가 규정되어 있을 뿐만 아니라 이러한 위탁받은 자가 이용자에게 손해를 입힌 경우 위탁한 정보통신서비스 제공자등에게도 손해배상 책임이 있음을 주지하도록 한다.

※ 관련 법규 : 법 제25조(개인정보의 취급위탁), 제64조의3(과징금의 부과 등), 제71조(벌칙) 및 제76조(과태료)

(개인정보의 취급위탁) ① 정보통신서비스 제공자와 그로부터 제24조의2제1항에 따라 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)는 제3자에게 이용자의 개인정보를 수집·보관·처리·이용·제공·관리·파기 등(이하 "취급"이라 한다)을 할 수 있도록 업무를 위탁(이하 "개인정보 취급위탁"이라 한다)하는 경우에는 다음 각 호의 사항 모두를 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

1. 개인정보 취급위탁을 받는 자(이하 "수탁자"라 한다)

2. 개인정보 취급위탁을 하는 업무의 내용

② 정보통신서비스 제공자등은 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 경우로서 제1항 각 호의 사항 모두를 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 취급위탁에 따른 제1항의 고지절차와 동의절차를 거치지 아니할 수 있다. 제1항 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

③ 정보통신서비스 제공자등은 개인정보 취급위탁을 하는 경우에는 수탁자가 이용자의 개인정보를 취급할 수 있는 목적을 미리 정하여야 하며, 수탁자는 이 목적을 벗어나서 이용자의 개인정보를 취급하여서는 아니 된다.

④ 정보통신서비스 제공자등은 수탁자가 이 장의 규정을 위반하지 아니하도록 관리·감독하여야 한다.

⑤ 수탁자가 개인정보 취급위탁을 받은 업무와 관련하여 이 장의 규정을 위반하여 이용자에게 손해를 발생시키면 그 수탁자를 손해배상책임에 있어서 정보통신서비스 제공자등의 소속 직원으로 본다.[전문개정 2008.6.13]

(과징금의 부과 등) ① 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 1 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 다만, 제6호에 해당하는 행위가 있는 경우에는 1억원 이하의 과징금을 부과할 수 있다. <개정 2012.2.17>

1. ~ 4. (생략)

5. 제25조제1항을 위반하여 이용자의 동의를 받지 아니하고 개인정보 취급위탁을 한 경우

6. ~ 7. (생략)

② ~ ⑦ (생략)[본조신설 2008.6.13] [시행일 : 2012.8.18] 제76조]

(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

1. ~ 3. (생략)

4. 제25조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보 취급위탁을 한 자

5. ~ 11. (생략)[전문개정 2008.6.13]

(과태료) ① (생략)

② 다음 각 호의 어느 하나에 해당하는 자에게는 2천만원 이하의 과태료를 부과한다.

1. 제25조제2항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자에게 개인정보 취급위탁에 관한 사항을 공개하지 아니하거나 알리지 아니한 자

2. ~ 4. (생략)

③ ~ ⑦ (생략)[전문개정 2008.6.13]

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

[개인정보 교육내용(예시)]

- 개인정보보호의 중요성
- 내부관리계획의 준수 및 이행
- 개인정보시스템 하드웨어 및 소프트웨어를 포함한 시스템의 정확한 사용법
- 개인정보의 기술적·관리적 보호조치 기준 이행
- 개인정보보호 관련자들의 금지 항목들
- 개인정보보호 위반을 보고해야 할 필요성
- 개인정보보호 준수검사 관련 절차 등
- 보안정책, 보안지침, 지시사항, 위험관리 전략
- 개인정보보호업무의 절차, 책임, 작업 설명

③ 정보통신서비스 제공자등은 제1항 및 제2항에 대한 세부 계획, 제4조부터 제8조까지의 보호조치 이행을 위한 세부적인 추진방안을 포함한 내부 관리계획을 수립·시행하여야 한다.

▶ 제3조(내부관리계획의 수립 · 시행)제1항 및 제2항, 제4조(접근통제), 제5조(접속기록의 위 · 변조 방지), 제6조(개인정보의 암호화), 제7조(악성프로그램 방지), 제8조(출력 · 복사시 보호조치)는 본 해설서 참조

【FAQ】

[문1] 개인정보관리책임자는 별도로 채용을 해야 하나요?

▶ 법 시행령 제13조는 개인정보관리책임자의 자격에 대해 임원 또는 개인정보와 관련하여 이용자의 고충처리 담당부서의 장으로 정하고 있습니다. 별도로 인력을 채용하여 위의 직위에 보하거나 기존에 위의 직위에 재직하고 있는 자에게 개인정보관리책임자의 임무를 부여하고 지정해도 됩니다. 그러나 개인정보관리책임자의 지정을 구두로 하는 경우에는 실효적인 업무수행이 곤란하고 책임 소재에도 문제가 있으므로, 내부관리계획과 개인정보취급방침에 반영하는 것이 바람직합니다.

[문2] 개인정보관리자 및 취급자를 대상으로 매년 2회 이상 교육실시는 개인정보를 다루는 모든 사람에게 개별적으로 적용되는 것인가요?

▶ 조직 내에서 개인정보를 다루는 개인정보관리자 및 취급자는 모두 회사에서 수립한 교육 계획에 따라 최소 연 2회 이상의 교육을 받아야 합니다. 만약 회사에서 연 2회 이상의 교육 기회를 제공하였으나 개인정보관리자 및 취급자가 개별적인 사정으로 교육을 실시하지 않았다면 별도로 교육을 받을 수 있는 기회를 제공하여야 합니다.

[문3] 정보보호 교육의 일부분으로 개인정보보호 교육이 포함되었다면 교육으로 인정되는 것인가요?

▶ 정보보호 교육이라 하더라도 회사 내부의 개인정보보호 교육 계획에 의해 실시되었다면 개인정보보호 교육으로 인정될 수 있습니다. 다만, 이때에는 개인정보보호 교육 목적과 대상, 내용, 일정 및 방법이 개인정보보호 교육 계획과 부합되어야 하며 교육 실시에 대한 자료는 문서화하여 보관할 필요가 있습니다.

4. 접근통제

제4조(접근통제) ①정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여한다.
②정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.
③정보통신서비스 제공자등은 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다.
④정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 공인인증서 등 안전한 인증 수단을 적용하여야 한다.
⑤정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

⑥정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 한다.
⑦정보통신서비스 제공자등은 이용자가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성규칙을 수립하고, 이행한다.
⑧정보통신서비스 제공자등은 개인정보취급자를 대상으로 다음 각 호의 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 한다.

1. 다음 각 목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성
   가. 영문 대문자(26개)
   나. 영문 소문자(26개)
   다. 숫자(10개)
   라. 특수문자(32개)
2. 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고
3. 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경

⑨정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 한다.

【취 지】

▶ 접근통제의 목적은 개인정보처리시스템에 대하여 인가되지 않은 접근을 차단하는 것으로, 인가되지 않은 접근은 개인정보의 불법 사용, 누출, 변조·훼손 등을 야기할 수 있으므로 적절히 차단되어야 한다.

- 일반적으로 시스템 사용자는 식별과 인증이라는 보안정책[1]에 의해 구분되어 허용 여부가 결정된다. 식별과 인증은 시스템 자원을 보호하기 위한 가장 기본적인 접근통제 수단이다.

▶ 개인정보보호 책임은 인력의 채용부터 퇴직 시까지 지속되어야 하고, 해당 인력들의 고의 또는 실수로 인한 정보의 누출이나 변조·훼손 등의 위험을 예방하고 대응하기 위해 기본적인 내부인력에 대한 접근통제 조치들이 필요하다.

【해 설】

①정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보관리책임자 또는 개인정보취급자에게만 부여한다.

▶ 개인정보처리시스템에 대한 접근권한은 정보통신서비스 제공자등의 사업장 내에서 고객(이용자, 정보주체)을 대상으로 업무를 수행하는 개인정보관리책임자 및 개인정보취급자에게만 부여하여야 한다.

※ 관련 법규 : 법 제28조(개인정보의 보호조치)제2항

(개인정보의 보호조치) ① (생략) ② 정보통신서비스 제공자등은 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여야 한다.[전문개정 2008.6.13]

▶ 즉, 정보가 유출되거나 무결성이 훼손되는 것을 방지하기 위하여 고객의 개인정보에 접근할 수 있는 자를 서비스 제공 또는 업무 수행 목적으로 개인

1) 보안정책이란 접근통제시스템의 설계 및 관리를 다루기 위한 지침으로서 대개 어떤 주체(who)가 언제(when), 어디(where)에서 어떤 객체(what)에 대해 행위(how)하는 것을 허용 또는 거부할 것인지 정의하는 것을 의미한다.

정보를 이용하는 자(개인정보관리책임자, 개인정보취급자)로 한정하여 접근을 허용해야 하는 것이다.

②정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.
③정보통신서비스 제공자등은 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다.

▶ 관리자 계정을 가진 자는 개인정보처리시스템에 접근한 모든 행위에 대해 책임이 있다는 점을 인식하고, 개인정보취급자의 개인정보처리시스템 접근에 대한 권한을 통제하기 위한 절차를 수립하여 적용하여야 한다.

- 조직 내의 임직원 전보 또는 퇴직 등 인사이동을 통해 사용자 계정의 변경·삭제가 필요한 경우에는 공식적인 사용자 계정 관리절차에 따라 통제될 수 있도록 한다.

- 내부 인력의 퇴직 시 해당 인력의 계정 뿐만 아니라 해당 인력이 알고 있는 공용계정에 대한 위험도 존재하게 된다. 따라서 내부 인력의 퇴직 시에는 해당 인력의 계정을 삭제하고 내부 인력들이 공용으로 사용하는 계정의 비밀번호를 즉시 변경하도록 지침에 반영하여 이행하도록 한다.

- 임직원의 퇴직 시 계정을 폐쇄하고 접근권한을 효과적으로 제거하기 위해서는 퇴직 점검표에 사용계정의 폐쇄항목을 반영하여, 계정의 폐쇄 여부에 대해 확인을 받는 것이 바람직하다.

▶ 정보통신서비스 제공자등은 제1항 및 제2항에 의한 권한 부여, 변경, 말소에 대한 내역을 기록하고 해당 기록을 최소한 5년간 보관하여야 한다.

- 정보통신서비스 제공자등은 개인정보취급자를 선정함에 있어 인사 명령 등을 통하여 이를 공식화하고 퇴직 등 인사명령 시 비밀유지의무 등에 대한 서약서를 받아야 한다.

④정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 공인인증서 등 안전한 인증 수단을 적용하여야 한다.

▶ 외부에서 개인정보처리시스템 접속 시 단순히 아이디와 비밀번호만을 이용할 경우, 키로깅 등에 의해 아이디와 비밀번호만 유출되어도 개인정보처리시스템이 위험에 노출되게 된다. 이러한 위험성을 감소시키기 위해 아이디와 비밀번호를 통한 개인정보취급자 식별·인증과 더불어 공인인증서 등을 활용한 추가적인 인증 수단의 적용이 필요하다.

- 공인인증서(그 사람이 가지고 있는 것: what you have)는 안전한 인증 수단으로 아이디와 비밀번호를 이용하는 인증(그 사람이 알고 있는 내용을 사용: what you know)과 다른 특성을 갖고 있어 효과적인 이중 인증을 구성할 수 있다. 공인인증서는 PC에 보관하는 것보다 이동식 저장매체에 보관하는 것이 안전하다.
- 아이디와 비밀번호를 이용하는 인증과 별도의 인증수단으로 보안토큰, 휴대폰 인증, 일회용 비밀번호(OTP: One Time Password), 바이오정보 등을 사용할 수 있으며 외부에서 접근하는 단말기 IP 인증도 고려될 수 있다.
- 개인정보처리시스템에 대한 외부 접속시 인증 수단과 더불어 전송구간의 보호조치가 필요하다.

⑤정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

▶ 정보통신망을 통해 개인정보처리시스템에 불법적으로 접근하는 행위를 방지·차단하기 위해 아래와 같은 시스템 등을 설치·운영함으로써 네트워크 보안을 강화하여야 한다.

- 개인정보처리시스템으로의 접근을 IP 주소 등으로 제한하여 인가받지 않은 자를 차단하는 기능(침입차단기능)을 갖는 시스템의 설치·운영
- 개인정보처리시스템에 접속한 IP 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능(침입탐지기능)을 갖는 시스템의 설치·운영

▶ 침입차단 및 침입탐지 기능을 갖춘 설비의 설치 방법

- 일정 규모 이상의 개인정보처리시스템을 운영하고 있는 사업자는 전문기업이 제공하는 침입차단시스템 및 침입탐지시스템을 설치·운영하거나, 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템(IPS : Intrusion Prevention System), 웹방화벽 또는 보안 운영체제(Secure OS) 등을 도입할 수 있다.

※ 국내에서 인증 받은 시스템에 대한 정보는 국가정보원 IT보안인증사무국 웹사이트(service1.nis.go.kr)에서 확인할 수 있다.
- 침입차단시스템 : 인증제품목록 - FW(제품유형) 검색
- 침입탐지시스템 : 인증제품목록 - IDS(제품유형) 검색
- 침입방지시스템 : 인증제품목록 - IPS(제품유형) 검색
- 웹방화벽 : 인증제품목록 - 웹방화벽(제품유형) 검색
- 보안운영체제 : 인증제품목록 - 접근통제시스템(제품유형) 검색

▶ 전문 침입차단시스템 및 침입탐지시스템의 설치 운영이 곤란한 SOHO 등 소기업의 경우 인터넷데이터센터(IDC) 등에서 제공하는 보안서비스(방화벽, 침입방지, 웹방화벽 등)를 활용함으로써 초기 투자비용 등을 줄일 수 있다.

- 또한, 공개용(무료) S/W를 사용하여 해당 기능을 구현한 시스템을 설치·운영할 수 있다. 다만, 공개용(무료) S/W를 사용하는 경우에는 적절한 보안이 이루어지는지를 사전에 점검할 필요가 있다.

※ 참고사이트
- 한국인터넷진흥원(KISA) 인터넷침해대응센터 - 웹 보안 서비스 - 공개용 웹방화벽 (http://www.krcert.or.kr/kor/webprotect/webprotect_04.jsp)
- 침입탐지시스템 Snort 다운로드 웹사이트(http://www.snort.org)

▶ 불법적인 접근 및 침해사고 방지를 위한 목적 달성을 위해서는 침입차단과 침입탐지 기능을 갖는 시스템 도입과 더불어 침입차단 정책 설정 및 침입탐지 로그 분석, 로그 훼손 방지 등 적절한 운영·관리가 중요하다.

⑥정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리하여야 한다.

▶ 망분리 의무사업자는 전년도말 기준 직전 3개월간 저장·관리되고 있는 개인정보가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인의 경우에는 전 사업연도) 매출액이 100억원 이상인 정보통신서비스 제공자등만 해당한다. (시행령 제15조제2항)

▶ 기업의 망분리 구축 기간 및 비용을 고려하여 해당 조항은 2013년 2월 18일부터 시행한다.

▶ 고시에서 규정한 권한을 가진 개인정보취급자의 컴퓨터 등은 외부 인터넷망과 업무망을 분리하여야 한다.

- 즉, 개인정보처리 시스템에 접근하여 다운로드, 파기 또는 접근권한 설정이 가능한 개인정보취급자는 외부 인터넷망이 차단된 업무망에서 업무를 수행하여야 한다.

※ 다운로드 : 개인정보처리시스템에 접근하여 개인정보취급자의 컴퓨터 등에 개인정보를 엑셀, 워드 등의 파일형태로 저장하는 것
※ 파기 : 개인정보처리시스템에 저장된 개인정보 테이블 또는 DB전체를 삭제하는 것
※ 접근권한 설정 : 개인정보처리시스템에 접근하는 개인정보취급자의 다운로드, 파기에 대한 접근권한을 설정하는 것

▶ 업무망과 외부 인터넷망을 분리하는 방법

- 업무망과 외부 인터넷망은 서로의 영역에 접근할 수 없도록 차단되어야 한다.

- 물리적 망분리와 논리적 망분리는 보안성, 효율성, 도입비용 등 각각의 장단점을 가지고 있으며 해당 기업의 시스템 환경에 따라 선택하여 구축할 수 있다.

※ 물리적 망분리 : 통신망, 장비 등을 물리적으로 이원화하여 내부 업무망과 외부 인터넷망의 접근 경로를 단절
※ 논리적 망분리 : 물리적으로 하나의 통신망, 장비 등을 사용하지만 가상화 등의 방법을 사용하여 내부 업무망과 외부 인터넷망이 서로 접근할 수 없도록 구성

- 전문기업이 제공하는 물리적 또는 논리적 망분리 솔루션을 적용할 수 있다.
※ 국내에서 인증 받은 시스템에 대한 정보는 국가정보원 IT보안인증사무국 웹사이트(http://service1.nis.go.kr)에서 확인할 수 있다. 사업자는 인증된 자료유출방지 제품 중에 망분리 솔루션을 선택하여 적용할 수 있다.
·망분리 솔루션 : 인증제품 - 자료유출방지(제품유형) 검색

- 고시에서 규정하지 않은 개인정보취급자의 컴퓨터도 정보유출을 예방하기 위해 적용범위를 확대하여 적용할 수 있다.

▶ 업무망의 컴퓨터는 최신 보안 업데이트, 저장매체 관리 등 적절한 운영·관리가 중요하다.

- 인터넷망이 차단된 컴퓨터는 내부망, 그룹웨어, 저장매체 등을 통해 최신 보안 업데이트를 수행할 수 있다.
- 또한, 외부저장매체 등을 통해 업무망 또는 외부망으로 데이터 전달이 필요한 경우, 악성코드 유입 또는 개인정보 유출이 일어나지 않도록 안전한 보안 대책을 마련하는 것이 필요하다.

⑦정보통신서비스 제공자등은 이용자가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성규칙을 수립하고, 이행한다.

▶ 안전하지 못한 비밀번호를 사용할 경우 정보가 노출될 위험성이 있다. 안전한 비밀번호란 제3자가 쉽게 추측할 수 없으며 비밀번호 크래킹을 통해서도 비밀번호를 얻어낼 수 없거나 얻어내는데 많은 시간이 소요되는 것을 의미한다.

- 따라서 이용자가 생일, 전화번호 등 추측하기 쉬운 숫자나 문자 등을 비밀번호로 이용하지 않도록 비밀번호 작성규칙을 수립하고 이행하도록 하는 것이 필요하다.

▶ 비밀번호 작성규칙을 수립한 경우 이용자의 비밀번호 설정 시 입력된 비밀번호의 보안강도를 알려주거나 일정 수준 이하의 비밀번호는 설정되지 못하도록 시스템을 구성하는 것도 효과적인 이행을 위한 수단이 될 수 있다. 다만, 이용자가 사용하는 비밀번호에 대해서는 이용자의 편의성 등도 고려하여 이용자가 적절한 수준으로 비밀번호를 설정할 수 있도록 비밀번호 설정기준을 마련하는 것이 필요하다.

※ 한국인터넷진흥원(KISA)은 비밀번호 안전성 검증 소프트웨어를 사업자들이 적용할 수 있도록 검증도구를 보급하고 있다.
- 검증도구 보급신청은 KISA 암호이용활성화 홈페이지[http://seed.kisa.or.kr - 패스워드 안전성 검증 - 보급신청]에서 참고

⑧정보통신서비스 제공자등은 개인정보취급자를 대상으로 다음 각 호의 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 한다.

1. 다음 각 목의 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성
   가. 영문 대문자(26개)
   나. 영문 소문자(26개)
   다. 숫자(10개)
   라. 특수문자(32개)
2. 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고
3. 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경

▶ 정보통신서비스 제공자등은 개인정보취급자의 비밀번호 작성규칙을 수립하고 이를 개인정보처리시스템 및 접근통제시스템 등에 적용하여 운영하여야 한다.

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

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

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

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

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

※ 특수문자 32개 예시

~ · ! @ # $ % ^ & * ( ) _ - + = { } [ ] | \ ; : ‘ “ < > , . ? /

- 추측하기 어려운 비밀번호의 생성 :

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

· love, happy 등과 같은 잘 알려진 단어나 키보드 상에서 나란히 있는 문자열도 포함되지 않도록 한다.

[안전한 비밀번호 설정 방안]

□ 예측이 어려운 문자구성의 비밀번호 설정방법

o 영문자(대/소문자), 숫자, 특수 기호들을 혼합한 구성으로 비밀번호 설정
- #3kLfN2x*S1$, 3$La#4dU7Ff% 등과 같은 구성의 비밀번호 설정

o 비밀번호의 길이를 증가시키기 위해서는 특정위치 외에 특수문자 및 숫자 등을 삽입하여 비밀번호 설정
※특정위치는 알파벳 문자 앞뒤에 위치하는 것을 말함

o 알파벳 대소문자를 구별할 수 있을 경우, 대·소문자를 혼합하여 비밀번호 설정
- 특정위치의 문자를 대문자변경하거나, 모음만을 대문자변경하여 비밀번호 설정
- "gkswjdqhwlsdnjs"는 "gKsWjDqHwLsDnJs"로, "rnrqhghgmd"는 "rNrQhGhGmD"로 활용하여 비밀번호 설정

□ 기억하기 쉬운 비밀번호 설정방법

o 특정명칭을 선택하여 예측이 어렵도록 가공하여 비밀번호 설정
- 특정명칭의 홀수·짝수 번째의 문자를 구분하는 등의 가공방법을 통해 설정
- 국내 사용자는 한글 자판을 기준으로 특정명칭을 선택하고 가공하여 설정
  · 예를 들어 '한국인터넷진흥원'의 경우, 홀수 번째는 "한인넷흥"이 "gksdlssptgmd"로, 짝수 번째는 "국터진원"이 "rnrxjwlsdnjs"으로 비밀번호 설정 가능함

o 노래 제목이나 명언, 속담, 가훈 등을 이용·가공하여 비밀번호 설정
- 영문사용의 경우, "This May Be One Way To Remember"를 "TmB1w2R"이나 "Tmb1w>r~"로 활용가능
- 한글사용의 경우, "백설공주와 일곱 난쟁이"를 "백설+7난장"로 구성하고 "QorTjf+7SksWkd" 등으로 활용가능

- 비밀번호의 주기적인 변경 : 비밀번호에 유효기간을 설정하고 적어도 6개월마다 변경함으로써 동일한 비밀번호를 장기간 사용하지 않도록 한다.

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

- 개인정보취급자는 자신의 비밀번호가 제3자에게 노출되지 않도록 주의해야 하며, 정보통신서비스 제공자등은 비밀번호 설정 원칙이 정상적으로 이행되고 있는지 정기적으로 점검할 필요가 있다. 비밀번호에 사용될 수 있는 최소길이 및 문자 혼합 정도, 비밀번호 만료 기간 등이 적용될 수 있도록 시스템을 구성하는 것도 효과적인 이행을 위한 수단이 될 수 있다.

【참고 사항】

▶ 비밀번호 설정 원칙은 아래 문서 등을 참조할 수 있다.

- 한국인터넷진흥원(KISA)의 패스워드 선택 및 이용 가이드
  (http://seed.kisa.or.kr - 패스워드 안전성 검증 - 패스워드 선택 및 이용 가이드)
- SANS의 비밀번호 정책
  (http://www.sans.org/resources/policies/Password_Policy.pdf)

⑨정보통신서비스 제공자등은 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리 시스템 및 개인정보취급자의 컴퓨터에 조치를 취하여야 한다.

▶ 개인정보취급자의 부주의로 고객 개인정보가 인터넷 홈페이지 또는 P2P를 통해 게시되거나, 공유 설정된 PC 폴더에 고객명단 파일을 둠으로써 열람 권한이 없는 자에게 공개되는 사례가 많이 발견되고 있다.

▶ 과실로 인한 인터넷 홈페이지에서 노출 방지

- 인터넷 홈페이지 운영자 또는 자료게시 담당 직원의 실수로 게시판 등에 고객 주민등록번호 등이 포함된 파일을 게시하는 사례가 있다.
- 이를 방지하기 위하여 다음과 같은 조치를 취하여야 한다.
  - 웹사이트를 통해 고객의 개인정보를 수집·관리하는 경우에는 ID 및 비밀번호를 통한 사용자 인증(login) 기능을 적용하여야 한다.
  - 수시로 웹사이트 게시판 등에서의 주민번호 노출 여부 등을 점검하여 조치하도록 한다.

▶ 인터넷 홈페이지 취약점으로 인한 노출 방지

- 인터넷 홈페이지 개발시 보안기준을 따르지 않아 발생하는 취약점으로 인해 구글 등의 검색엔진을 통해 개인정보 DB가 노출되는 사례도 발생하므로 수시로 인터넷 홈페이지 취약점을 점검하여 조치하도록 한다.

  ※ 한국인터넷진흥원(KISA)은 웹 취약점 원격점검서비스(http://toolbox.krcert.or.kr)를 통해 중소기업 또는 비영리 단체를 대상으로 무료로 제공하고 있다.

- 회사 홈페이지를 개발할 때 한국인터넷진흥원(KISA)이 권고하는 웹 보안

서비스(http://www.krcert.or.kr - 웹 보안 서비스)를 따르도록 하여 취약점을 최소화 한다

▶ P2P 프로그램에서의 노출

- P2P 프로그램 사용 시 자료 공유를 위해 이용자 본인이 공유할 폴더를 선택할 수 있는데 부주의로 PC전체를 공유 폴더로 설정하거나, 공유 폴더에 엑셀 등으로 작성된 고객 개인정보 파일을 올려놓아 외부로 유출될 수 있다.

- 따라서, 개인정보취급자의 컴퓨터인 경우 원칙적으로 P2P 프로그램을 사용하지 않는 것이 바람직하나, 반드시 사용해야 할 경우 공유폴더에 개인정보 파일이 포함되지 않도록 정기적으로 점검하여 조치하도록 한다.

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

▶ 공유설정을 통한 노출

- 내 컴퓨터에 있는 파일들을 다른 사람과 손쉽게 공유하기 위해 공유폴더를 사용할 수 있는데 공유설정 부주의로 개인정보 파일이 권한 없는 자에게 노출될 수 있다.

- 따라서, 공유폴더를 사용할 경우 드라이브 전체 또는 불필요한 폴더가 공유되지 않도록 조치하고, 공유폴더에 개인정보 파일이 포함되지 않도록 정기적으로 점검하여 조치하도록 한다.

  ※ 윈도우즈의 경우 시작 - 제어판 - 성능 및 유지관리 - 관리도구 - 컴퓨터 관리를 실행하여, 공유폴더 메뉴에서 확인 가능

【FAQ】

[문1] 현재 운영중인 침입방지나 침입차단시스템을 업데이트할 계획인데, 이 기준에서 이러한 시스템에 대한 특별한 규격을 정하고 있는지, 아니면 적합한 제품이라면 어떠한 것이든 상관없는지요?

▶ 기준에서 침입차단시스템 등에 대해 특별히 규격을 정해 놓고 있지는 않습니다. 귀사의 시스템 규모를 감안하여 적절한 제품을 선택하시기 바랍니다.

[문2] 온라인과 오프라인으로 서비스를 제공하고 있는 업체입니다. 오프라인으로 수집한 개인정보도 100만명 이상 개인정보의 기준에 포함되어 망분리를 적용해야 하나요?

▶ 오프라인으로 수집한 개인정보도 온라인으로 서비스 된다면 개인정보의 기술적·관리적 보호조치 기준을 따라야 합니다. 따라서, 수집 경로에 상관없이 정보통신망을 통해 일일평균 100만명 이상 이용자의 개인정보를 보유하고 있거나 정보통신서비스 부문의 전년도 매출액이 100억원 이상인 경우라면 망분리 시스템을 구축하여야 합니다.

[문3] 법령에 따라 외부 인터넷망을 분리할 계획입니다. 망분리 구축 방법에 대한 기준은 없는지요?

▶ 기준에서 망분리에 대해 특별한 기술규격을 제시하지는 않습니다. 귀사의 시스템 규모, 환경에 따라 물리적 또는 논리적 망분리 솔루션을 선택하시거나 구축하시기 바랍니다.

[문4] 소량의 개인정보를 다운로드하는 개인정보취급자도 망분리 대상인지요?

▶ 법령에 따라 일일평균 100만명 이상 이용자의 개인정보를 보유하고 있거나 정보통신서비스 부문의 전년도 매출액이 100억원 이상인 경우 망분리 대상이 되며 다운로드 건수에 대한 제한을 두고 있지는 않습니다. 외부 침입이 탐지되지 않을 경우 지속적인 다운로드를 시도하여 다량의 유출로 이어질 수 있습니다. 따라서, 건수에 관계없이 다운로드 권한을 가지고 있다면 망분리 하여야 합니다.

[문5] 비밀번호 작성 규칙에서 저희의 경우 4자리로 해야 하나 8자리로 해야 하는지 결정하기 힘든 상황입니다. 그런데 반드시 8자리 또는 10자리로 해야 하는지 아니면 다른 조치가 있다면(예를 들어 3번 이상 비밀번호가 틀리면 중지) 자리 수는 상관없는지요?

▶ 개인정보취급자에 대한 비밀번호 작성규칙은 법적 의무사항이므로 보호조치 기준에서 정의한 내용대로 이행하셔야 합니다. 비밀번호 선택 시 사용하는 문자의 종류에 따라 최소 10자리(2종류 이상) 또는 최소 8자리(3종류 이상) 이상으로 설정하고, 최소 6개월마다 변경해야 합니다.

5. 접속기록의 위·변조 방지

제5조(접속기록의 위·변조방지) ①정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리하여야 한다.

② 단, 제1항의 규정에도 불구하고 「전기통신사업법」 제5조의 규정에 따른 기간통신사업자의 경우에는 보존·관리해야할 최소 기간을 2년으로 한다.

③정보통신서비스 제공자등은 개인정보취급자의 접속기록이 위·변조되지 않도록 별도의 물리적인 저장 장치에 보관하여야 하며 정기적인 백업을 수행하여야 한다.

【취 지】

▶ 접속기록은 개인정보의 입·출력 및 수정사항, 파일별·담당자별 데이터접근내역 등을 자동으로 기록하는 로그 파일을 생성하여 불법적인 접근 또는 행동을 확인할 수 있는 중요한 자료이며, 접속기록의 백업은 개인정보 DB의 안전성을 유지하기 위한 중요한 요소이다.

- 그러나 본 조항에서 다루는 접속기록은 네트워크에서의 침입탐지 시도를 위한 로그기록 전반이 아닌 개인정보 DB에서의 개인정보 열람·수정·삭제·출력 등의 작업을 위한 접속기록을 의미한다.

【해 설】

①정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 6개월 이상 접속기록을 보존·관리하여야 한다.

▶ 정보통신서비스 제공자 등은 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우에는 처리일시, 처리내역 등 접속기록을 최소 6개월 이상 저장하고 이를 월 1회 이상 정기적으로 확인·감독하여야 한다.

- 즉, 개인정보처리시스템의 사용자 권한 설정 등의 제반 보호장치에 관한 사항을 확인하고, 개인정보 보호업무의 수행과 관련하여 오류 및 부정행위가 발생하거나 예상되는 경우 즉각적인 보고 조치가 되도록 한다.

- 접속기록 항목으로는 정보주체 식별정보, 개인정보취급자 식별정보, 접속일시, 접속지 정보, 부여된 권한 유형에 따른 수행업무 등을 포함하여야 한다.

[접속기록 항목(예시)]

정보주체 식별정보	취급자 식별정보	접속일시	접속지	수행업무
123456789	홍길동(HGD)	2012.06.03, 15:00:00	172.168.168.11	조회(고객응대)

- 사업 환경에 따라, 개인정보취급자가 처리한 정보주체의 개인정보 항목에 대해서도 접속기록에 추가적으로 기록할 수도 있다.

▶ 개인정보처리시스템에 대한 접속기록 유지·관리를 위하여 다음 사항을 포함하여 접속기록 관리 방법 및 절차를 수립하도록 한다.

- 기록 유지·관리가 필요한 주요 접속기록 식별
- 개인정보처리시스템에서 생성되는 접속기록 파일 내용
- 접속기록 파일의 생성량 및 생성주기
- 요구되는 보안성에 따른 분석주기
- 접속기록 파일 생성 및 보관정책 등

▶ 최근 개인정보처리시스템에 대한 접속기록 및 이에 대한 실시간 모니터링 또는 확인·감독을 위해 다양한 시스템이 보급되고 있으므로 서비스를 제공하는 고객의 규모 또는 사업 환경에 따라 별도의 시스템을 도입할 수 있다.

※ 국내에서 인증 받은 시스템에 대한 정보는 국가정보원 IT보안인증사무국 웹사이트(service1.nis.go.kr)에서 확인할 수 있다.
· 인증제품목록 - DB접근통제(제품유형) 검색

② 단, 제1항의 규정에도 불구하고 「전기통신사업법」 제5조의 규정에 따른 기간통신사업자의 경우에는 보존·관리해야할 최소 기간을 2년으로 한다.

▶ 기간통신사업자의 경우, 사업자의 특성상 대량의 개인정보를 보유·이용하고 있으며 개인정보의 유출·침해로 인한 피해 가능성도 높다고 할 수 있다. 이에 따라, 기간통신사업자에 대해서는 통상의 6개월이 아니라 이용자의 권익보호, 접속기록 보존능력 등을 종합적으로 고려하여 최소 기간으로 2년을 설정하였다.

③정보통신서비스 제공자등은 개인정보취급자의 접속기록이 위·변조되지 않도록 별도의 물리적인 저장 장치에 보관하여야 하며 정기적인 백업을 수행하여야 한다.

▶ 정보통신서비스 제공자등은 개인정보처리시스템의 접속 기록이 위·변조되지 않도록 별도 저장 장치에 백업 보관하여야 한다.

- 즉, 데이터 손·망실에 대비하여 별도의 물리적인 저장 장치에 보관하고 정규적인 백업을 수행해야 한다.

- 접속기록이 위·변조되지 않도록 쓰기 권한을 제한하여 보관하는 것이 바람직하며, 수정이 가능하더라도 위·변조 여부를 확인할 수 있도록 별도의 보호조치를 취할 수 있다.

※ 접속기록의 위·변조 여부를 확인할 수 있는 정보(HMAC 값 또는 전자서명값 등)는 별도의 HDD 또는 관리대장에 보관하는 방법으로 관리할 수 있다.

※ 이외에 접속기록에 대한 타임스탬프 값을 공인인증기관으로부터 공증 받는 방법 또는 전자문서 보관소를 활용하는 방법 등이 있다.

6. 개인정보의 암호화

제6조(개인정보의 암호화) ①정보통신서비스 제공자등은 비밀번호 및 바이오정보는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.
②정보통신서비스 제공자등은 주민등록번호, 신용카드번호 및 계좌번호에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다.
③ 정보통신서비스 제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호 중 하나의 기능을 갖추어야 한다.
1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능
2. 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능

④정보통신서비스 제공자등은 이용자의 개인정보를 개인용컴퓨터(PC)에 저장할 때에는 이를 암호화해야 한다.

【취 지】

▶ 비밀번호, 바이오정보, 주민등록번호 등과 같은 개인정보가 암호화되지 않고 저장 및 전송되는 경우, 노출 및 위·변조 등의 위험이 있으므로 개인정보처리시스템에 저장하거나 네트워크를 통해 전송할 때에는 해당정보의 불법적인 노출 또는 위·변조 방지를 위한 암호화가 제공되어야 한다.

【해 설】

①정보통신서비스 제공자등은 비밀번호 및 바이오정보는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.

▶ 정보통신서비스 제공자등은 개인정보취급자 및 이용자의 비밀번호, 바이오정보(지문, 홍채 등)의 소유자임을 인증하는 정보가 노출 또는 위·변조되지 않도록 일방향 함수(해쉬함수)를 이용하여 저장하여야 한다.

- 사용자가 입력한 인증과 관련된 정보는 평문 형태로 저장되지 않고 일방향

함수를 통해 얻은 결과 값이 시스템에 저장된다.

- 인증검사 시에는 사용자가 입력한 정보를 일방향 함수에 적용하여 얻은 결과 값과 시스템에 저장된 값을 비교하여 인증된 사용자임을 결정할 수 있다.
- 안전한 암호알고리듬은 CPU 및 메모리 등 관련 장비의 발전에 따라 달라질 수 있다. 일방향 함수인 해쉬함수의 경우 아래와 같은 안전성을 권고한다.

[보안강도에 따른 해쉬함수 분류]

보안강도	해쉬 함수	안전성
80 비트 미만	MD5, SHA-1	권고하지 않음
80 비트	HAS-160	
112 비트	**SHA-224**	**2013년까지 권고함**
128 비트	**SHA-256**	**2013년 이후에도 가능**
192 비트	**SHA-384**	
256 비트	**SHA-512**	

▶ 정보통신서비스 제공자등은 일방향 암호화한 이용자의 비밀번호 등 본인임을 인증하는 정보의 내용을 알 수 없으므로,

- 이용자가 비밀번호의 분실 등을 이유로 재발급을 원하는 경우에는 이용자에게 임의의 비밀번호를 부여하고 회원정보에 등록된 이메일 등으로 부여된 임의의 비밀번호를 전송하고 이용자가 확인 후 사이트에 접속하여 비밀번호를 다시 설정할 수 있도록 시스템을 구성할 수 있다.

②정보통신서비스 제공자등은 주민등록번호, 신용카드번호 및 계좌번호에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다.

▶ 개인정보 유·노출 시에 2차 피해가 발생할 확률이 높은 주민등록번호, 신용카드번호 및 계좌번호에 대해서는 안전한 알고리듬으로 암호화하여 저장·관리해야 한다.

Tip 주민등록번호의 사용 제한

- 법 제23조의2에서 규정한 경우를 제외하고는 이용자의 주민등록번호를 수집할 수 없다. 자세한 자료는 개인정보보호 포털[http://www.i-privacy.kr - 사업자 - 주민번호 사용 제한 안내 - 주민번호 사용 제한 안내서 다운로드] 참조

※ 관련 법규 : 법 제23조의2(주민등록번호의 사용제한)

(주민등록번호의 사용제한) ① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다.

1. 제23조의3에 따라 본인확인기관으로 지정받은 경우
2. 법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우
3. 영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는 경우

② 제1항제2호 또는 제3호에 따라 주민등록번호를 수집·이용할 수 있는 경우에도 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하 "대체수단"이라 한다)을 제공하여야 한다.

- 본 해설서에서 권고하는 안전한 암호알고리듬은 대칭키 암호 알고리듬의 경우 다음 표와 같다.

[보안강도에 따른 대칭키 암호 알고리듬 분류]

보안강도	대칭키 암호 알고리듬	안전성
80 비트 미만	DES	권고하지 않음
80 비트	2TDEA	
112 비트	3TDEA	
128 비트	SEED, HIGHT, ARIA-128, AES-128	권고함
192 비트	ARIA-192, AES-192	
256 비트	ARIA-256, AES-256	

※ 3TDEA는 112비트 이상의 보안강도를 가지고 있지만, 보안성이 낮다고 평가되어 권고하지 않음

- 자세한 자료는 한국인터넷진흥원(KISA) 암호이용활성화 홈페이지 [http://seed.kisa.or.kr - 알림마당 - 공지사항 - 암호기술 구현 안내서 보급] 참조

- 2012년 9월 현재 KISA에서는 보안강도 112 비트(2013년 까지) 이상의 암호화 알고리듬을 사용할 것을 권고하고 있다. 위 권고 암호 알고리듬은 IT 환경의 기술수준(컴퓨팅 성능, 해킹 능력 등)에 따라 변경될 수 있으며, 향후 연구를 통해 보안강도에 따른 적정 안전성 유지기간을 도출할 예정이다. 이 밖에도 미국 NIST, 일본 CRYPTREC, 유럽 ECRYPT 등의 외국 암호 연구기관에서 권고하는 알고리듬을 적용할 수 있으나, 국내의 IT 환경을 고려하여 국내 권고 암호화 알고리듬을 적용하는 것이 바람직하다.

▶ 고유식별정보, 금융정보 등의 개인정보는 원칙적으로 전부 암호화해야 하지만, 신용카드번호 등 시스템 운영을 위한 키 값 또는 이용자에게 서비스 혜택 제공 등을 위해 상시적으로 사용하여 암호화/복호화의 부하가 발생할 수 있다. 이러한 경우라면 최소한의 정보만을 평문으로 저장하고 이외 정보는 암호화하는 부분 암호화 조치를 취할 수 있다.

- 신용카드 번호의 경우 카드유형 정보(국내/VISA/MASTER 등)를 포함한 6자리를 제외한 뒷자리 10개 번호 이상을 암호화 조치하는 것이 바람직하다.
  (4902-20$……^)

▶ 보안강도가 높은 암호화 기법 및 프로그램을 사용하더라도 암호화키 및 비밀번호의 관리가 잘못될 경우에는 암호화된 정보들이 노출될 수 있으므로 암호화키 및 비밀번호에 대한 안전한 관리가 중요하다.

③ 정보통신서비스 제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호 중 하나의 기능을 갖추어야 한다.

1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능
2. 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능

▶ 정보통신서비스 제공자등은 신용카드번호, 계좌번호 등의 개인정보와 비밀번호, 바이오정보 등의 인증정보를 정보통신망 외부로 송·수신할 경우에는 해당 데이터를 임의의 사용자가 내용을 확인할 수 없도록 암호화 전송하여 노출 및 불법적인 접근을 차단해야 한다.

- SSL 인증서를 이용한 보안서버는 별도의 보안 프로그램 설치 없이, 웹서버에

설치된 SSL 인증서를 통해 개인정보를 암호화 전송하는 방식이다.

- 응용프로그램을 이용한 보안서버는 웹 서버에 접속하여 보안 프로그램을 설치하여 이를 통해 개인정보를 암호화 전송하는 방식이다.

▶ 보안서버 구축에 관한 자세한 사항은 한국인터넷진흥원(KISA) 홈페이지 [http://www.kisa.or.kr - 주요사업 - 개인정보보호 - 보안서버] 참조

④정보통신서비스 제공자등은 이용자의 개인정보를 개인용컴퓨터(PC)에 저장할 때에는 이를 암호화해야 한다.

▶ 고객의 개인정보를 개인정보처리시스템으로부터 개인정보취급자의 PC에 내려받아 저장할 때는 파일암호화 제품 등을 이용하여 암호화함으로써 불법적인 노출 및 접근으로부터 차단하여야 한다.

- 개인정보취급자는 아래의 방법 등을 사용하여 개인정보 파일을 안전하게 PC에 저장할 수 있다. 파일 암호화에 사용되는 비밀번호 및 암호화 알고리듬은 본 해설서에서 안내하는 안전한 비밀번호 및 보안강도 112비트 이상의 암호화 알고리듬을 사용해야 한다.

※ 2014년부터는 128비트 이상의 암호화 알고리듬을 권고

⑴ 자료유출방지나 문서암호화 전용시스템을 활용

※ 국내에서 인증 받은 시스템에 대한 정보는 국가정보원 IT보안인증사무국 웹사이트(service1.nis.go.kr)에서 확인할 수 있다.

・자료유출방지시스템 : 인증제품 - 자료유출방지(제품유형) 검색

・문서암호화시스템 : 암호제품 - 문서 암호화(제품군) 검색

⑵ Windows XP 등의 OS 자체에서 지원하는 파일 암호화 기능

※ http://support.microsoft.com/kb/307877/ko

⑶ 개인정보의 저장형태가 어플리케이션 파일 형태일 경우 해당 어플리케이션에서 제공하는 암호 설정 기능

※ 한글, 오피스 파일 암호화 : 메뉴 -> 파일 -> 문서암호

※ MS오피스 파일 암호화 : http://office.microsoft.com/ko-kr/excel/HA101483331042.aspx

【FAQ】

[문1] 개인정보수집이 필요한 웹기반 시스템을 개발 중인데 일방향 암호화를 어떻게 적용하라는 의미인지요?

▶ 사용자 인증(로그인)기능을 개발할 때, 예를 들어 특정사용자의 비밀번호가 123456이고 웹기반 시스템의 DB에 123456으로 평문으로 저장되어 단순 비교로 인한 인증 시스템 개발이 되지 않아야 한다는 의미입니다. 즉, 개발 시 상용 암호 모듈을 이용하여 적용하거나, 자체 DB 시스템에서 제공하는 암호 모듈 방법 활용, 공개용 암호 라이브러리 등을 사용한 프로그램 직접개발이 있는데 그중에 일방향함수(해쉬함수) 기능이 제공되는 라이브러리를 이용하여 개발해야 합니다.

[문2] 비밀번호가 아닌 신용카드정보, 계좌정보 또는 기타 고객정보도 일방향 암호화의 적용이 필요한가요?

▶ 개인정보의 기술적·관리적 보호조치 기준의 제6조제2항에 의하여 신용카드번호 및 계좌번호는 일방향 암호화하여 저장할 필요는 없으며, 본 해설서에서 권고하는 안전한 암호화 알고리듬으로 암호화하여 저장하면 됩니다.

7. 악성프로그램 방지

제7조(악성프로그램 방지) 정보통신서비스 제공자등은 백신 소프트웨어를 월 1회 이상 주기적으로 갱신·점검하고, 악성 프로그램 관련 경보가 발령된 경우 및 백신소프트웨어 또는 운영체제 제작업체에서 업데이트 공지가 있는 경우에는 응용프로그램과 정합성을 고려하여 최신 소프트웨어로 갱신·점검하여야 한다.

【취 지】

▶ 악성 프로그램이란 제작자가 의도적으로 다른 정보통신서비스 이용자에게 피해를 주고자 악의적 목적으로 만든 프로그램 및 실행 가능한 코드를 의미하는 것으로 악성 코드라고 불리기도 한다. 악성 프로그램은 컴퓨터 바이러스, 스파이웨어, 악성봇 등의 형태로 감염되며, 최근에는 다수의 악성봇(좀비PC)에 의한 DDoS 공격이 사회적 문제가 되고 있다.

▶ 악성프로그램은 컴퓨터에서 동작하는 일종의 프로그램으로 자료를 손상·유출하거나 기타 프로그램을 파괴하여 정상적인 작업을 방해한다. 이를 방지하기 위해 백신 소프트웨어 등을 이용하여 해당 프로그램을 제거하거나 예방할 필요가 있다.

【해 설】

▶ 백신 소프트웨어는 항상 실행시켜 둔 채로 하루에 1회 정도 사용자 임의로 점검시간을 설정하여 악성 프로그램 검사를 자동으로 실행할 수 있도록 설정하는 것이 필요하다.

- 백신 소프트웨어의 중요성에도 불구하고 시스템의 속도를 조금이나마 빠르게 하기 위하여 백신소프트웨어의 실시간 감지 기능 등을 꺼버리는 경우가 있으므로 주기적으로 정상 작동 여부를 확인한다.

▶ 백신소프트웨어는 데모용으로 사용자에게 정품 구입 전 제품에 대한 평가를 받고 구입을 제안하는 제품들도 있지만, 추가적인 기술지원이나 백신회사에서 제공하는 전체기능을 제공받으려면 정식 버전을 구입할 필요가 있다.

- 또한, 임시로 혹은 정식 버전을 구입한 고객에게 인터넷을 통해 악성 프로그램을 진단해주는 서비스를 이용할 수도 있다.

※ 한국인터넷진흥원(KISA)이 운영하는 보호나라 사이트에서 일반인에게 제공되는 바이

러스 백신에 대한 정보를 확인할 수 있다. [www.boho.or.kr]

▶ 스파이웨어는 본인도 모르게 타인의 PC에 설치되어 어떤 사람이나 조직에 관련된 정보를 수집하는 프로그램을 말하며, 스파이웨어를 통하여 개인정보가 유출되는 등의 부작용이 발생될 수 있다.

- 스파이웨어 대응 소프트웨어를 설치·운영하여 스파이웨어 자동 감지 및 제거 등을 수행하여야 한다.

▶ 악성 프로그램은 계속해서 새롭게 만들어지고, 변화하고, 유포되고 있다. 이에 대응하여 백신회사는 새로운 바이러스에 대하여 백신소프트웨어를 업데이트하고 있으므로, 새로운 유형의 악성 프로그램이 공지되면 자동 업데이트 기능 등을 이용하여 신속하게 긴급 업데이트를 실행하여야 한다.

▶ 백신 소프트웨어는 최소 월 1회 이상 주기적으로 갱신 및 점검하여야 하는데, 인터넷을 이용한 자동 업데이트/실시간 감지 기능 등을 활용하면 편리하고 신속하게 갱신 및 점검할 수 있다.

- 바이러스 경보가 발령된 경우나 백신 소프트웨어 제작 업체에서 업데이트 공지가 있는 경우에는 최신 소프트웨어로 갱신·점검하도록 한다.

▶ 보안패치는 운영체제(OS)나 응용 프로그램에 내재된 보안 취약점을 보완하는 소프트웨어로, 보안 패치를 할 경우 취약점을 악용하는 악성 코드 감염을 방지하고 각종 개인용 컴퓨터(PC)의 오류 원인을 제거해 준다. 또한 운영체제나 응용 프로그램의 보안 취약점은 악의적인 공격자에 의한 공격 경로를 제공할 수 있다. 따라서, 운영체제 제작사 등에서 업데이트 공지가 있는 경우 현재 운영중인 응용 프로그램과의 정합성을 고려하여 최신 보안패치를 적용하는 것이 필요하며, 가능한 자동으로 보안패치가 설정되도록 할 필요가 있다.

- 자동 보안패치 설정하는 방법은 보호나라 웹사이트 참조 (http://www.boho.or.kr)

8. 출력·복사시 보호조치

제8조(출력·복사시 보호조치) ①정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화 한다.
②정보통신서비스 제공자등은 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등 필요한 보호조치를 갖추어야 한다.

【취 지】

▶ 접근통제(Access Control), 암호화 등의 방법은 개인정보취급자가 아닌 비인가자에 의한 개인정보 유출을 방지하는데 효과적이나, 개인정보취급자로 인한 유출을 방지하기 위해서는 별도의 조치가 필요하다.

- 개인정보 DB가 개인정보취급자에 의해 유출되는 최종적인 경로 중 하나는 프린터 출력 및 콤팩트디스크, USB 메모리 등에 복사되는 것이다.

※ 출력·복사된 개인정보는 사용 목적 달성후 지체없이 파기되어야 하나 방치되어 유출되는 사례가 빈번하게 발생함

【해 설】

①정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화 한다.

▶ 정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보의 출력시 허가된 규칙에 의해서만 개인정보를 출력할 수 있도록 절차를 마련하여 해당 문서에서 출력되는 개인정보가 최소화될 수 있도록 관련 정책을 수행해야 한다.

▶ "용도에 따라 출력항목을 최소화"하여야 한다는 것은 대리점, 고객상담, 본사 등 각각의 다양한 업무장소나 업무형태 및 제4조제1항에 따른 개인정보처리시스템에의 접근권한에 따라 보여지는 출력항목을 다르게 설정하거나 최소화하는 것을 의미한다.

- 예를 들면 업무위탁에 따른 대리점에서 인터넷 모니터 화면을 통해 위탁된 업무와 연관이 없는 정보(이용자의 주소 등)를 볼 수 없게 하는 것 등의 조치가 이에 해당한다.

- 즉, 개인정보처리시스템을 다루는 회사에서 각각의 용도에 맞게 자율적으로 정의하여 업무처리에 필요한 범위를 초과하는 개인정보의 획득을 방지하고자 하는 것이다.

②정보통신서비스 제공자등은 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등 필요한 보호조치를 갖추어야 한다.

▶ 출력·복사시 출력·복사 기록 등 필요한 보호조치를 하는 이유는

- 출력·복사물의 생성, 이용, 전달, 파기 과정까지의 책임관계를 명확히 하여 사후 문서 유출 발생시 출처를 확인할 수 있도록 하고,

- 또한, 임의적인 고객 개인정보 명단을 출력·복사하는 행위를 억제하여 개인정보 유출 위험을 최소화하기 위해서이다.

▶ 출력·복사 기록 등 필요한 보호조치를 하는 방법

- 개인정보가 포함된 출력·복사물의 안전한 관리를 위해 관련 내용 기록 등의 보호조치를 취하여야 한다. 개인정보관리책임자는 출력·복사물의 보호조치를 위해 업무의 상황에 따라 기록할 정보를 정할 수 있지만, 출력·복사물의 책임관계 및 출처를 명확히 하기 위해 관련정보를 기록하여 관리하여야 한다.

9. 개인정보 표시제한 보호조치

제9조(개인정보 표시 제한 보호조치) 정보통신서비스 제공자등은 개인정보 업무처리를 목적으로 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보 보호를 위하여 개인정보를 마스킹하여 표시제한 조치를 취하는 경우에는 다음의 원칙으로 적용할 수 있다.

1. 성명 중 이름의 첫 번째 글자 이상
2. 생년월일
3. 전화번호 또는 휴대폰 전화번호의 국번
4. 주소의 읍·면·동
5. 인터넷주소는 버전 4의 경우 17~24비트 영역, 버전 6의 경우 113~128비트 영역

【취 지】

▶ 정보통신서비스 제공자등이 이용자의 개인정보 보호를 위해 내부 직원에게 개인정보의 마스킹을 통해 표시제한 조치를 취하려 하는 경우, 해당 사업자에게 마스킹 적용규칙을 권고하여 마스킹 방식에 있어서 일관성을 확보하기 위함이다.

【해 설】

▶ 개인정보취급자가 개인정보를 조회하거나 출력할 때 개인정보의 일부분을 마스킹하는 동일한 기준을 적용한다면 2개 이상의 사업장에서 유출된 개인정보를 이용하더라도 완전한 개인정보 집합을 구성할 수 없도록 하기 위해 표시 제한 보호조치가 필요하다.

▶ 본 조항은 필수 사항이 아닌 권고 사항으로 사업자의 서비스 목적에 따라 표시 제한 규정을 준수하지 못하는 경우에 과태료 또는 벌금 등의 제재를 부과하기 위한 목적이 아니며,

- 사업자가 개인정보 표시 제한 보호조치를 자율적으로 준수하는 경우에 일관성을 갖게 하여 개인정보 유출로 인한 2차 피해 확산을 방지하기 위함이다.

[개인정보 표시제한 보호조치가 적용된 개인정보 조회 화면(예시)]

성명	홍*동	생년월일	****년 *월 *일
전화번호	02-****-1234	핸드폰	010-****-1234
주소	서울 종로구 ***동 12-3	접속지 IP	123.123.***.123

【FAQ】

[문] 정보통신서비스제공자는 개인정보를 의무적으로 마스킹 처리하여야 합니까?

▶ 정보통신서비스제공자가 이용자의 개인정보의 보호를 위해 개인정보를 마스킹하여 표시하는 조치를 취할 경우 마스킹 방식에 관한 일관된 기준에 따를 수 있도록 권고하는 사항으로서, 의무적으로 적용해야 하는 조치는 아닙니다.

개인정보의 기술적·관리적 보호조치 기준 해설서

2012년 9월 인쇄
2012년 9월 발행

발행처: **방송통신위원회 · 한국인터넷진흥원**
110-777 서울특별시 종로구 세종대로 178
방송통신위원회
Tel: (02) 750-1114

138-950 서울특별시 송파구 중대로 109
대동빌딩 한국인터넷진흥원
Tel: (02) 405-5118

인쇄처: 호정씨앤피
Tel: (02) 2277-4718

<비매품>

개인정보의 기술적·관리적
보호조치 기준 해설서

방송통신위원회
110-777 서울시 종로구 세종대로 178 방송통신위원회
T. 02-750-1114
H. www.kcc.go.kr

KISA 한국인터넷진흥원
138-950 서울시 송파구 중대로 109 대동빌딩
T. 02-405-4118 F. 02-405-5119
H. www.kisa.or.kr