
개인정보의 기술적·관리적 보호조치 기준 해설서

2022. 10.



개인정보보호위원회



한국인터넷진흥원

본 해설서는 「개인정보보호법」(이하 “법”이라 한다.)에 따라 정보통신서비스 제공자등이 이용자의 개인정보를 처리함에 있어 안전성 확보를 위하여 필요한 「개인정보의 기술적·관리적 보호조치 기준」해설을 목적으로 합니다.

해설서에서 안내하고 있는 방법이나 예시 등은 정보통신서비스 제공자등이 처리하는 개인정보의 유형 및 중요도, 개인정보를 처리하는 방법 및 환경, 보안 위험요인 등에 따라 다르게 적용될 수 있습니다.

목 차

| | |
|---------------------------------------|----|
| I. 「개인정보의 기술적·관리적 보호조치 기준」 개요 | 1 |
| 1. 개 요 | 2 |
| 2. 법적 근거 | 3 |
| II. 「개인정보의 기술적·관리적 보호조치 기준」 전문 | 5 |
| III. 「개인정보의 기술적·관리적 보호조치 기준」 해설 | 12 |
| 제 1조 (목적) | 13 |
| 제 2조 (정의) | 22 |
| 제 3조 (내부관리계획의 수립·시행) | 31 |
| 제 4조 (접근통제) | 46 |
| 제 5조 (접속기록의 위·변조방지) | 60 |
| 제 6조 (개인정보의 암호화) | 62 |
| 제 7조 (악성프로그램 방지) | 68 |
| 제 8조 (물리적 접근 방지) | 71 |
| 제 9조 (출력·복사시 보호조치) | 73 |
| 제10조 (개인정보 표시 제한 보호조치) | 75 |
| 제11조 (재검토 기한) | 76 |
| [부칙] | 76 |
| IV. 부록 | 77 |
| 1. 정보통신서비스 제공자등을 위한 망분리 해설 | 78 |
| 2. FAQ | 91 |

I. 「개인정보의 기술적·관리적 보호조치 기준」 개요

- 1. 개 요**
- 2. 법적 근거**

I. 「개인정보의 기술적·관리적 보호조치 기준」 개요

1. 개 요

| 구 분 | 「개인정보의 기술적·관리적 보호조치 기준」 |
|-------------|--|
| 법적 근거 | <ul style="list-style-type: none"> ○ 개인정보 보호법 제29조(안전조치의무) ○ 같은 법 시행령 제48조의2의제3항(개인정보의 안전성 확보조치에 관한 특례) |
| 과징금 부과 및 벌칙 | <ul style="list-style-type: none"> ○ 위반행위와 관련한 매출액의 100분의 3 이하의 과징금(법 제39조의15제1항제5호) ○ 2년 이하의 징역 또는 2천만원 이하의 벌금(법 제73조제1호) ○ 3천만원 이하의 과태료(법 제75조제2항제6호) |
| 적용 대상 | <ul style="list-style-type: none"> ○ 정보통신서비스 제공자 ○ 정보통신서비스 제공자로부터 개인정보를 제공받은 자 ○ 정보통신서비스 제공자로부터 개인정보 처리를 위탁받은 자(이하 ‘수탁자’, 준용) ○ 방송사업자(준용) |
| 목 적 | <ul style="list-style-type: none"> ○ 정보통신서비스 제공자등이 이용자의 개인정보를 처리할 때 개인정보가 분실·도난·유출·위조·변조 또는 훼손되는 것을 방지하고 개인정보의 안전성 확보를 위하여 필요한 보호조치의 기준을 정함 |
| 성 격 | <ul style="list-style-type: none"> ○ 반드시 준수해야 하는 최소한의 기준 |
| 주요 내용 | <ul style="list-style-type: none"> ○ 내부관리계획의 수립·시행 ○ 접근통제 ○ 접속기록의 위·변조방지 ○ 개인정보의 암호화 ○ 악성프로그램 방지 ○ 물리적 접근 방지 ○ 출력·복사시 보호조치 ○ 개인정보 표시 제한 보호조치 등 |

2.

법적 근거

- 이 기준은 「개인정보 보호법」 제29조 및 같은 법 시행령 제48조의2의제3항에 근거한다.
- 따라서, 정보통신서비스 제공자등은 개인정보를 처리할 때 이 기준을 준수하여야 한다.
- 이 기준에 따른 기술적·관리적 조치를 하지 아니한 자 등에게는 관련 법률에 따라 과징금, 벌칙(징역 또는 벌금), 과태료를 부과할 수 있다.

개인정보 보호법

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.

제39조의15(과징금의 부과 등에 대한 특례) ① 보호위원회는 정보통신서비스 제공자등에게 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.

5. 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우로서 제29조의 조치(내부 관리계획 수립에 관한 사항은 제외한다)를 하지 아니한 경우(제39조의14에 따라 준용되는 경우를 포함한다)

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 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자

제48조의2(개인정보의 안전성 확보 조치에 관한 특례) ① 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제3호에 해당하는 자를 말한다. 이하 같다)와 그로부터 이용자(같은 법 제2조제1항제4호에 해당하는 자를 말한다. 이하 같다)의 개인정보를 법 제17조제1항제1호에 따라 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)는 이용자의 개인정보를 처리하는 경우에는 제30조에도 불구하고 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다.

1. 개인정보의 안전한 처리를 위한 다음 각 목의 내용을 포함하는 내부관리계획의 수립·시행
 - 가. 개인정보 보호책임자의 지정 등 개인정보 보호 조직의 구성·운영에 관한 사항
 - 나. 정보통신서비스 제공자등의 지휘·감독을 받아 이용자의 개인정보를 처리하는 자(이하 이 조에서 "개인정보취급자"라 한다)의 교육에 관한 사항
 - 다. 제2호부터 제6호까지의 규정에 따른 조치를 이행하기 위하여 필요한 세부 사항
2. 개인정보에 대한 불법적인 접근을 차단하기 위한 다음 각 목의 조치
 - 가. 개인정보를 처리할 수 있도록 체계적으로 구성된 데이터베이스시스템(이하 이 조에서 "개인정보처리시스템"이라 한다)에 대한 접근 권한의 부여·변경·말소 등에 관한 기준의 수립·시행
 - 나. 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영
 - 다. 개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등에 대한 외부 인터넷망 차단(전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제2호에 따른 정보통신서비스를 말한다. 이하 같다) 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등만 해당한다)
 - 라. 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정 및 운영
 - 마. 그 밖에 개인정보에 대한 접근 통제를 위하여 필요한 조치
3. 접속기록의 위조·변조 방지를 위한 다음 각 목의 조치
 - 가. 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독
 - 나. 개인정보처리시스템에 대한 접속기록을 별도의 저장장치에 백업 보관
4. 개인정보가 안전하게 저장·전송될 수 있도록 하기 위한 다음 각 목의 조치
 - 가. 비밀번호의 일방향 암호화 저장
 - 나. 주민등록번호, 계좌정보 및 제18조제3호에 따른 정보 등 보호위원회가 정하여 고시하는 정보의 암호화 저장
 - 다. 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안 서버 구축 등의 조치
 - 라. 그 밖에 암호화 기술을 이용한 보안조치
5. 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 하기 위한 백신소프트웨어 설치 및 주기적 갱신·점검 조치
6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 조치
 - ② 보호위원회는 정보통신서비스 제공자등이 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 기술적·관리적 보호조치 기준」 전문

II. 「개인정보의 기술적·관리적 보호조치 기준」 전문

개정 2021. 9. 15. 개인정보보호위원회 고시 제2021-3호

제1조(목적) ① 이 기준은 「개인정보 보호법」(이하 “법”이라 한다) 제29조 및 같은 법 시행령 제48조의2제3항에 따라 정보통신서비스 제공자등(법 제39조의14에 따라 준용되는 자를 포함한다. 이하 같다)이 이용자의 개인정보를 처리함에 있어서 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성 확보를 위하여 필요한 기술적·관리적 보호조치의 최소한의 기준을 정하는 것을 목적으로 한다.

② 정보통신서비스 제공자등은 사업규모, 개인정보 보유 수 등을 고려하여 스스로의 환경에 맞는 개인정보 보호조치 기준을 수립하여 시행하여야 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. “개인정보 보호책임자”란 이용자의 개인정보보호 업무를 총괄하거나 업무처리를 최종 결정하는 임직원을 말한다.
2. “개인정보취급자”란 이용자의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.
3. “내부관리계획”이라 함은 정보통신서비스 제공자등이 개인정보의 안전한 처리를 위하여 개인정보보호 조직의 구성, 개인정보취급자의 교육, 개인정보 보호조치 등을 규정한 계획을 말한다.
4. “개인정보처리시스템”이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성된 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. "생체정보"라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
- 8의2. "생체인식정보"라 함은 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.
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.
13. "모바일 기기"란 스마트폰, 태블릿PC 등 무선망을 이용할 수 있는 휴대용 기기를 말한다.
14. "보조저장매체"란 이동형 하드디스크(HDD), USB메모리, CD(Compact Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 쉽게 분리·접속할 수 있는 저장매체를 말한다.

제3조(내부관리계획의 수립.시행) ① 정보통신서비스 제공자등은 다음 각 호의 사항을 정하여 개인정보보호 조직을 구성·운영하여야 한다.

1. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
 2. 개인정보 보호책임자와 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. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
 6. 개인정보의 분실·도난·유출·위조·변조·훼손 등이 발생한 경우의 대응 절차 및 방법에 관한 사항
 7. 그 밖에 개인정보보호를 위해 필요한 사항
- ② 정보통신서비스 제공자등은 다음 각 호의 사항을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수 등을 고려하여 필요한 교육을 정기적으로 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 개인정보 보호책임자 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 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 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업 연도를 말한다) 매출액이 100억원 이상인 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. 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성

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 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보 처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.
- ⑩ 정보통신서비스 제공자등은 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 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 1년 이상 접속기록을 보존·관리하여야 한다.

② 단, 제1항의 규정에도 불구하고 「전기통신사업법」 제5조의 규정에 따른 기간통신사업자의 경우에는 보존·관리해야 할 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 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.

② 정보통신서비스 제공자등은 다음 각 호의 정보에 대해서는 안전한 암호알고리즘으로 암호화하여 저장한다.

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

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 암호화

하여 송·수신하는 기능

2. 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능

④ 정보통신서비스 제공자등은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화해야 한다.

제7조(악성프로그램 방지) 정보통신서비스 제공자등은 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각호의 사항을 준수하여야 한다.

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

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

제8조(물리적 접근 방지) ① 정보통신서비스 제공자등은 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소에 대한 출입통제 절차를 수립·운영하여야 한다.

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

③ 정보통신서비스 제공자등은 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다.

제9조(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·복사기록 등 필요한 보호조치를 갖추어야 한다.

제10조(개인정보 표시 제한 보호조치) 정보통신서비스 제공자 등은 개인정보 업무처리를 목적으로 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보보호를 위하여 개인정보를 마스킹하여 표시제한 조치를 취할 수 있다.

제11조(재검토 기한) 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.

부칙<제2020-5호, 2020.8.11.>

이 고시는 고시한 날부터 시행한다.

부칙<제2021-3호, 2021.9.15.>

이 고시는 고시한 날부터 시행한다.

III. 「개인정보의 기술적·관리적 보호조치 기준」 해설

제 1 조 [목적]

제 2 조 [정의]

제 3 조 [내부관리계획의 수립·시행]

제 4 조 [접근통제]

제 5 조 [접속기록의 위·변조방지]

제 6 조 [개인정보의 암호화]

제 7 조 [악성프로그램 방지]

제 8 조 [물리적 접근 방지]

제 9 조 [출력·복사시 보호조치]

제10조 [개인정보 표시 제한 보호조치]

제11조 [재검토 기한]

III. 「개인정보의 기술적·관리적 보호조치 기준」 해설

제 1 조

목적

제1조(목적) ① 이 기준은 「개인정보 보호법」(이하 “법”이라 한다) 제29조 및 같은 법 시행령 제48조의2제3항에 따라 정보통신서비스 제공자등(법 제39조의14에 따라 준용되는 자를 포함한다. 이하 같다)이 이용자의 개인정보를 처리함에 있어서 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성 확보를 위하여 필요한 기술적·관리적 보호조치의 최소한의 기준을 정하는 것을 목적으로 한다.

② 정보통신서비스 제공자등은 사업규모, 개인정보 보유 수 등을 고려하여 스스로의 환경에 맞는 개인정보 보호조치 기준을 수립하여 시행하여야 한다.



① 이 기준은 「개인정보 보호법」(이하 “법”이라 한다) 제29조 및 같은 법 시행령 제48조의2제3항에 따라 정보통신서비스 제공자등(법 제39조의14에 따라 준용되는 자를 포함한다. 이하 같다)이 이용자의 개인정보를 처리함에 있어서 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성 확보를 위하여 필요한 기술적·관리적 보호조치의 최소한의 기준을 정하는 것을 목적으로 한다.

■ 이 기준은 「개인정보 보호법」 제29조 및 같은 법 시행령 제48조의2제3항에 근거한다.

개인정보 보호법

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

제48조의2(개인정보의 안전성 확보 조치에 관한 특례) ① 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제3호에 해당하는 자를 말한다. 이하 같다)와 그로부터 이용자(같은 법 제2조제1항제4호에 해당하는 자를 말한다. 이하 같다)의 개인정보를 법 제17조제1항제1호에 따라 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)는 이용자의 개인정보를 처리하는 경우에는 제30조에도 불구하고 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다.

1. 개인정보의 안전한 처리를 위한 다음 각 목의 내용을 포함하는 내부관리계획의 수립·시행
가. 개인정보 보호책임자의 지정 등 개인정보 보호 조직의 구성·운영에 관한 사항
나. 정보통신서비스 제공자등의 지휘·감독을 받아 이용자의 개인정보를 처리하는 자(이하 이 조에서 "개인정보취급자"라 한다)의 교육에 관한 사항
다. 제2호부터 제6호까지의 규정에 따른 조치를 이행하기 위하여 필요한 세부 사항
2. 개인정보에 대한 불법적인 접근을 차단하기 위한 다음 각 목의 조치
가. 개인정보를 처리할 수 있도록 체계적으로 구성된 데이터베이스시스템(이하 이 조에서 "개인정보처리시스템"이라 한다)에 대한 접근 권한의 부여·변경·말소 등에 관한 기준의 수립·시행
나. 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영
다. 개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등에 대한 외부 인터넷망 차단[전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제2호에 따른 정보통신서비스를 말한다. 이하 같다) 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등만 해당한다]
라. 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정 및 운영
마. 그 밖에 개인정보에 대한 접근 통제를 위하여 필요한 조치
3. 접속기록의 위조·변조 방지를 위한 다음 각 목의 조치
가. 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독
나. 개인정보처리시스템에 대한 접속기록을 별도의 저장장치에 백업 보관
4. 개인정보가 안전하게 저장·전송될 수 있도록 하기 위한 다음 각 목의 조치
가. 비밀번호의 일방향 암호화 저장
나. 주민등록번호, 계좌정보 및 제18조제3호에 따른 정보 등 보호위원회가 정하여 고시하는 정보의 암호화 저장
다. 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안 서버 구축 등의 조치
라. 그 밖에 암호화 기술을 이용한 보안조치
5. 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록

하기 위한 백신소프트웨어 설치 및 주기적 갱신·점검 조치

6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 조치

② 보호위원회는 정보통신서비스 제공자등이 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 개인정보를 처리하는 정보통신서비스 제공자등(법 제39조의14에 따라 준용되는 자를 포함한다.)에게 적용된다.

- 정보통신서비스 제공자 : 「전기통신사업법」에 의한 전기통신사업자(기간·부가통신사업자) 및 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

참 고

☞ 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자 : 인터넷 홈페이지 등을 이용하여 정보 및 서비스를 제공하는 자를 의미하며, 보통 영업 행위를 하는 주체가 홈페이지를 개설하고 회원가입을 받을 때에는 모두 적용 대상이 된다. ('영리를 목적'은 자기 또는 제3자의 재산적 이익을 얻기 위한 목적을 말하는 것으로 해석하고 있으며 여기서의 이익은 계속적, 반복적일 필요가 없다.)

- 정보통신서비스 제공자로부터 이용자의 개인정보를 제공받은 자 : 「개인정보 보호법」 제17조에 따라 정보통신서비스 제공자로부터 이용자의 개인정보를 제공받은 자를 말한다.

개인정보 보호법

제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.

1. 정보주체의 동의를 받은 경우

2. 제15조제1항제2호·제3호·제5호 및 제39조의3제2항제2호·제3호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보를 제공받는 자

2. 개인정보를 제공받는 자의 개인정보 이용 목적

3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

제39조의3(개인정보의 수집·이용 동의 등에 대한 특례) ② 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 제1항에 따른 동의 없이 이용자의 개인정보를 수집·이용할 수 있다.

2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
3. 다른 법률에 특별한 규정이 있는 경우

-
- 방송사업자 : 「개인정보 보호법」 제39조의14에 따라 제29조 등을 준용한다.
 - 수탁자 : 「개인정보 보호법」 제26조제7항에 따라 제29조 등을 준용한다.

개인정보 보호법

제39조의14(방송사업자등에 대한 특례) 「방송법」 제2조제3호가목부터 마목까지와 같은 조 제6호·제9호·제12호 및 제14호에 해당하는 자(이하 이 조에서 "방송사업자등"이라 한다)가 시청자의 개인정보를 처리하는 경우에는 정보통신서비스 제공자에게 적용되는 규정을 준용한다. 이 경우 "방송사업자등"은 "정보통신서비스 제공자" 또는 "정보통신서비스 제공자등"으로, "시청자"는 "이용자"로 본다.

제26조(업무위탁에 따른 개인정보의 처리 제한) ⑦ 수탁자에 관하여는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.

참 고

| | | | | |
|-----------------|---------------------------------|--|-----------------------------|---|
| 기준 적용 대상자 | 정 보 통 신 서 비 스 | 정 기 통 신 사 업 자 | 기간통신사업자 (전기통신사업법 제5조제2항) | 음성·데이터 등의 송·수신, 주파수 할당·제공, 전기통신회선설비임대역무, 기간통신역무제공 등 |
| | | | 부가통신사업자 (전기통신사업법 제5조제3항) | 기간통신사업자의 전기통신회선설비를 임차하여 기간통신역무 외의 전기통신역무 제공 등 |
| | 제 공 자 등 | 영리를 목적으로 전기통신사업자의 전기통신역무를 이용해 정보를 제공하거나 매개하는 자 | | 인터넷 홈페이지 등을 운영하는 영리를 목적으로 하는 사업자 등 |
| | | 정보통신서비스 제공자로부터 법 제17조에 따라 이용자의 동의를 얻어 개인정보를 제공받은 자 | | 업무제휴 등을 위해 이용자의 동의를 얻어 개인정보를 제공받은 자 등 |
| | 방송사업자 (개인정보 보호법 제39조의14) | | | 시청자의 개인정보를 수집·이용 또는 제공하는 자 등 (IPTV 사업자는 직접 적용) |
| | 수탁자 (개인정보 보호법 제26조) | | | 수탁자는 법 제29조의 기술적·관리적 보호조치 규정을 준용 등 |
| | 다른 법률에서 이 법의 적용을 받는 자 | | | 다른 법률에서 특별히 규정된 때 등 |

– 이외, 다른 법률에서 「개인정보 보호법」의 관련 규정을 준용할 것을 명시할 때에는 이 기준이 적용된다.

- 정보통신서비스 제공자 등은 이용자의 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 보호조치를 취하여야 한다.

– 특히, 개인의 생명·신체·재산상 안전에 중대한 영향을 미칠 수 있는 고유 식별정보 또는 민감정보를 처리하는 경우 법 제23조(민감정보의 처리 제한) 제2항, 제24조(고유식별정보의 처리 제한)제3항 및 같은 법 시행령 제21조(고유식별정보의 안전성 확보조치)에 따라 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 하여야 한다.

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.

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.

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

- 정보통신서비스 제공자 등이 가명정보 및 추가 정보를 처리하는 경우, 법 제28조의4 및 동법 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(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(가명정보 등의 안전성 확보조치 등) ① 개인정보처리자는 법 제28조의4제1항에 따라 가명정보 및 추가 정보에 대하여 다음 각 호의 안전성 확보에 필요한 조치를 하여야 한다.

1. 제30조제1항·제2항에 따른 안전성 확보 조치
2. 가명정보와 추가 정보를 분리하여 보관(추가정보가 불필요한 경우에는 추가정보의 파기)
3. 가명정보와 추가 정보에 대한 접근 권한 분리(다만, 「소상공인 보호 및 지원에 관한 법률」 제2조에 따른 소상공인으로서 가명정보를 취급할 자를 추가로 둘 여력이 없는 경우 등 접근권한의 분리가 어려운 정당한 사유가 있는 경우에는 접근 권한 관리·통제)

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.
-

■ 정보통신서비스 제공자등의 스스로의 환경에 맞는 개인정보 보호조치에 관한 기준을 ‘최소한의 기준’으로 정함을 원칙으로 한다.

- 정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보가 분실·도난·유출·위조·변조 또는 훼손 등이 되지 않도록 기술적·관리적 및 물리적 보호조치에 관한 최소한의 기준을 준수하여야 한다.
- 정보통신서비스 제공자등은 사업규모, 서비스의 유형, 개인정보 보유 수, 처리하는 개인정보의 유형 및 중요도, 개인정보를 처리하는 방법 및 환경, 보안위험요인 등을 고려하여 스스로의 환경에 맞는 개인정보 보호조치 기준을 수립하고 시행하여야 한다.

- 정보통신서비스 제공자등이 이 기준을 준수하지 않은 경우에는 「개인정보 보호법」의 관련 규정에 따라 제재받을 수 있다.

개인정보 보호법

제39조의15(과징금의 부과 등에 대한 특례) ① 보호위원회는 정보통신서비스 제공자등에게 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.

5. 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우로서 제29조의 조치(내부 관리계획 수립에 관한 사항은 제외한다)를 하지 아니한 경우(제39조의14에 따라 준용되는 경우를 포함한다)

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 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자
-

② 정보통신서비스 제공자등은 사업규모, 개인정보 보유 수 등을 고려하여 스스로의 환경에 맞는 개인정보 보호조치 기준을 수립하여 시행하여야 한다.

- 정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성 확보를 위하여 필요한 보호조치를 하여야 한다.
- 개인정보의 안전성 확보를 위하여 필요한 개인정보 보호조치 기준은 다음과 같은 사항 등을 고려하여 수립하여야 한다.
 - 이 기준에서 정하는 기술적·관리적 및 물리적 보호조치에 관한 사항은 모두 포함하여야 한다.
 - 사업규모, 서비스의 유형, 개인정보 보유 수, 처리하는 개인정보의 유형 및 중요도, 개인정보를 처리하는 방법 및 환경, 보안위험요인 등을 고려하여 스스로의 환경에 맞는 개인정보 보호조치 기준을 수립하여야 한다.

개인정보 보호조치 기준 (예시)

- ☞ 이 기준에서 최소한으로 정하는 수준 이상의 기술적·관리적 및 물리적 보호조치
 - * 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경 → 분기별 1회 이상 변경
- ☞ 그 밖에 개인정보보호를 위해 필요한 사항
 - * 웹 해킹 위험이 높은 경우에는 웹방화벽을 도입하고 정책설정, 이상행위 대응 등 운영·관리에 관한 사항 등을 수립 등

- 정보통신서비스 제공자등은 수립한 개인정보 보호조치 기준에 따라 시행하여야 한다.

참 고

- ☞ 이 기준 제1조제2항의 ‘개인정보 보호조치 기준’은 제3조제3항에 따른 ‘내부관리계획’에 포함하여 수립·시행하도록 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. “개인정보 보호책임자”란 이용자의 개인정보보호 업무를 총괄하거나 업무 처리를 최종 결정하는 임직원을 말한다.
2. “개인정보취급자”란 이용자의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.
3. “내부관리계획”이라 함은 정보통신서비스 제공자등이 개인정보의 안전한 처리를 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. “생체정보”라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보를 말한다.

8의2. "생체인식정보"라 함은 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.

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.

13. "모바일 기기"란 스마트폰, 태블릿PC 등 무선망을 이용할 수 있는 휴대용 기기를 말한다.


14. "보조저장매체"란 이동형 하드디스크(HDD), USB메모리, CD(Compact Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 쉽게 분리·접속할 수 있는 저장매체를 말한다.

해설

1. "개인정보 보호책임자"란 이용자의 개인정보보호 업무를 총괄하거나 업무처리를 최종 결정하는 임직원을 말한다.

- 정보통신서비스 제공자등은 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보 보호책임자를 지정 요건에 맞게 지정하고, 법률에 따라 업무를 수행하도록 보장하여야 한다.


참 고

 개인정보 보호책임자의 자격요건 및 지정 등에 관한 사항은 이 기준 제3조제1항 해설에서 보다 자세하게 확인할 수 있다.

2. “개인정보취급자”란 이용자의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.

- 개인정보취급자란 정보통신서비스 제공자의 지휘·감독을 받아 이용자의 개인정보를 처리하는 자로서, 고용관계가 없더라도 실질적으로 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자는 개인정보취급자에 포함된다.
 - 지휘·감독 : 조직·인사 상의 지휘·감독 뿐만 아니라, 개인정보 처리 또는 시스템 등과 관련된 정책상의 지휘·감독을 포함할 수 있다.
 - 처리 : 개인정보를 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.
 - 개인정보취급자는 근로형태를 불문하며, 이용자의 개인정보를 처리한다면 정규직, 비정규직, 파견직, 시간제 근로자 등이 모두 이에 해당한다. 또한 고용관계가 없더라도 실질적으로 정보통신서비스 제공자의 지휘·감독을 받아 이용자의 개인정보를 처리하는 자도 개인정보취급자에 포함된다.(예시: 이동통신사 영업점, 오픈마켓 판매자 등)

참 고

 개인정보취급자의 역할 및 책임 등에 관한 사항은 이 기준 제3조제1항 해설에서 보다 자세하게 확인할 수 있다.

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

- 내부관리계획이란 정보통신서비스 제공자등이 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성 확보를 위하여 필요한 사항 등을 규정한 계획, 지침 등을 말한다.

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

- 여기서 말하는 데이터베이스시스템이란 일반적으로 데이터가 저장되는 데이터베이스(DB)와 데이터베이스 내의 데이터를 처리할 수 있도록 해주는 데이터베이스 관리 시스템(DBMS), 응용프로그램 등이 통합된 것을 의미한다.
- 따라서 개인정보처리시스템에는 개인정보가 저장되는 데이터베이스(DB), 데이터베이스를 생성하고 관리하는 데이터베이스 관리 시스템(DBMS), 데이터베이스를 용이하게 이용하는데 필요한 응용프로그램 등 데이터베이스시스템의 구성요소가 모두 포함된다.
- 개인정보처리시스템은 정보통신서비스 제공자등의 개인정보 처리 방법, 시스템 구성 및 운영 환경 등에 따라 달라질 수 있다.

개인정보처리시스템 (예시)

- ☞ 데이터베이스를 구성·운영하는 시스템 그 자체
- ☞ 응용프로그램(Web 서버, WAS 등) 등을 데이터베이스의 개인정보를 처리할 수 있도록 구성한 때
- ☞ 개인정보의 처리를 위해 파일처리시스템으로 구성한 때 등


- 업무용 컴퓨터, 노트북 등도 데이터베이스 관련 응용프로그램이 설치·운영되어 개인정보 취급자가 개인정보를 처리할 수 있도록 구성되었다면 개인정보처리시스템에 해당될 수 있다.

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

- 망분리는 정보통신서비스 제공자등이 개인정보를 처리하는 과정에서의 외부와의 접점을 차단하여 외부로부터 들어오는 공격이나, 내부에서 외부로의 개인정보 유출 등을 차단하기 위한 조치를 말한다.

- 망분리는 업무망과 외부 인터넷망에 속하거나 접근하는 컴퓨터를 각 각 분리하여 두 영역이 서로 접근할 수 없도록 하는 것으로 일반적으로 다음과 같이 구분할 수 있으며 기술 발전에 따라 확대될 수 있다.
 - 물리적 망분리 : 통신망, 장비 등을 물리적으로 이원화하여 인터넷 접속이 불가능한 컴퓨터와 인터넷 접속만 가능한 컴퓨터로 분리하는 방식이다.
 - 논리적 망분리 : 물리적으로 하나의 통신망, 장비 등을 사용하지만 가상화 등의 방법으로 내부 업무영역과 인터넷 접속영역을 분리하는 방식이다.

참 고

 불법적인 접근 : 인가되지 않은 자(내·외부자 모두 포함)가 사용자계정 탈취, 자료유출 등의 목적으로 개인정보처리시스템, 개인정보취급자의 컴퓨터 등에 접근하는 것을 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.

- 식별자는 정보주체 식별을 위한 목적으로 사용되는 ID, 사용자 이름, 사용자 계정명 등을 말한다.
- 문자열은 영대문자(A~Z), 영소문자(a~z), 숫자(0~9), 특수문자(~, !, @ 등)을 말한다.
- 타인에게 공개되지 않은 정보의 의미는 타인이 비밀번호를 파악할 수 있도록 관리되어서는 안 된다는 것이다. 이는 본인 이외의 내부직원 또는 비인가자나 공격자 등이 개인정보처리시스템 등에 접속하여 개인정보를 유출하는 등 불법행위가 가능하기 때문이다.

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.

- 접속기록은 이용자와 개인정보취급자 등의 접속기록을 모두 포함한다.
- 식별자는 개인정보처리시스템에 접속한 자를 식별할 수 있도록 부여된 ID 등을 말한다.
- 접속일시는 개인정보처리시스템에 접속한 시점 또는 업무를 수행한 시점(년-월-일, 시:분:초)을 말한다.
- 접속지를 알 수 있는 정보는 개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소 등을 말한다.
- 수행업무는 이용자 또는 개인정보취급자가 개인정보처리시스템을 이용하여 수행한 업무를 알 수 있는 정보를 말한다.
 - 이용자 측면에서는 자신의 개인정보 조회, 수정, 탈퇴 등을 한 내용을 알 수 있는 정보를 말한다.
 - 개인정보취급자 측면에서는 개인정보처리시스템에서 처리(개인정보를 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 행위)한 내용을 알 수 있는 정보를 말한다.
- 전자적으로 기록한 것이란 수기로 작성한 문서가 아니라 개인정보처리시스템의 로그(Log) 파일 또는 로그관리시스템 등에 전자적으로 기록한 것을 말한다.

8. "생체정보"라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 일정한 기술적 수단을 통해 처리되는 정보를 말한다.

- 생체정보는 특정 개인을 인증·식별하거나 개인의 특징을 알아보기 위한 목적으로 처리되는 정보로서 신체적 특징, 생리적 특징과 행동적 특징을 기반으로 생성된 정보로 구분할 수 있다.
 - 신체적 특징 : 지문, 얼굴, 홍채·망막의 혈관 모양, 손바닥·손가락의 정맥 모양, 장문, 귓바퀴의 모양 등
 - 생리적 특징 : 뇌파, 심전도, 유전정보 등
 - 행동적 특징 : 음성, 필적, 걸음걸이, 자판입력 간격·속도 등

- ‘특정 개인을 인증·식별’은 지문·홍채·얼굴 등에서 추출한 특징점 등을 이용(비교·대조)하여 특정 개인임을 확인하는 것을 의미하고, ‘개인에 관한 특징을 알아보기 위해’는 인증·식별 이 외의 목적으로 사람의 연령·성별·감정 등의 상태를 확인 또는 분류하는 것을 의미한다.
- 열람·보관 등을 목적으로 수집하는 일반적인 얼굴 사진, 음성파일 등 개인의 신체적, 생리적, 행동적 특징에 관한 정보가 ‘특정 개인을 인증·식별하거나 개인에 관한 특징을 알아보기 위해 기술적으로 처리’되지 않는다면 생체정보가 아닌 일반적인 개인정보에 해당한다.

8의2. "생체인식정보"라 함은 생체정보 중 특정 개인을 인증 또는 식별할 목적으로 일정한 기술적 수단을 통해 처리되는 정보를 말한다.

- 지문, 얼굴, 홍채, 정맥, 음성, 필적 등의 생체정보가 특정 개인을 인증 또는 식별할 목적으로 사용되는 경우 생체인식정보에 해당하며, 생체인식정보는 제6조 제2항에 따라 안전한 알고리즘으로 암호화하여 저장해야 한다.

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

- P2P는 서버 등의 중간매개자 없이 정보 제공자(개인)와 정보 수신자(개인)가 직접 연결되어 각 개인이 가지고 있는 파일 등을 공유하는 것을 말한다.(개인↔개인)
- 정보 제공자 및 정보 수신자 모두가 동시에 접속하지 않고서도 정보 제공자가 어떠한 파일을 공유하면 정보 수신자가 그 파일을 내려 받을 수 있는 형태를 말한다.
 - 개인이 인터넷 상에서 정보 검색 등을 통해 파일을 찾는 방식(개인↔서버)과는 다른 개념이다.

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

- 공유설정은 컴퓨터 소유자의 파일, 폴더 등을 타인이 접근하여 조회, 변경, 복사 등을 할 수 있도록 권한을 설정하는 것을 말한다.

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

- 보안서버는 정보통신망에서 송·수신하는 정보를 암호화하는 기능을 말한다.{이용자 PC↔(암호화 통신)↔개인정보처리시스템 등}
- 보안서버는 일반적으로 서버기반 시스템의 유효성을 증명하여 보안 인증서를 설치하거나 암호화 소프트웨어를 설치하여 암호 통신 기능을 제공한다. 주요 보안 프로토콜에는 SSL/TLS, SHTTP, PCT 및 IPSec 등이 있다.

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 ID 등의 정보로서, 시스템에 등록 시 이용자가 선택하거나 계정(또는 권한) 관리자가 부여한 고유한 문자열이다.
- ‘신원을 검증하는데 사용되는 정보’는 해당 시스템에서 업무를 수행할 수 있는 정당한 식별자임을 증명하기 위하여 식별자와 연계된 정보로서 비밀번호, 생체인식정보, 전자서명값 등이 있다.


13. “모바일 기기”란 스마트폰, 태블릿PC 등 무선망을 이용할 수 있는 휴대용 기기를 말한다.

- 모바일 기기는 손에 들거나 몸에 간편하게 지니고 다닐 수 있는 스마트폰, 태블릿PC 등 무선망(이동통신망, 와이파이(Wi-Fi) 등)을 이용할 수 있는 휴대용 기기를 말한다.

14. “보조저장매체”란 이동형 하드디스크(HDD), USB메모리, CD(Compact Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 쉽게 분리·접속할 수 있는 저장매체를 말한다.

- 보조저장매체에는 이동형 하드디스크, USB메모리, CD, SD메모리카드 등은 물론 경우에 따라 스마트폰도 포함될 수 있다.

참 고

 이 기준에서 정의되지 않은 용어 정의는 통상적인 IT용어 정의와 같다.

제3조(내부관리계획의 수립·시행) ① 정보통신서비스 제공자등은 다음 각 호의 사항을 정하여 개인정보보호 조직을 구성·운영하여야 한다.

1. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
2. 개인정보 보호책임자와 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. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
6. 개인정보의 분실·도난·유출·위조·변조·훼손 등이 발생한 경우의 대응절차 및 방법에 관한 사항
7. 그 밖에 개인정보보호를 위해 필요한 사항

② 정보통신서비스 제공자등은 다음 각 호의 사항을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수 등을 고려하여 필요한 교육을 정기적으로 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.

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

■ 정보통신서비스 제공자등은 개인정보를 안전하게 처리하기 위하여 다음 각 호의 사항을 정하여 개인정보보호 조직을 구성하고 운영하여야 한다.

1. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
2. 개인정보 보호책임자와 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. 개인정보 처리업무를 위탁하는 경우 수탁자 관리 및 감독에 관한 사항
6. 개인정보의 분실·도난·유출·변조·훼손 등이 발생한 때의 대응절차 및 방법에 관한 사항
7. 그 밖에 개인정보보호를 위해 필요한 사항

참 고

☞ 그 밖에 개인정보보호를 위해 필요한 사항으로는 정보통신서비스 제공자등의 사업규모, 서비스의 유형, 개인정보 보유 수, 처리하는 개인정보의 유형 및 중요도, 개인정보를 처리하는 방법 및 환경, 보안위험요인 등을 고려하도록 한다.

■ 개인정보보호 조직은 인사명령, 업무분장, 내부관리계획 등에 명시하도록 하며 해당 인력의 역량 및 요건 등 적정성에 관한 사항 등을 추가적으로 정할 수 있다.

1. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항

- 정보통신서비스 제공자등은 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보 보호책임자를 인사명령 등을 통해 공식적으로 지정하여야 한다.
- 책임 있는 의사결정을 할 수 있는 임원, 개인정보의 처리에 대해 실질적 권한을 가지는 부서의 장 등을 개인정보 보호책임자로 지정할 수 있다.
- 정보통신서비스 제공자등은 스스로의 환경을 고려하여 다음의 법률에서 정하는 자격요건을 충족한 자를 개인정보 보호책임자로 지정하여야 하며, 이에 관한 사항을 내부관리계획에 포함하여야 한다.

개인정보 보호법

- 제31조(개인정보 보호책임자의 지정)** ① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다.
- 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.
- ⑥ 개인정보 보호책임자의 지정요건, 업무, 자격요건, 그 밖에 필요한 사항은 대통령령으로 정한다.

개인정보 보호법 시행령

- 제32조(개인정보 보호책임자의 업무 및 지정요건 등)** ① 법 제31조 제2항 제7호에서 "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
- ② 개인정보처리자는 법 제31조 제1항에 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. 제2조 제5호에 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)

참 고

☞ 개인정보 보호책임자(CPO)와 「정보통신망법」 제45조의3에서 정하고 있는 정보보호 최고책임자(CISO)는 동일인으로 지정하거나 또는 별도로 지정할 수 있다.

* 기술적·관리적 및 물리적 보호조치에 관하여 상호간의 명확한 업무분장 필요

2. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항

- 개인정보 보호책임자는 정보통신서비스 제공자등의 개인정보보호에 관한 업무를 총괄하여야 한다.
 - 개인정보보호 관련 계획 수립·시행, 처리 실태 조사 및 개선, 이용자 고충 처리, 내부통제시스템 구축 등의 역할을 한다.
 - 개인정보 처리 실태 등에 대하여 조사하거나 관계 당사자로부터 보고를 받을 수 있으며, 필요하면 정보통신서비스 제공자등의 사업주 또는 대표자에게 조사결과 및 개선조치를 보고하는 등 개인정보보호 업무에 관하여 책임질 수 있어야 한다.

개인정보 보호책임자의 역할 및 책임 (예시)

- ☞ 개인정보보호 관련 계획 수립 및 시행
- ☞ 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
- ☞ 개인정보 처리와 관련한 불만의 처리 및 피해 구제
- ☞ 개인정보 유출 및 오·남용 방지를 위한 내부통제시스템의 구축
- ☞ 개인정보보호 교육 계획 수립 및 시행
- ☞ 개인정보파일의 보호 및 관리·감독
- ☞ 개인정보 처리방침의 수립·변경 및 시행
- ☞ 개인정보 보호 관련 자료의 관리
- ☞ 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기 등

- 개인정보취급자는 정보통신서비스 제공자의 지휘·감독을 받아 이용자의 개인정보를 처리(개인정보를 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 행위)하는 역할을 한다.

개인정보취급자의 역할 및 책임 (예시)

- ☞ 내부관리계획 등 각종 규정, 지침 등 준수
- ☞ 개인정보처리시스템의 안전한 운영 및 관리
- ☞ 개인정보의 기술적·관리적 보호조치 기준 이행
- ☞ 개인정보보호 교육 참석
- ☞ 개인정보 침해사고 발생 시 대응 및 보고
- ☞ 개인정보 처리 현황, 처리 체계 등의 점검 및 보고 등

- 정보통신서비스 제공자등은 스스로의 환경에 맞도록 개인정보 보호책임자와 개인정보 취급자의 역할 및 책임에 관한 사항을 내부관리계획에 포함하여야 한다.

개인정보 보호법

제31조(개인정보 보호책임자의 지정) 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.

제39조의15(과징금의 부과 등에 대한 특례) ① 보호위원회는 정보통신서비스 제공자등에게 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.

4. 제26조제4항(제39조의14에 따라 준용되는 경우를 포함한다)에 따른 관리·감독 또는 교육을 소홀히 하여 특례 수탁자가 이 법의 규정을 위반한 경우

5. 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우로서 제29조의 조치(내부 관리계획 수립에 관한 사항은 제외한다)를 하지 아니한 경우(제39조의14에 따라 준용되는 경우를 포함한다)

제65조(고발 및 징계권고) ① 보호위원회는 개인정보처리자에게 이 법 등 개인정보 보호와 관련된 법규의 위반에 따른 범죄혐의가 있다고 인정될 만한 상당한 이유가 있을 때에는 관할 수사기관에 그 내용을 고발할 수 있다.

② 보호위원회는 이 법 등 개인정보 보호와 관련된 법규의 위반행위가 있다고 인정될 만한 상당한 이유가 있을 때에는 책임이 있는 자(대표자 및 책임있는 임원을 포함한다)를 징계할 것을 해당 개인정보처리자에게 권고할 수 있다. 이 경우 권고를 받은 사람은 이를 존중하여야 하며 그 결과를 보호위원회에 통보하여야 한다.

3. 개인정보 내부관리계획의 수립 및 승인에 관한 사항

- 정보통신서비스 제공자등은 스스로의 환경을 고려하여 내부관리계획의 수립에 관한 사항을 마련하여야 한다.

- 내부관리계획은 조직(회사) 전체를 대상으로 마련
- 이 기준에서 정하는 기술적·관리적 및 물리적 보호조치에 관한 사항은 모두 포함

참 고

- ☞ 내부관리계획의 문서 제목은 가급적 “내부관리계획”이라는 용어를 사용하는 것이 바람직하나, 정보통신서비스 제공자등의 내부 방침에 따라 다른 용어를 사용 할 수 있다.
- ☞ 다른 용어를 사용할 때에도 이 기준에 관한 사항을 이행하여야 한다.

- 법률 또는 이 기준에서 규정하는 내용만을 그대로 반영하는 것이 아니라, 스스로의 환경에 맞는 내부관리계획을 수립

참 고

- ☞ 사업규모, 서비스의 유형, 개인정보 보유 수, 처리하는 개인정보의 유형 및 중요도, 개인정보를 처리하는 방법 및 환경, 보안위험요인 등을 고려

- 내부관리계획을 구체적으로 수립하고, 이를 기초로 세부 지침, 절차, 가이드, 안내서 등을 추가적으로 수립 등

- 정보통신서비스 제공자등은 스스로의 환경을 고려하여 수립한 내부관리계획의 승인에 관한 사항을 다음과 같이 마련하여야 한다.

- 내부관리계획은 전사적인 계획 내에서 시행될 수 있도록 사업주 또는 대표자에게 내부결재 등의 승인을 득함
- 사내 게시판 게시, 교육 등의 방법으로서 모든 임직원 및 관련자에게 전파

참 고

- ☞ 예시 : ‘내부관리계획은 ○○회사 CEO의 승인을 거쳐 ○○회사 전 임직원에게 공표한다.’

- 개인정보 처리 방법 및 환경 등의 변화로 인하여 내부관리계획에 중요한 변경이 있을 때에는 변경 사항을 즉시 반영하고 내부관리계획을 승인
- 내부관리계획 수정·변경 시 내용 및 시행 시기 등 그 이력의 관리 등

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

- 정보통신서비스 제공자등은 이 기준에서 정하는 기술적·관리적 및 물리적 보호조치에 관한 사항은 모두 이행하여야 한다.

참 고

☞ 제3조(내부관리계획의 수립·시행)부터 제10조(개인정보 표시 제한 보호조치)까지

- 내부관리계획의 적정성과 실효성을 보장하기 위하여 내부관리계획에 따른 기술적·관리적 및 물리적 보호조치의 이행 여부의 점검·관리에 관한 사항을 포함하여야 한다.
 - “○○년 개인정보 보호조치 이행 점검 계획(안)” 등과 같은 형태로 수립할 수 있으며, 점검 대상, 점검 항목 및 방법 등을 포함하도록 한다.

이행 점검 (예시)

- ☞ 점검 대상 및 시기
- ☞ 점검 조직 및 인력
- ☞ 점검 항목 및 내용
- ☞ 점검 방법 및 절차
- ☞ 점검 결과 기록 및 보관
- ☞ 점검 결과 후속조치(개선, 보고) 등

- 이행 점검은 사내 독립성이 보장되는 부서(감사팀 등), 관련 부서(개인정보 보호팀) 또는 개인정보보호 전문업체 등에서 수행할 수도 있다.
- 이행 점검은 개인정보취급자가 적절하게 개인정보 보호조치를 이행하고 있는지 여부 등을 파악할 수 있도록 정기적으로(최소 연 1회 권고) 점검하도록 한다.
- 이행 점검 결과는 “○○년 개인정보 보호조치 이행 점검 결과” 등과 같은 형태로 작성할 수 있으며, 필요하면 사업주 또는 대표자에게 점검결과 및 개선조치를 보고할 수 있다.

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

- 정보통신서비스 제공자등은 수탁자가 개인정보의 안전성 확보를 위해 이 기준을 준수하도록 하는 등 수탁자를 관리·감독하여야 한다.

수탁자 관리 및 감독 (예시)

- ☞ 관리·감독 대상 및 시기
- ☞ 관리·감독 항목 및 내용
- ☞ 관리·감독 방법 및 절차
- ☞ 관리·감독 결과 기록 및 보관
- ☞ 관리·감독 결과 후속조치(개선, 보고) 등

참 고

- ☞ 사업자 선정부터 사업 종료 시까지 전 과정에 걸쳐 안전성 확보를 위한 보호조치 사항 포함
 - * 제안요청서, 계약서 등에 기술적·관리적 및 물리적 보호조치에 관한 사항을 명시하고, 이에 대한 이행여부를 분기별 또는 반기별로 주기적 관리·감독 및 확인

개인정보 보호법

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

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

개인정보 보호법 시행령

제28조(개인정보의 처리 업무 위탁 시 조치) ① 법 제26조 제1항 제3호에서 “대통령령으로 정한 사항”이란 다음 각 호의 사항을 말한다.

1. 위탁업무의 목적 및 범위
 2. 재위탁 제한에 관한 사항
 3. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
 4. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
- ⑥ 위탁자는 수탁자가 개인정보 처리 업무를 수행하는 경우에 법 또는 이 영에 따라 개인정보처리자가 준수하여야 할 사항과 법 제26조 제1항 각 호의 사항을 준수하는지를 같은 조 제4항에 따라 감독하여야 한다.

6. 개인정보의 분실·도난·유출·위조·변조·훼손 등이 발생한 경우의 대응 절차 및 방법에 관한 사항

- 개인정보가 분실·도난·유출·위조·변조 또는 훼손 등(이하 ‘유출’)이 발생한 때에는 신속한 대응 조치를 통해 개인정보의 추가 유출을 막고, 유출로 인한 이용자 피해를 최소화하기 위한 대응절차 및 그 방법에 관한 사항을 포함하여야 한다.
- 개인정보 유출 신속대응체계 구축 : 개인정보 유출 사실을 알게 된 때에는 개인정보 보호책임자는 즉시 사업주 또는 대표자에게 보고하고 개인정보보호·정보보호 부서를 중심으로 「개인정보 유출 신속대응팀」을 구성하여, 추가 유출 및 이용자 피해발생 방지를 위한 조치를 강구하여야 한다.
- 유출 원인 파악 및 추가 유출 방지 조치 : 개인정보 유출 원인을 파악한 후 추가 유출 방지를 위해 유출 원인별 보호조치를 실시하여야 한다.
- 개인정보 유출 신고 및 통지
(신고) 개인정보의 유출 사실을 알게 된 때에는 즉시(24시간 이내) 개인정보 유출 사실을 보호위원회 또는 한국인터넷진흥원에 신고하여야 한다.

참 고

- ☞ 개인정보 유출로 인한 피해를 막기 위해서는 해커 등 개인정보 유출자 검거를 위해 경찰청 사이버안전국에 범인 검거를 위한 수사를 요청하고 유출된 개인정보 회수를 위한 조치 실시
- ☞ 인터넷 상 침해사고가 발생하면 과학기술정보통신부 또는 한국인터넷진흥원에 신고하여 침해사고 원인분석 및 취약점 보완조치 등을 실시

(통지) 유출된 개인정보로 인하여 추가적인 피해가 발생하지 않도록 개인정보 유출 사실을 알게 된 후 즉시(24시간 이내) 해당 이용자에게 개인정보 유출 사실을 통지하여야 한다.

- 이용자 피해구제 및 재발방지 대책 마련 : 이용자 피해구제 방법을 안내하고 유사 사고의 재발방지를 위한 대책을 마련하여야 한다.

참 고

- ☞ 보호위원회·한국인터넷진흥원이 운영하는 개인정보보호 포털(<https://www.privacy.go.kr>)에서 제공하는 ‘정보통신서비스 제공자들을 위한 개인정보 유출 대응 매뉴얼’을 활용할 수 있다.

7. 그 밖에 개인정보보호를 위해 필요한 사항

- 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 안전성 확보를 위하여 필요한 개인정보 보호조치에 관한 사항을 추가적으로 포함하여야 한다.
- 정보통신서비스 제공자등은 사업규모, 서비스의 유형, 개인정보 보유 수, 처리하는 개인정보의 유형 및 중요도, 개인정보를 처리하는 방법 및 환경, 보안위험요인 등을 고려하도록 한다.

그 밖에 개인정보 보호조치 (예시)

- ☞ 개인정보보호 관리체계(PIMS) 등 개인정보보호 관련 인증 획득
 - ☞ 개인정보보호 컨설팅
 - ☞ 위험관리(자산식별, 위험평가, 대책마련, 사후관리)
 - ☞ 개인정보처리시스템 설계, 개발, 운영 보안
 - ☞ 보안장비 및 보안솔루션 도입 및 운영, 형상·운영 관리 및 기록
 - ☞ 개인정보보호 예산 및 인력의 적정수준 반영
 - ☞ 개인정보보호 관련 지침, 규정 등 수립 및 시행
 - ☞ 개인정보 파기 절차 수립 및 시행 등
-

② 정보통신서비스 제공자등은 다음 각 호의 사항을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수 등을 고려하여 필요한 교육을 정기적으로 실시하여야 한다.

1. 교육목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

- 정보통신서비스 제공자등은 개인정보의 안전한 처리를 위하여 개인정보 보호책임자 및 개인정보취급자에게 최소 연1회 이상 필요한 교육을 실시하여야 한다.
- 개인정보보호 교육의 구체적인 사항은 교육 목적 및 대상, 교육 내용(프로그램 등), 교육 일정 및 방법 등을 포함하도록 한다. 내부관리계획 등에 규정하거나 “○○년 개인정보보호 교육 계획(안)” 등과 같은 형태로 수립할 수 있다.
- 교육 내용은 개인정보 보호책임자 그리고 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, 내부관리계획 등 필히 알고 있어야 하는 사항을 포함하여 교육을 실시하도록 한다.

교육 내용 (예시)

- ☞ 개인정보 보호의 중요성
- ☞ 개인정보 내부관리계획 등 규정, 지침의 제·개정에 따른 사항
- ☞ 개인정보처리시스템의 안전한 운영·사용법(하드웨어, 소프트웨어 등)
- ☞ 개인정보의 기술적·관리적 보호조치 기준
- ☞ 개인정보 처리업무 위·수탁시 보호조치
- ☞ 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.

참 고

- ☞ 보호위원회·한국인터넷진흥원이 운영하는 개인정보보호 포털(<https://www.privacy.go.kr>)에서 제공하는 온라인 및 현장 교육 프로그램, 교육 자료 그리고 전문강사단 등을 활용할 수 있다.

- 교육 실시 결과는 “○○년 개인정보보호 교육 결과” 등과 같은 형태로 작성할 수 있으며, 교육 일시·내용·참석자 등을 확인할 수 있는 정보를 전자적으로 기록하거나 수기로 작성하여야 한다.

참 고

- ☞ 교육 결과의 세부 실적은 정보통신서비스 제공자등이 실시한 개인정보보호 관련 사내교육, 외부교육, 위탁교육 등에서 교육 과정별 수료증 등을 발급·보관함으로써 관리할 수 있다.
- ☞ 교육 참석자를 확인할 수 있는 정보로는 해당 교육 시간에 교육장소에 출입한 기록(태그 등), 교육 참석자 명단에 수기로 서명한 자료 등을 활용할 수 있다.

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

- 정보통신서비스 제공자등은 개인정보의 안전한 처리를 위하여 보호조치 이행을 위한 세부적인 추진방안을 포함하는 내부관리계획을 수립하여야 한다.
 - 제1항제4호(개인정보의 기술적·관리적 보호조치 이행 여부의 내부 점검에 관한 사항)에 따라 이 기준에서 정하는 기술적·관리적 및 물리적 보호조치에 관한 사항은 모두 포함되어야 한다.

참 고

- ☞ 제3조 : 개인정보 보호책임자의 지정 등 개인정보보호 조직의 구성·운영에 관한 사항, 개인정보 취급자 등 대상 정기적인 교육, 그 밖에 필요한 사항 등
- ☞ 제4조 : 접근권한 부여·변경·말소, 정보통신망을 통한 불법적인 접근 및 침해사고 방지 등
- ☞ 제5조 : 개인정보취급자가 개인정보처리시스템에 접속한 기록 보존·관리 및 확인·감독 등
- ☞ 제6조 : 비밀번호 등 암호화 저장, 개인정보 등 암호화 송·수신 등
- ☞ 제7조 : 악성 프로그램 등을 방지·치료할 수 있는 보안 프로그램 설치·운영 등
- ☞ 제8조 : 개인정보의 물리적 보관 장소에 출입통제 등
- ☞ 제9조 : 개인정보의 출력·복사물을 안전하게 관리하기 위한 보호조치 등
- ☞ 제10조 : 개인정보의 조회·출력시 마스킹을 통한 표시제한 등

- 이 기준 제1조제2항에 따라 정보통신서비스 제공자등이 스스로 정하는 ‘개인정보 보호조치 기준’에 관한 사항도 포함되어야 한다.

개인정보 내부관리계획 목차 (예시)

- ☞ 제1조 총칙
 - * 목적
 - * 용어정의
 - * 적용범위
- ☞ 제2조 내부관리계획의 수립 및 시행
 - * 내부관리계획의 수립 및 승인
 - * 내부관리계획의 공표
- ☞ 제3조 개인정보보호 조직 구성 및 운영
 - * 개인정보 보호책임자의 지정
 - * 개인정보 보호책임자의 역할 및 책임
 - * 개인정보취급자의 역할 및 책임
- ☞ 제4조 개인정보보호 교육
 - * 개인정보 보호책임자의 교육
 - * 개인정보취급자의 교육
- ☞ 제5조 기술적·관리적 및 물리적 보호조치
 - * 접근통제
 - * 접속기록의 위·변조방지
 - * 개인정보의 암호화
 - * 악성프로그램 방지
 - * 물리적 접근 방지
 - * 출력·복사시 보호조치
 - * 개인정보 표시 제한 보호조치

☞ 제6조 관리 및 감독

- * 기술적·관리적 및 물리적 보호조치 이행 점검
- * 수탁자 관리 및 감독

☞ 제7조 개인정보 침해사고 대응절차 및 방법

☞ 제8조 그 밖에 개인정보보호를 위해 필요한 사항

- 내부관리계획은 전사적인 계획 내에서 개인정보가 관리될 수 있도록 사업주 또는 대표자에게 내부결재 등의 승인을 받아 모든 임직원 및 관련자에게 알리고 이를 준수할 수 있도록 하여야 한다.

참 고

☞ 개인정보 처리방침을 내부관리계획으로 사용할 수 없다.

- * 개인정보 처리방침: 개인정보 처리에 관한 사항을 이용자에게 홈페이지 등으로 공개(근거: 법 제30조(개인정보 처리방침의 수립 및 공개))
 - * 개인정보 내부관리계획: 개인정보를 안전하게 처리하기 위한 조직(회사) 전체 대상(근거: 법 제29조(안전조치의무))
-

- 정보통신서비스 제공자등은 제3항에 따라(이 기준 제1조제2항에 따른 ‘개인정보 보호조치 기준’을 포함한다.) 수립한 내부관리계획을 시행하여야 한다.

참 고

☞ 내부관리계획이 적절하게 시행되기 위해서는 개인정보 보호책임자가 정기적으로 내부관리계획의 이행 실태를 점검·관리하고, 그 결과에 따라 적절한 조치를 취하여야 한다.

- * 중대한 영향을 초래하거나 해를 끼칠 수 있는 사안 등에 대해서는 사업주 또는 대표자에게 보고 후, 의사결정 절차를 통하여 적절한 대책을 마련하여야 한다.
-

제4조(접근통제) ① 정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근 권한을 서비스 제공을 위하여 필요한 개인정보 보호책임자 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 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 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 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. 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성
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 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유 설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.

⑩ 정보통신서비스 제공자등은 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하여야 한다.

해설

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

- 정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위해 필요한 최소한의 인원에게 부여하여야 한다.
 - 특히, 개인정보처리시스템의 데이터베이스(DB)에 직접 접속은 데이터베이스 운영·관리자에 한정하는 등의 보호조치를 적용할 필요성이 있다.
- 정보통신서비스 제공자등은 개인정보처리시스템에 열람, 수정, 다운로드 등 접근권한을 부여할 때에는 서비스 제공을 위해 필요한 범위에서 구체적으로 차등화 하여 부여하여야 한다.

- 정보통신서비스 제공자등이 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), 가명정보로부터 특정 개인을 알아보지 못하도록 가명정보 및 추가 정보에 접근할 수 있는 권한을 엄격하게 관리 및 통제하여야 한다.
- 여기서 말하는 접근권한은 본인 이외의 개인정보에 대한 접근권한을 의미하며, 이용자가 자신의 개인정보를 조회·수정 하는 등의 접근권한은 포함하지 않는다.

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

- 정보통신서비스 제공자등은 개인정보취급자가 전보 또는 퇴직, 휴직 등 인사이동이 발생하여 개인정보처리시스템에 사용자계정 등 접근권한의 변경·말소 등이 필요할 때에는 정당한 사유가 없는 한 즉시 조치하여야 한다.
- 정보통신서비스 제공자등은 불완전한 접근권한의 변경 또는 말소 조치로 인하여 정당한 권한이 없는 자가 개인정보처리시스템에 접근될 수 없도록 하여야 한다.

접근권한 변경·말소 미조치 사례 (예시)

- ☞ 다수 시스템의 접근권한 변경·말소가 필요함에도 일부 시스템의 접근권한만 변경·말소할 때
- ☞ 접근권한의 전부를 변경·말소하여야 함에도 일부만 변경·말소할 때
- ☞ 접근권한 말소가 필요한 계정을 삭제 또는 접속차단조치를 하였으나, 해당 계정의 인증값 등을 이용하여 우회 접근이 가능할 때 등

참 고

- ☞ 내부관리계획 등에 ‘개인정보취급자가 퇴직할 때에는 개인정보처리시스템에 사용자계정 등 접근권한을 지체 없이 말소한다.’ 등을 반영하여 이행할 수 있다.
- ☞ 개인정보취급자가 퇴직할 때에는 사용자계정 말소를 효과적으로 이행하기 위해서는 퇴직 점검표에 사용자계정 말소 등의 내용을 반영하여 이행 여부에 대해 확인을 받을 수도 있다.

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

■ 정보통신서비스 제공자등은 개인정보처리시스템에 접근권한 부여, 변경, 말소 내역을 전자적으로 기록하거나 수기로 작성한 관리대장 등에 기록하고 해당 기록을 최소 5년간 보관하여야 한다.

– 관리대장 등에는 신청자 정보, 신청 및 적용 일시, 승인자 및 발급자 정보, 신청 및 발급 사유 등의 내용이 포함되어야 하며 공식적인 절차를 통하여 관리하도록 한다.

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

■ 인터넷 구간 등 외부로부터 개인정보처리시스템에 접속은 원칙적으로 차단하여야 하나, 정보통신서비스 제공자등의 업무 특성 또는 필요에 의해 개인정보취급자가 노트북, 업무용 컴퓨터, 모바일 기기 등으로 외부에서 정보통신망을 통해 개인정보처리시스템에 접속이 필요할 때에는 안전한 인증수단을 적용하여야 한다.

– 안전한 인증 수단의 적용 : 개인정보처리시스템에 사용자계정과 비밀번호를 입력하여 정당한 개인정보취급자 여부를 식별·인증하는 절차 이외에 추가적인 인증 수단의 적용을 말한다.

인증 수단 (예시)

- ☞ 인증서(PKI, Public Key Infrastructure) : 전자상거래 등에서 상대방과의 신원확인, 거래사실 증명, 문서의 위변조 여부 검증 등을 위해 사용하는 전자서명으로서 해당 전자서명을 생성한 자의 신원을 확인하는 수단
- ☞ 보안토큰 : 암호 연산장치 등으로 내부에 저장된 정보가 외부로 복사, 재생성 되지 않도록 공인인증서 등을 안전하게 보호할 수 있는 수단으로 스마트카드, USB 토큰 등이 해당
- ☞ 일회용 비밀번호(OTP, One Time Password) : 무작위로 생성되는 난수를 일회용 비밀번호로 한번 생성하고, 그 값을 한 번만 사용할 수 있도록 하는 방식

- 안전한 인증 수단을 적용할 때에도 보안성 강화를 위하여 VPN, 전용선 등 안전한 접속수단의 적용을 권고한다.

참 고

- ☞ 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 말한다.
- * 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.
- ☞ 전용선 : 두 지점간에 독점적으로 사용하는 회선으로 본점과 지점간 직통으로 연결하는 회선 등을 말한다.

- 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 허가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

- 정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음과 같은 시스템 등을 스스로의 환경을 고려하여 접근 제한 기능 및 유출 탐지 기능이 적합하게 수행되도록 설치·운영하여야 한다. 다만, 어느 경우라도 접근 제한 기능 및 유출 탐지 기능이 모두 충족되어야 한다.

참 고

- ☞ 불법적인 접근 : 인가되지 않은 자(내·외부자 모두 포함)가 사용자계정 탈취, 자료유출 등의 목적으로 개인정보처리시스템, 개인정보취급자의 컴퓨터 등에 접근하는 것을 말한다.
- ☞ 침해사고 : 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다.(「정보통신망법」 제2조제1항제7호)

- 해당 시스템으로는 침입차단시스템, 침입탐지시스템, 침입방지시스템, 보안 운영체제(Secure OS), 웹방화벽, 로그분석시스템, ACL(Access Control List)을 적용한 네트워크 장비, 통합보안관제시스템 등을 활용할 수 있다.
- 인터넷데이터센터(IDC), 클라우드 서비스, 보안업체 등에서 제공하는 보안서비스 등도 활용할 수 있다.
- 공개용(무료) S/W를 사용하거나, 운영체제(OS)에서 제공하는 기능을 활용하여 해당 기능을 포함한 시스템을 설치·운영할 수 있다. 다만, 공개용(무료) S/W를 사용하는 경우에는 접근 제한 기능 및 유출 탐지 기능이 모두 충족되는지, 해당 S/W가 정기적으로 업데이트되는지 등을 사전에 점검하고 설치·운영하여야 한다.

참 고

- ☞ 보안제품 등을 도입할 때에는 IT보안인증사무국(<https://www.itscc.kr>)에서 제공하는 인증제품 목록(제품유형 : 개인정보보호, DB접근통제, 통합로그관리 등) 등을 활용할 수도 있다.

- 접근 제한 기능 및 유출 탐지 기능의 충족을 위해서는 단순히 시스템을 설치하는 것만으로는 부족하며, 신규 위협 대응 및 정책의 관리를 위하여 다음과 같은 방법 등을 활용하여 체계적으로 운영·관리하여야 한다.
- 정책 설정 운영 : 신규 위협 대응 등을 위하여 접근 제한 정책 및 유출 탐지 정책을 설정하고 지속적인 업데이트 적용 및 운영·관리

정책 설정 운영 (예시)

- ☞ 신규 취약점 또는 침해사고 발생 시 보안 업데이트 적용
- ☞ 과도하게 허용되거나 사용되지 않는 정책 등에 대하여 주기적 검토 및 조치 등

- 이상 행위 대응 : 모니터링 등을 통해 인가받지 않은 접근을 제한하거나 인가자의 비정상적인 행동에 대응

이상 행위 대응 (예시)

- ☞ 동일 IP, 해외 IP 주소에서의 과도한 또는 비정상적인 접속시도 탐지 및 차단 조치
- ☞ 개인정보처리시스템에서 과도한 또는 비정상적인 트래픽 발생 시 탐지 및 차단 조치 등

- 로그 분석 : 로그 등의 대조 또는 분석을 통하여 이상 행위를 탐지 또는 차단

참 고

- ☞ '로그'는 침입차단시스템 또는 침입탐지시스템의 로그기록에 한정하지 않고 개인정보처리시스템의 접속기록, 네트워크 장비의 로그기록, 보안장비소프트웨어의 기록 등을 포함

- IP주소 등에는 IP주소, 포트 그 자체뿐만 아니라, 해당 IP주소의 행위(과도한 접속성공 및 실패, 부적절한 명령어 등 이상 행위 관련 패킷)를 포함한다.

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

- 망분리를 하여야 하는 정보통신서비스 제공자등은 다음과 같다.

- 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상(제공하는 정보통신서비스가 다수일 때에는 전체를 합산하여 적용)
- 정보통신서비스 부문 전년도(법인일 때에는 전 사업연도를 말한다) 매출액이 100억원 이상(정보통신서비스와 그 외 서비스를 함께 제공할 때에는 정보통신서비스 부문을 합산한 매출액만 적용)

참 고

- ☞ 위에 해당하지 아니하는 정보통신서비스 제공자등은 망분리를 적용하지 아니할 수 있으나, 보안성 강화 등을 위해서 적용을 권고한다.

- 망분리는 다음과 같은 방법 등을 활용할 수 있으며, 세부내용은 “[부록] 정보통신서비스 제공자등을 위한 망분리 해설”을 참고하도록 한다.

- 물리적 망분리 : 통신망, 장비 등을 물리적으로 이원화하여 인터넷 접속이 불가능한 컴퓨터와 인터넷 접속만 가능한 컴퓨터로 분리하는 방식이다.
- 논리적 망분리 : 물리적으로 하나의 통신망, 장비 등을 사용하지만 가상화 등의 방법으로 인터넷 접속이 불가능한 내부 업무영역과 인터넷 접속영역을 분리하는 방식이다.

참 고

- ☞ 정보통신서비스 제공자등은 스스로의 환경에 맞는 망분리를 적용하여 개인정보를 처리하는 과정에서의 외부와의 접점을 최소화함으로써 외부로부터 들어오는 공격이나 내부에서 외부로의 개인정보 유출 등을 차단하여야 한다.

- 정보통신서비스 제공자등이 망분리를 할 때 인터넷망으로부터 분리되어야 하는 대상은 다음과 같다.

- 개인정보처리시스템에서 개인정보를 다운로드 할 수 있는 개인정보취급자의 컴퓨터 등

참 고

- ☞ 다운로드 : 개인정보처리시스템에 직접 접속하여 개인정보취급자의 컴퓨터 등에 개인정보를 엑셀, 워드, 텍스트, 이미지 등의 파일형태로 저장하는 것을 말한다.

- 개인정보처리시스템에서 개인정보를 파기할 수 있는 개인정보취급자의 컴퓨터 등

참 고

- ☞ 파기 : 개인정보처리시스템에 저장된 개인정보 파일, 레코드, 테이블 또는 데이터베이스(DB)를 삭제하는 것을 말한다.

- 개인정보처리시스템에 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등

참 고

- ☞ 접근권한 설정 : 개인정보처리시스템에 접근하는 개인정보취급자에게 다운로드, 파기 등의 접근권한을 설정하는 것을 말한다.

- 개인정보처리시스템에서 단순히 개인정보를 열람, 조회 등만을 할 때에는 망분리를 적용하지 아니할 수 있다.

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

- 정보통신서비스 제공자등은 이용자가 안전한 비밀번호를 설정하여 이용할 수 있도록 비밀번호 작성규칙을 수립하고, 이를 인터넷 홈페이지 등에 적용하여야 한다.

안전한 비밀번호 이용 방안 (예시)

- ☞ (생성) 비밀번호 길이와 복잡도 설정, 계정(ID)과 비밀번호를 동일하게 생성 금지, 비밀번호 재발급 시 랜덤하게 임시 비밀번호를 발급하여 최초 로그인시 새로운 비밀번호로 변경하도록 적용 등
- ☞ (암호화) 비밀번호는 전송 시 암호화 적용, 저장 시 일방향(해쉬) 암호화 적용 등
- ☞ (변경) 비밀번호 사용 만료일 이전에 이용자에게 알려주어 변경 유도, 비밀번호 유효기간을 설정하여 강제 변경 등
- ☞ (공격 대응) 5회 이상 로그인 시도 실패 시 계정 잠금, 로그인 실패 횟수에 따라 로그인 지연시간 설정, 사전에 있는 단어 사용 금지, 비밀번호에 난수 추가(Salting) 등
- ☞ (운영 관리) 일정시간 작업이 없는 로그온 세션 종료, 장기 휴면계정 계정 삭제, 비밀번호 공유 금지, 초기값(Default) 비밀번호 변경 후 사용, 로그인 시도 및 로그인 기록 유지, 비밀번호 재사용 금지 등

이용자 비밀번호 작성규칙 (예시)

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

참 고

- ☞ 비밀번호 이외의 추가적인 인증에 사용되는 SMS 인증, 일회용 비밀번호(OTP) 등은 비밀번호 작성규칙을 적용하지 아니할 수 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.

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

1. 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성
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 개인정보취급자가 안전한 비밀번호를 설정하여 이행할 수 있도록 다음의 사항을 포함하는 비밀번호 작성규칙을 수립하고 이를 개인정보처리 시스템 등에 적용하여야 한다.

- 영대문자, 영소문자, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성하여야 한다.
- 연속적인 문자열이나 숫자, 생년월일, 전화번호 등 추측하기 쉬운 정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고한다.
- 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경하여야 한다.

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

개인정보취급자 비밀번호 작성규칙 (예시)

- ☞ 비밀번호는 문자, 숫자의 조합·구성에 따라 최소 10자리 또는 8자리 이상의 길이로 설정
(기술 발달에 따라 비밀번호의 최소 길이는 늘어날 수 있다.)
 - ★ 최소 10자리 이상: 두 종류 이상의 문자로 구성한 경우
 - ※ 문자 종류 : 알파벳 대문자와 소문자, 특수문자, 숫자
 - ★ 최소 8자 이상: 세 종류 이상의 문자를 이용하여 구성한 경우
 - ☞ 비밀번호는 추측하거나 유추하기 어렵도록 설정
 - ★ 일련번호(12345678 등), 전화번호, 잘 알려진 단어(love, happy 등), 키보드 상에서 나란히 있는 문자열(qwer 등) 등을 사용하지 않도록 한다.
 - ☞ 비밀번호를 최소 6개월마다 변경하도록 변경기간을 적용하는 등 장기간 사용하지 않는다.
 - ★ 변경시 동일한(예시: Mrp15@*1aT와 Mrp15@*1at) 비밀번호를 교대로 사용하지 않도록 한다.
-

- 개인정보처리시스템에 권한 없는 자의 접근을 방지하기 위하여 비밀번호 등을 일정 횟수 이상 잘못 입력할 때에는 개인정보처리시스템에 접근을 제한하는 등의 보호조치를 추가적으로 적용할 수 있다.

⑨ 정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보 처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.

■ 인터넷 홈페이지를 통한 개인정보 유·노출 방지 조치

- 정보통신서비스 제공자등은 규모, 여건 등을 고려하여 스스로의 환경에 맞는 보호조치를 하되, 보안대책 마련, 보안 기술 마련, 운영 및 관리 측면에서의 개인정보 유·노출 방지 조치를 하여야 한다.

참 고

- ☞ 인터넷 홈페이지를 통한 개인정보 유·노출 유형
 - * 검색엔진(구글링 등) 등을 통한 개인정보 유·노출
 - * 웹 취약점을 통한 개인정보 유·노출
 - * 인터넷 게시판을 통한 개인정보 유·노출
 - * 홈페이지 설계·구현 오류로 인한 개인정보 유·노출
 - * 기타 방법을 통한 개인정보 유·노출

- (보안대책 마련) 인터넷 홈페이지 설계 시 개인정보 유·노출에 영향을 미칠 수 있는 위험요소를 분석하여 필요한 보안대책을 마련하여야 한다.

보안대책 (예시)

- ☞ 입력 데이터의 유효성을 검증
- ☞ 인증, 접근통제 등의 보호조치 적용
- ☞ 에러, 오류 상황이 처리되지 않거나 불충분하게 처리되지 않도록 구성
- ☞ 세션을 안전하게 관리하도록 구성 등

- (보안 기술 적용) 인터넷 홈페이지 개발 시 개인정보 유·노출 방지를 위한 보안 기술을 적용하여야 한다.

보안 기술 적용 (예시)

- ☞ 홈페이지 주소(URL), 소스코드, 임시 저장 페이지 등에 개인정보 사용 금지
- ☞ 홈페이지에 관리자 페이지의 주소 링크 생성 금지, 관리자 페이지 주소는 쉽게 추측하기 어렵도록 생성, 관리자 페이지 노출 금지
- ☞ 엑셀 파일 등 숨기기 기능에 의한 개인정보 유·노출 금지
- ☞ 시큐어 코딩(Secure coding) 도입
- ☞ 취약점을 점검하고 그 결과에 따른 적절한 개선 조치
- ☞ 인증 우회(Authentication bypass)에 대비하는 조치 등

참 고

- ☞ 시큐어 코딩 항목: 입력데이터 검증 및 표현(SQL 삽입 등), 보안기능(부적절한 인가 등), 시간 및 상태(종료되지 않는 반복문 등), 에러처리(오류 상황 대응 부재 등), 코드오류(해제된 자원 사용), 캡슐화(잘못된 세션에 의한 정보 노출), API 오용(취약한 API 사용 등) 등
- * 시큐어 코딩에 관한 세부 내용은 소프트웨어 개발보안 가이드(행정안전부·한국인터넷진흥원, 2019.11월) 등을 참고하도록 한다.

- (운영 및 관리) 인터넷 홈페이지 운영·관리 시 개인정보 유·노출 방지를 위한 보안대책 및 기술 적용에 따른 적정성을 검증하고 개선 조치를 하여야 한다.

운영 및 관리 (예시)

- ☞ 인터넷 홈페이지 등에 보안대책을 정기적으로 검토
- ☞ 홈페이지 게시물, 첨부파일 등에 개인정보 포함 금지, 정기적 점검 및 삭제 등의 조치
- ☞ 서비스 중단 또는 관리되지 않는 홈페이지는 전체 삭제 또는 차단 조치
- ☞ 공격패턴, 위험분석, 침투 테스트 등을 수행하고 발견되는 결함에 따른 개선 조치
- ☞ 취약점을 점검하고 그 결과에 따른 적절한 개선 조치 등

참 고

- ☞ 취약점 점검 항목: SQL Injection 취약점, CrossSiteScript 취약점, File Upload 및 Download 취약점, ZeroBoard 취약점, Directory Listing 취약점, URL 및 Parameter 변조 등
- * 취약점 점검 항목은 행정안전부, 국가사이버안전센터(NCSC), 한국인터넷진흥원(KrCERT), OWASP(오픈소스웹보안프로젝트) 등에서 발표하는 항목을 참조하도록 한다.

- ☞ 인터넷 홈페이지의 취약점 점검 시에는 기록을 남겨 책임추적성 확보 및 앞으로 개선조치 등에 활용할 수 있도록 할 필요가 있다.
- ☞ 인터넷 홈페이지의 취약점 점검은 정보통신서비스 제공자등의 자체인력, 보안업체 등을 활용할 수 있으며, 취약점 점검은 상용 도구, 공개용 도구, 자체 제작 도구 등을 사용할 수 있다.
- ☞ 취약점 점검과 함께 정기적으로 웹 쉘 등을 점검하고 조치한다면 처리중인 개인정보가 인터넷 홈페이지를 통해 열람권한이 없는 자에게 공개되거나 유출되는 위험성을 더욱 줄일 수 있다.
- ☞ 기술과 서비스 발전에 따라 시스템 등에 신규 취약점은 계속적으로 발생하고 있으며, 정기적인 취약점 점검 및 개선조치 등 개인정보 유출을 예방하기 위한 보호조치가 필요하다.

■ P2P 및 공유설정을 통한 개인정보 유·노출 방지 조치

- 개인정보처리시스템, 컴퓨터, 모바일 기기 등에서 P2P, 공유설정은 기본적으로 사용하지 않는 것이 원칙이나, 업무상 반드시 필요할 때에는 권한 설정 등의 조치를 통해 권한이 있는 자만 접근할 수 있도록 설정하여 개인정보가 열람권한이 없는 자에게 공개되거나 유출되지 않도록 접근 통제 등에 관한 보호조치를 하여야 한다.

P2P 및 공유설정을 통한 개인정보 유·노출 방지 조치 (예시)

- ☞ 불가피하게 공유설정 등을 할 때에는 업무용 컴퓨터에 접근 권한 비밀번호를 설정하고, 사용이 완료된 후에는 공유설정을 제거
 - ☞ 파일 전송이 주된 목적일 때에는 읽기 권한만을 주고 상대방이 쓰기를 할 때만 개별적으로 쓰기 권한을 설정
 - ☞ P2P 프로그램, 상용 웹메일, 웹하드, 메신저, SNS 서비스 등을 통하여 고의·부주의로 인한 개인정보 유·노출 방지
 - ☞ WPA2(Wi-Fi Protected Access 2) 등 보안 프로토콜이 적용된 무선망 이용 등
-

참 고

- ☞ P2P, 웹하드 등의 사용을 제한할 때에는 단순히 사용금지 조치를 취하는 것이 아니라 시스템 상에서 해당 포트를 차단하는 등 근본적인 보호조치를 취하는 것이 필요하다.
-

⑩ 정보통신서비스 제공자등은 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하여야 한다.

- 정보통신서비스 제공자등은 개인정보처리시스템에 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않을 때에는 자동으로 시스템 접속이 차단되도록 최대 접속시간 제한 등의 조치를 취하여야 한다.
- 최대 접속시간 제한 조치는 개인정보처리시스템에 접속하는 업무용 컴퓨터 등에서 해당 개인정보처리시스템에 대한 접속을 차단하는 것을 의미하며, 최대 접속시간이 경과하면 개인정보처리시스템과 연결이 완전히 차단되어 정보의 송·수신이 불가능한 상태가 되어야 한다.
- 개인정보취급자가 최대 접속시간 제한 등의 조치로 인하여 개인정보처리시스템에 대한 접속이 차단된 이후 다시 접속하고자 할 때에는 그 방법·절차 등이 최초의 접속 방법·절차 등과 동일한 수준 이상이 되어야 한다.

접속 차단 미조치 사례 (예시)

- ☞ 개인정보처리시스템에 접속 차단 등의 조치 없이 업무용 컴퓨터에 화면보호기만을 설정한 때
 - ☞ 개인정보처리시스템 등에 다시 접속 시 자동 로그인 기능을 사용한 때
 - ☞ 서버접근제어 프로그램 등을 이용하여 별도의 로그인 절차 없이 개인정보처리시스템에 접속이 가능하도록 구성하면서 해당 프로그램에 접속 차단 조치를 하지 않은 때
-

참 고

- ☞ 정보통신서비스 제공자등은 개인정보를 처리하는 방법 및 환경, 보안위험요인, 업무특성(DB 운영·관리, 시스템 모니터링 및 유지보수 등) 등을 고려하여 스스로의 환경에 맞는 최대 접속시간을 각각 정하여 시행할 수 있다.
 - ☞ 최대 접속시간은 최소한(통상 10~30분 이내)으로 정하여야 한다. 다만, 장시간 접속이 필요할 때에는 접속시간 등 그 기록을 보관·관리하여야 한다.
-

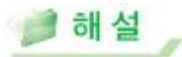
제 5 조

접속기록의 위·변조방지

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 1년 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.



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

- 정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여 개인정보 처리를 위한 업무수행과 관련이 없거나 과도한 개인정보의 조회, 정정, 다운로드, 삭제 등 비정상적인 행위를 탐지하고 적절한 대응조치를 하여야 한다.
- 정보통신서비스 제공자등은 개인정보처리시스템에 불법적인 접속 및 운영, 비정상적인 행위 등 이상 유무의 확인 등을 위해 다음의 사항 등을 포함하는 접속기록을 최소 1년 이상 보존·관리하여야 한다.
 - 식별자 : 개인정보처리시스템에서 개인정보취급자를 식별할 수 있도록 부여된 ID 등
 - 접속일시 : 개인정보처리시스템에 접속한 시점 또는 업무를 수행한 시점(년-월-일, 시:분:초)
 - 접속지 : 개인정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소 등

- 수행업무 : 개인정보처리시스템에서 개인정보취급자가 처리(개인정보를 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 행위)한 내용을 알 수 있는 정보를 말한다.

접속기록 항목 (예시)

- ☞ 식별자 : A0001(개인정보취급자 식별정보)
- ☞ 접속일시 : 2020-06-03, 15:00:00
- ☞ 접속지 : 172.168.168.11
- ☞ 수행업무 : 홍길동(이용자 식별정보) 연락처 조회 등

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

- 기간통신사업자일 때에는 대규모의 이용자 개인정보를 처리하고 개인정보의 유출 등으로 인한 피해 가능성이 매우 높은 특수성 등으로 인하여 기간통신사업자일 때에는 최소 2년 이상 접속기록을 보존·관리하여야 한다.

전기통신사업법

제5조(전기통신사업의 구분 등) ① 전기통신사업은 기간통신사업 및 부가통신사업으로 구분한다.

- ② 기간통신사업은 전기통신회선설비를 설치하거나 이용하여 기간통신역무를 제공하는 사업으로 한다.
- ③ 부가통신사업은 부가통신역무를 제공하는 사업으로 한다.

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

- 정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록이 위·변조되지 않도록 다음과 같은 보호조치 등을 취하여야 한다.
 - 정기적으로 접속기록 백업을 수행하여 개인정보처리시스템 이외의 별도의 물리적인 저장장치에 보관
 - 접속기록을 수정 가능한 매체(하드디스크, 자기 테이프 등)에 백업할 때에는 위·변조 여부를 확인할 수 있는 정보를 별도의 장비에 보관·관리
 - 다양한 접속기록 위·변조 방지 기술의 적용 등

제6조(개인정보의 암호화) ① 정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화하여 저장한다.

② 정보통신서비스 제공자등은 다음 각 호의 정보에 대해서는 안전한 암호알고리즘으로 암호화하여 저장한다.

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

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 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화해야 한다.

① 정보통신서비스 제공자등은 비밀번호는 복호화 되지 아니하도록 일방향 암호화 하여 저장한다.

■ 정보통신서비스 제공자등은 이용자 및 개인정보취급자 등의 비밀번호가 노출 또는 위·변조되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 보조저장매체 등에 일방향 암호화(해쉬함수 적용)하여 저장하여야 한다.

– 일방향 암호화는 개인정보취급자 및 이용자 등이 입력한 비밀번호를 평문 형태가 아닌 해쉬함수를 통해 얻은 결과 값으로 시스템에 저장하는 것을 말한다. 입력한 비밀번호와 시스템에 저장된 비밀번호를 비교하여 인증된 사용자임을 확인한다.

참 고

☞ 정보통신서비스 제공자등은 이용자가 비밀번호의 분실 등을 이유로 재발급을 원할 때에는 정당한 이용자 여부를 확인 가능한 수단(SMS, 이메일 등)을 활용하여 임시 비밀번호를 부여하고 이용자가 확인 후 사이트에 접속하여 비밀번호를 변경하여 사용하도록 한다.

– 비밀번호를 암호화 할 때에는 국내·외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호 알고리즘으로 암호화하여 저장하도록 한다.

사용 권고하는 일방향 암호 알고리즘 (예시)

| 미국(NIST) | 일본(CRYPTREC) | 유럽(ECRYPT) | 국내 |
|---------------------|-----------------|----------------------------------|---------------------|
| 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)
※ MD5, SHA-1 등 보안강도가 낮은 것으로 판명된 암호 알고리즘을 사용하여서는 안된다.

☞ 처리속도 등 기술발전에 따라 사용 권고 암호 알고리즘은 달라질 수 있으므로, 암호화 적용 시 국내·외 암호 관련 연구기관에서 제시하는 최신 정보 확인 필요

☞ 국내·외 암호 연구 관련 기관은 한국인터넷진흥원(KISA)의 암호이용활성화 홈페이지 (<https://seed.kisa.or.kr>)의 “암호 표준화 및 유관기관”에서도 확인 가능

■ 무작위 대입공격(Brute Force), 레인보우 테이블 공격 등을 이용한 비밀번호 복호화에 대응하기 위하여 난수 추가(Salting) 등의 조치를 하여야 한다.

② 정보통신서비스 제공자등은 다음 각 호의 정보에 대해서는 안전한 암호알고리즘으로 암호화하여 저장한다.

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

■ 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 생체인식정보는 국내 및 미국, 일본, 유럽 등의 국외 암호 연구 관련 기관에서 사용 권고하는 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

- 주민등록번호는 다음에 해당할 때를 제외하고는 수집·이용할 수 없다.

참 고

제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회 규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우

③ 개인정보처리자는 제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.

사용 권고하는 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) | RSAES-OAEP | RSAES-OAEP | RSAES |
| (키 길이 2048bits 이상) | | | | |

- ☞ 국내외 암호 연구 관련 기관에서 대표적으로 다루어지는 권고 암호 알고리즘만 표시('18.12월 기준)
- ☞ 처리속도 등 기술발전에 따라 사용 권고 암호 알고리즘은 달라질 수 있으므로, 암호화 적용 시 국내·외 암호 관련 연구기관에서 제시하는 최신 정보 확인 필요
- ☞ 국내외 암호 연구 관련 기관은 한국인터넷진흥원(KISA)의 암호이용활성화 홈페이지 (<https://seed.kisa.or.kr>)의 “암호 표준화 및 유관기관”에서도 확인 가능

- 암호화에 사용되는 암호 키는 암호화된 데이터를 복호화 할 수 있는 중요한 정보이므로 암호 키의 안전한 관리 절차 수립·시행을 권고한다.

참 고

- ☞ 암호이용활성화(<https://seed.kisa.or.kr>)에서 제공하는 “암호 키 관리 안내서” 등을 참고할 수 있다.

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 이용자의 성명, 연락처 등의 개인정보와 인증정보를 정보통신망을 통해 인터넷 구간으로 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 암호화하여야 한다.
- SSL 인증서를 이용한 보안서버는 별도의 보안 프로그램 설치 없이, 웹서버에 설치된 SSL 인증서를 통해 개인정보를 암호화 전송하는 방식이다.

참 고

- ☞ SSL(Secure Socket Layer)은 웹 브라우저와 웹 서버간에 데이터를 안전하게 주고받기 위해 암호화 기술이 적용된 보안 프로토콜이다.
- ☞ 보안서버 구축 시, 잘 알려진 취약점(예시: Open SSL의 HeartBleed 취약점 등)을 조치하여 운영할 필요가 있다.

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

④ 정보통신서비스 제공자등은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화해야 한다.

- 정보통신서비스 제공자등은 이용자의 개인정보를 업무용 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 다음과 같은 방법 등을 활용하여 암호화하여야 한다.

참 고

- ☞ 개인정보란 살아있는 개인에 관한 정보로 다음에 해당하는 정보를 말한다.
 - 가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
 - 나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.
 - 다. 가명정보 : ‘가’ 또는 ‘나’에 해당하는 정보를 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보

- 안전한 암호화 알고리즘이 탑재된 암호화 소프트웨어 등을 활용
- 개인정보의 저장형태가 오피스 파일 형태일 때에는 해당 프로그램에서 제공하는 암호 설정 기능을 활용

참 고

- ☞ 한컴 오피스: 파일 >> 다른 이름으로 저장하기 >> 문서 암호 설정에서 암호 설정 가능
- ☞ MS 오피스: 파일 >> 다른 이름으로 저장하기 >> 도구 >> 일반옵션에서 암호 설정 가능
- ☞ 어도비 아크로벳: 고급 >> 보안 >> 암호로 암호화 또는 인증서로 암호화

- MS Windows 등 운영체제에서 제공하는 암호화 기능을 활용

참 고

- ☞ MS Windows 폴더(파일) 암호화: 암호화 폴더(파일) 선택하고 마우스 오른쪽 버튼 클릭 >> 속성 >> 일반 >> 고급에서 암호 설정 가능
- ☞ 보다 자세한 오피스, 운영체제에서의 암호기능 이용 방법은 한국인터넷진흥원(KISA)의 암호 이용활성화 홈페이지(<https://seed.kisa.or.kr>)에서 제공하는 “상용 소프트웨어에서의 암호기능 이용 안내서” 등을 활용할 수 있다.

- 모바일 기기에 저장할 때에는 디바이스 암호화 기능을 활용

참 고

- ☞ 모바일 기기 분실·도난 등으로 개인정보가 유출되지 않도록 모바일 기기 제조사 및 이동통신사가 제공하는 기능을 이용한 원격 잠금, 원격 데이터 삭제 등
- ☞ MDM(Mobile Device Management) 등 모바일 단말 관리 프로그램을 설치하여 원격 잠금, 원격 데이터 삭제, 접속 통제 등을 추가적으로 할 수 있다.

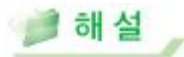
- 보조저장매체에 저장할 때에는 이용자의 개인정보를 암호화 한 후 저장하거나 암호화 기능을 제공하는 보안 USB 등을 활용 등
- 개인정보처리시스템으로부터 개인정보 파일을 내려 받는 경우 암호 설정이 된 상태로 내려 받는 기능을 활용
- 파일 암호화에 사용되는 비밀번호는 본 해설서에서 안내하는 제4조 제8항의 ‘비밀번호 작성규칙’을 적용하고, 암호 알고리즘은 보안강도 128비트 이상을 사용하는 것이 바람직하다.

제 7 조

악성프로그램 방지

제7조(악성프로그램 방지) 정보통신서비스 제공자등은 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

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



정보통신서비스 제공자등은 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

- 정보통신서비스 제공자등은 개인정보처리시스템, 컴퓨터 등에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치하여야 한다.
- 보안 프로그램은 그 목적과 기능에 따라 다양한 종류의 제품이 있으므로, 정보통신서비스 제공자등은 스스로의 환경에 맞는 보안 프로그램을 설치하도록 한다.

참 고

- ☞ 불법 또는 인가되지 않은 보안 프로그램 사용 시, 악성 프로그램 침투 경로로 이용되거나 보안 취약점 제거를 위한 업데이트 지원을 받지 못하여 개인정보 유출 사고 발생 가능성이 있으므로 정품 S/W만을 사용하도록 한다.

- 정보통신서비스 제공자등은 설치한 보안 프로그램을 적절하게 운영하여야 한다.
 - 보안 프로그램 설치 후, 최신 상태의 보안 업데이트 적용
 - 보안 프로그램의 정책·환경 설정 등을 통해 사내의 보안정책을 적용
 - 보안 프로그램을 통해 발견되는 악성 프로그램 등 확산 방지 조치(삭제·치료, 물리적 차단·분리 등)

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

- 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 프로그램 등이 유포됨에 따라 보안 프로그램을 최신의 업데이트 상태로 적용하여 유지해야 한다.

참 고

☞ 특히 대규모의 개인정보를 처리하거나 주민등록번호, 금융정보 등 중요도가 높은 개인정보를 처리할 때에는 키보드, 화면, 메모리해킹, 랜섬웨어 등 신종 악성 프로그램에 대해 대응할 수 있도록 보안프로그램을 운영할 필요가 있으며, 항상 최신의 상태로 유지하여야 한다.

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

- 응용 프로그램이나 운영체제(OS) 보안 취약점 등을 악용하는 악성 프로그램 관련 경보가 발령되었거나, 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있을 때에는 즉시 업데이트를 실시하여야 한다.

- 응용 프로그램이나 운영체제에 보안 업데이트를 적용할 때에는 업무 연속성이 이루어 질 수 있도록 보안 업데이트를 적용하는 것이 필요하며, 가능한 자동으로 보안 업데이트가 설정되도록 할 필요가 있다.

참 고

☞ 한컴 오피스, MS 오피스 등 개인정보 처리에 자주 이용되는 응용 프로그램은 자동업데이트 설정 시, 보안 업데이트 공지에 따른 즉시 업데이트가 용이하다.

- 개인정보처리시스템 등의 보안 업데이트 적용 일자 및 설치·변경·제거 내용 등을 기록하는 형상관리를 권고한다.
- 사이버위기 경보 단계 및 보안 업데이트 공지 여부를 지속적으로 확인하여 보안 업데이트 적용 시점 및 방법 등을 검토하고 적용하여야 한다.

참 고

☞ 한국인터넷진흥원이 운영하는 인터넷 보호나라&Krcert(<https://krcert.or.kr>)에서 제공하는 “보안공지” 등을 활용할 수 있다.

제 8 조

물리적 접근 방지

제8조(물리적 접근 방지) ① 정보통신서비스 제공자등은 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소에 대한 출입통제 절차를 수립·운영하여야 한다.

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

③ 정보통신서비스 제공자등은 개인정보가 포함된 보조저장매체의 반출·입통제를 위한 보안대책을 마련하여야 한다.

해설

① 정보통신서비스 제공자등은 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소에 대한 출입통제 절차를 수립·운영하여야 한다.

- 정보통신서비스 제공자등은 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소에 출입통제 절차를 수립·운영하여야 한다.
 - 출입 요청 및 승인: 전산실, 자료보관실 등에 ‘출입 신청서’를 작성하여 개인정보 보호책임자 또는 전산실, 자료보관실 등 운영·관리책임자의 승인을 받아야 한다.
 - 출입 기록 작성: 출입에 관한 사항을 ‘출입 관리대장’에 기록하고 해당 업무 관계자가 이를 확인하여야 한다.
 - 출입 기록 관리: 정상·비정상적인 출입 여부, 장비 반입·반출의 적정성 등을 정기적으로 검토하여야 한다.

출입 신청서 및 관리대장 작성 (예시)

- ☞ 출입 신청서: 소속, 부서명, 신청자, 연락처, 출입일자, 입실·퇴실시간, 출입목적, 작업내역 등
- ☞ 출입 관리대장: 출입일자, 입실·퇴실시간, 출입자 정보(소속, 성명, 연락처), 출입목적, 승인부서, 입회자 정보(성명 등), 승인자 서명 등

- 이외에도 출입을 통제하는 방법으로는 물리적 접근 방지 장치(비밀번호 기반, 스마트 카드 기반, 지문 등 생체인식정보 기반, CCTV·카메라 기반 출입통제 장치 등)를 설치·운영하고 출입 내역을 전자적인 매체에 기록하는 방법 등이 있다.

참 고

- ☞ 전산실은 다량의 정보시스템을 운영하기 위한 별도의 물리적인 공간으로 전기시설(UPS, 발전기 등), 공조시설(항온항습기 등), 소방시설(소화설비 등)을 갖춘 시설을 말한다.
- ☞ 자료보관실은 가입신청서 등의 문서나 DAT(Digital Audio Tape), LTO(Linear Tape Open), DLT(Digital Linear Tape), 하드디스크 등이 보관된 물리적 저장장소를 말한다.

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

- 정보통신서비스 제공자등은 개인정보가 포함된 서류, 보조저장매체(이동형 하드디스크, USB메모리 등) 등을 금고, 잠금장치가 있는 캐비닛 등 안전한 장소에 보관하여야 한다.

③ 정보통신서비스 제공자등은 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다.

- 정보통신서비스 제공자등은 USB메모리, 이동형 하드디스크 등의 보조저장매체를 통한 개인정보의 유출 등을 방지하기 위하여 개인정보가 저장·전송되는 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다.

보조저장매체 반출·입 통제 시 고려사항 (예시)

- ☞ 보조저장매체 보유 현황 파악 및 반출·입 관리 계획
- ☞ 개인정보취급자 및 수탁자 등에 의한 개인정보 유출 가능성
- ☞ 보조저장매체의 안전한 사용 방법 및 인가되지 않은 사용의 대응조치
- ☞ USB를 PC에 연결시 바이러스 점검을 디폴트로 설정하는 등 기술적 안전조치 방안 등

제 9 조

출력·복사시 보호조치

제9조(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.

해설

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

■ 정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보를 출력(인쇄, 화면표시, 파일생성 등) 할 때에는 다음과 같은 사항 등을 고려하여 용도를 특정하고, 용도에 따라 출력 항목을 최소화 하여야 한다.

- 정보통신서비스 제공자등의 업무 수행 형태 및 목적, 유형, 장소 등 여건 및 환경에 따라 개인정보처리시스템에 대한 접근권한 범위내에서 최소한의 개인정보를 출력

참 고

 출력시 주의사항

- * 오피스(엑셀 등)에서 개인정보가 숨겨진 필드 형태로 저장되지 않도록 조치
- * 웹페이지 소스 보기 등을 통하여 불필요한 개인정보가 출력되지 않도록 조치 등

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.

- 정보통신서비스 제공자등은 개인정보가 포함된 종이 인쇄물, 외부 저장매체 등 출력·복사물을 통해 개인정보의 분실·도난·유출 등을 방지하고 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등에 필요한 보호조치를 갖추어야 한다.

출력·복사물 보호조치 (예시)

- ☞ 출력·복사물 보호 및 관리 정책, 규정, 지침 등 마련
 - ☞ 출력·복사물 생산·관리 대장 마련 및 기록
 - ☞ 출력·복사물 운영·관리 부서 지정·운영
 - ☞ 출력·복사물 외부반출 및 재생산 통제·신고·제한 등
-

제10조

개인정보 표시 제한 보호조치

제10조(개인정보 표시 제한 보호조치) 정보통신서비스 제공자 등은 개인정보 업무처리를 목적으로 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보보호를 위하여 개인정보를 마스킹하여 표시제한 조치를 취할 수 있다.

해설

- 정보통신서비스 제공자 등은 개인정보 업무처리를 목적으로 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보보호를 위하여 개인정보를 마스킹하여 표시 제한 조치를 취할 수 있다.
- 이용자의 개인정보를 다수의 개인정보처리시스템 등에서 각기 다른 방식으로 마스킹 할 때에는 다수의 개인정보처리시스템을 이용하여 개인정보취급자가 이용자 개인정보 집합을 구성할 수 있으므로 동일한 방식의 표시제한 조치가 필요하다.
- 이용자의 개인정보를 마스킹하면 개인정보 유출로 인한 2차 피해 확산을 방지할 수도 있다.

표시 제한 조치 (예시)

☞ 성명: 홍*동

☞ 연락처: 010-****-1234

☞ 주소: 서울시 송파구 중대로 **

☞ 접속지 IP: 123.123.***.123

| 구분 | ㉠시스템 | ㉡시스템 |
|-----|---------------|---------------|
| 성명 | 홍길동 | 홍길동 |
| 연락처 | 010-****-5678 | 010-1234-**** |
| 주소 | 송파구 중대로 1 | 송파구 중대로 1 |

☞ 위와 같이 연락처를 다른 방식으로 마스킹 할 때 개인정보취급자가 ㉠,㉡시스템을 통하여 홍길동의 연락처가 02-1234-5678 이라는 것을 확인할 수 있으므로 동일한 방식의 표시제한 조치를 권고한다.

제11조

재검토 기한

제11조(재검토 기한) 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.

해설

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

[부칙]

부칙 <제2020-5호, 2020.8.11.>

이 고시는 고시한 날부터 시행한다.

부칙 <제2021-3호, 2021.9.15.>

이 고시는 고시한 날부터 시행한다.

IV. 부 록

1. 정보통신서비스 제공자등을 위한 망분리 해설
2. F A Q

I. 정보통신서비스 제공자등을 위한 망분리 해설

1. 망분리 개요

1. 법적 근거 및 취지

- 개인정보취급자의 업무용 컴퓨터 등이 정보통신망을 통하여 악성코드에 감염되는 등 불법적인 접근을 차단하고 침해사고를 방지하기 위하여 망분리 제도가 시행되었다. 정보통신망법에서는 대규모 개인정보 유출사고가 발생하는 것을 방지하기 위하여 다음과 같이 망분리에 관한 사항을 규정하고 있다.

개인정보 보호법 시행령

제48조의2(개인정보의 안전성 확보 조치에 관한 특례) ① 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제3호에 해당하는 자를 말한다. 이하 같다)와 그로부터 이용자(같은 법 제2조제1항제4호에 해당하는 자를 말한다. 이하 같다)의 개인정보를 법 제17조제1항제1호에 따라 제공받은 자(이하 "정보통신서비스 제공자등"이라 한다)는 이용자의 개인정보를 처리하는 경우에는 제30조에도 불구하고 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다.

2. 개인정보에 대한 불법적인 접근을 차단하기 위한 다음 각 목의 조치

다. 개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등에 대한 외부 인터넷망 차단[전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제2호에 따른 정보통신서비스를 말한다. 이하 같다) 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등만 해당한다)

개인정보의 기술적·관리적 보호조치 기준

제4조(접근통제) ⑥ 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 제공자등은 개인정보처리 시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 한다.

2. 용어 정의

- “망분리”란 외부 인터넷망을 통한 불법적인 접근과 내부정보 유출을 차단하기 위해 업무망과 외부 인터넷망을 분리하는 망 차단조치를 말한다.
- “다운로드”란 개인정보처리시스템에 접근하여 개인정보취급자의 컴퓨터 등에 개인정보를 엑셀, 워드 등의 파일형태로 저장하는 것을 말한다.
- “파기”란 개인정보처리시스템에 저장된 개인정보 파일, 테이블 또는 데이터베이스(DB)를 삭제하는 것을 말한다.
- “접근권한 설정”이란 개인정보처리시스템에 접근하는 개인정보취급자에게 다운로드, 파기 등 접근권한을 설정하는 것을 말한다.

3. 적용 대상 및 범위

- 망분리를 적용하여야 하는 정보통신서비스 제공자등은 다음과 같다.

| 적용 대상 |
|--|
| 전년도말 기준 직전 3개월간 개인정보가 저장·관리되고 있는 이용자수가 일일평균 100만명 이상 |
| ※ 일일평균 이용자수 = $\frac{\text{일일 보유량(10, 11, 12월)의 총합}}{92(\text{일수})}$ |
| 또는 정보통신서비스 부문 전년도(전 사업년도) 매출액이 100억원 이상 |

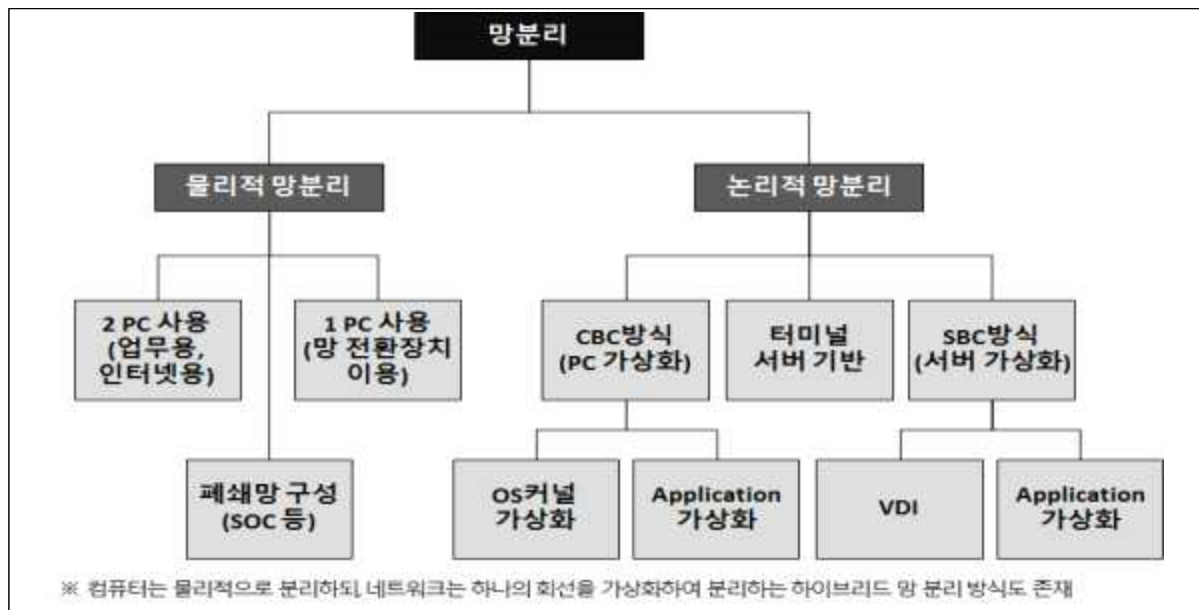
- 위에 해당하는 정보통신서비스 제공자등은 다음에 대하여 망분리를 적용하여야 한다.

| 적용 범위 |
|---|
| ① 개인정보처리시스템에서 개인정보를 다운로드할 수 있는 개인정보취급자의 컴퓨터 등 |
| ② 개인정보처리시스템에서 개인정보를 파기할 수 있는 개인정보취급자의 컴퓨터 등 |
| ③ 개인정보처리시스템에 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등 |

2. 주요 망분리 방식

1. 망분리 방식 비교

- 업무망과 인터넷망을 분리하는 방식은 물리적 망분리와 논리적 망분리 등으로 구분할 수 있으며, 다음에서 제시된 방식 이외에도 다양한 방식이 존재할 수 있다. 다만, 외부 인터넷망을 통한 불법적인 접근과 내부정보 유출을 차단할 수 있도록 업무망과 외부 인터넷망을 분리하여야 한다.



- 물리적 망분리와 논리적 망분리는 다음과 같은 장·단점을 가지고 있다. 이러한 장·단점은 일반적인 상황을 가정한 것으로서 구성 방식과 설정 등에 따라 달라질 수 있다.

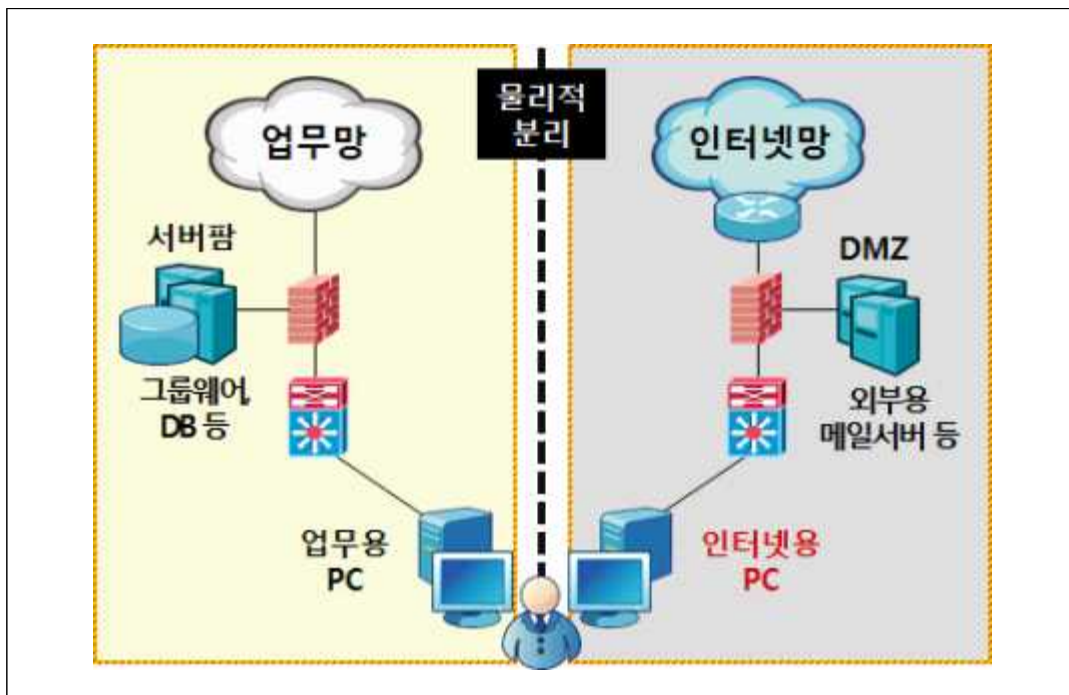
| 구 분 | 물리적 망분리 | 논리적 망분리 |
|-------|---------------------------|-------------------------------------|
| 운영 방법 | - 업무용 망과 인터넷용 망을 물리적으로 분리 | - 가상화 등의 기술을 이용하여 논리적으로 분리 |
| 도입 비용 | - 높음(추가 PC, 별도 망 구축 등) | - 구축환경에 따라 상이함 |
| 보안성 | - 높은 보안성(근본적 분리) | - 상대적으로 낮은 보안성(구성 방식에 따라 취약점 발생 가능) |
| 효율성 | - 업무 환경의 효율성 저하 | - 상대적으로 관리 용이 |

2. 물리적 망분리

- 물리적 망분리는 업무망과 인터넷망을 물리적으로 분리할 뿐만 아니라 각 망에 접속하는 컴퓨터도 물리적으로 분리하여 망간 접근경로를 차단하는 방식을 말한다.
 - 어떠한 때에도 동일한 시점에 한 컴퓨터에서 업무망과 인터넷망을 동시에 접속할 수 없도록 하는 방식
 - 업무망 컴퓨터에서 인터넷망과의 연결점을 제거하여 인터넷으로부터의 악성코드 감염, 해킹, 개인정보 유출 등의 경로를 원천적으로 차단하는 방법
- 물리적 망분리를 적용하기 위해서는 ① [방식1] 2대 컴퓨터 이용 망분리, ② [방식2] 망전환장치 이용 망분리, ③ [방식3] 물리적 폐쇄망 구축 등의 방식을 선택할 수 있다.
 - 이외에도 물리적 망분리와 논리적 망분리를 혼용하거나, 컴퓨터는 2대로 분리하되 네트워크는 하나의 망을 가상화하는 등의 하이브리드 형태의 망 분리도 적용 가능
- 물리적 망분리 적용 시, 업무망 컴퓨터에서 인터넷이 접속되거나 악성코드가 감염되지 않도록 하는 등의 보안정책을 수립하고 안전하게 관리하는 것이 매우 중요하며 다음과 같은 방법 등이 활용될 수 있다.
 - 비인가된 디바이스(컴퓨터, 스마트폰 등)의 업무망(폐쇄망) 연결 통제
 - 업무망 컴퓨터의 IP변경, 인터넷용 랜케이블 연결 등을 통한 인터넷망 연결 차단
 - 업무망 컴퓨터에서의 테더링 등 망분리 우회 등을 통한 인터넷 사용 차단
 - 2개의 랜카드를 사용하여 업무망과 인터넷망 동시 연결 차단
 - 업무망과 인터넷망 간의 자료 전송이 반드시 필요할 때에는 안전한 방식 적용(망연계시스템, 보안 USB 등)
 - 외부 이메일을 통한 악성코드 유입 및 개인정보 유출 차단(인터넷용 메일 시스템 도입 등)
 - USB 연결을 통한 악성코드 유입 및 개인정보 유출 차단
 - 프린터 등 주변기기에 대하여도 업무용, 인터넷용 분리 운영

① [방식1] 2대 컴퓨터 이용 망 분리

- “2대 컴퓨터 이용 망분리”란 인터넷망에 접근하는 컴퓨터와 업무망에 접근하는 컴퓨터를 별도로 사용하는 방식을 말한다.
 - 인터넷용 컴퓨터와 업무용 컴퓨터를 구분하고, 인터넷용 컴퓨터는 인터넷망에 그리고 업무용 컴퓨터는 업무망에 연결하여 사용한다.

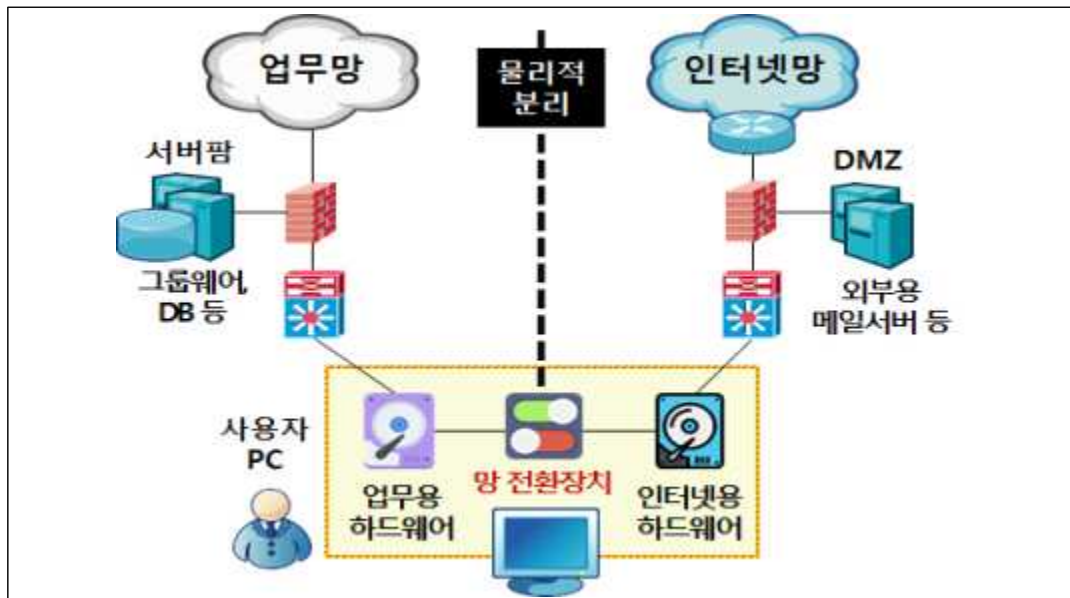


- 이 방식은 업무망과 인터넷망간의 접근경로가 물리적으로 차단되어 보안성이 높다는 장점이 있으나 별도 네트워크 구축, 컴퓨터 추가 구매 등에 따라 비용 증가 및 관리의 어려움이 있다는 단점이 있다.

| 구 분 | 설 명 |
|-----|--|
| 장 점 | - 인터넷망과 업무망 간 접근경로가 물리적으로 차단되어 보안성 높음 |
| 단 점 | - 별도 네트워크 구축, PC 등 추가 장비에 비용 소요 - 추가 장비로 인한 공간 및 에너지 소비 증가 - 추가 장비에 보안 관리의 부담 증가 등 |

② [방식2] 1대 컴퓨터 이용 망 분리

- “1대 컴퓨터 이용 망분리”란 하드디스크, IP주소 등 정보처리 및 네트워크 연결 자원을 분할한 컴퓨터에 망 전환장치를 사용하여 인터넷망과 업무망에 선택적으로 접속하는 방식을 말한다.

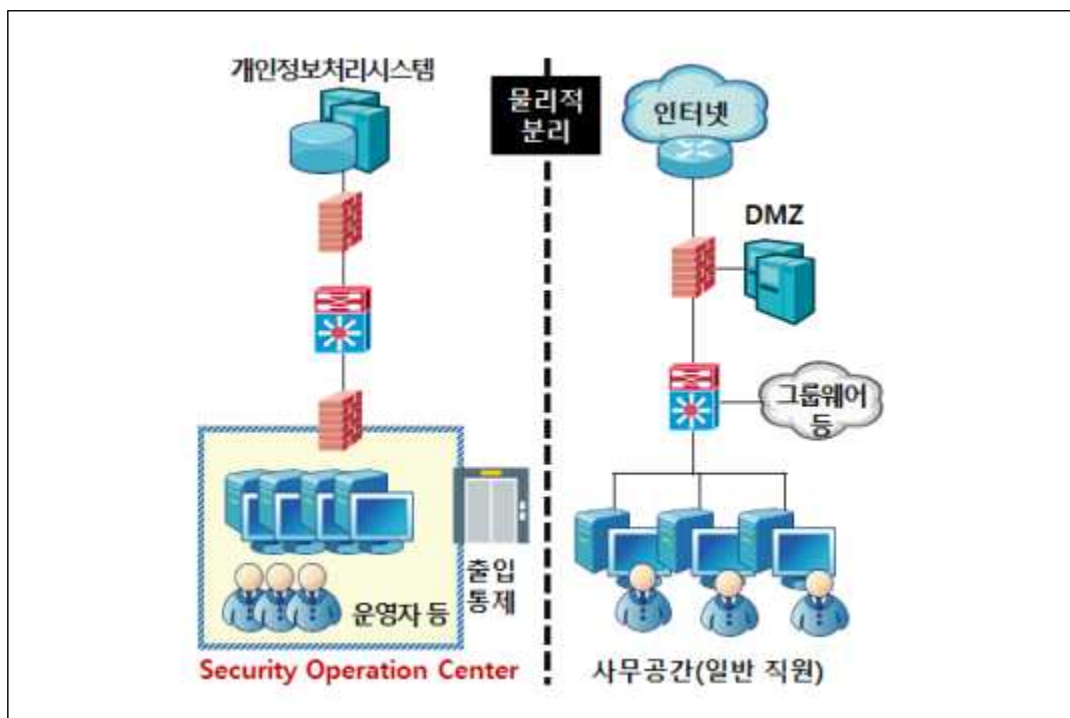


- 이 방식은 사무 공간이 협소할 때 적합할 수 있으나 망 전환 시 재부팅 등 이용자 불편을 초래하는 단점이 있을 수 있다.
 - 하나의 컴퓨터 케이스에 2개의 메인보드, 하드드라이브가 각각 설치되어 동시에 부팅 및 사용이 가능한 듀얼 컴퓨터 등 다양한 하드웨어 장치가 존재한다.

| 구 분 | 설 명 |
|-----|--|
| 장 점 | <ul style="list-style-type: none"> - 인터넷망과 업무망 간 접근경로가 물리적으로 차단되어 보안성 향상 - 협소한 사무 공간에 적합 |
| 단 점 | <ul style="list-style-type: none"> - 별도 네트워크 구축, 망 전환장치 설치 등 추가 장비에 비용 소요 - 망 전환 시 재부팅이 필요할 수 있으며, 이에 따라 업무 수행시간 지연 가능 |

③ [방식2] 물리적 폐쇄망 구성(SOC 등)

- 업무적으로 인터넷 사용이 반드시 필요할 때가 아니라면, 업무망 컴퓨터에 인터넷망과의 연결점을 제거하여 특정 물리적 공간을 폐쇄망으로 구성하는 방식을 고려할 수 있다.
 - SOC(Security Operation Center) : 물리적으로 접근이 통제된 공간을 폐쇄망으로 구성하여, 개인정보처리시스템의 운영, 관리 목적의 접근은 SOC에서만 가능하도록 구성한다.
 - 데이터센터 운영실을 인터넷 접속이 불가능한 폐쇄망으로 구성하고 인터넷 접속이 필요할 때 별도의 인터넷 접속용 컴퓨터를 통해서 접속하도록 구성한다.



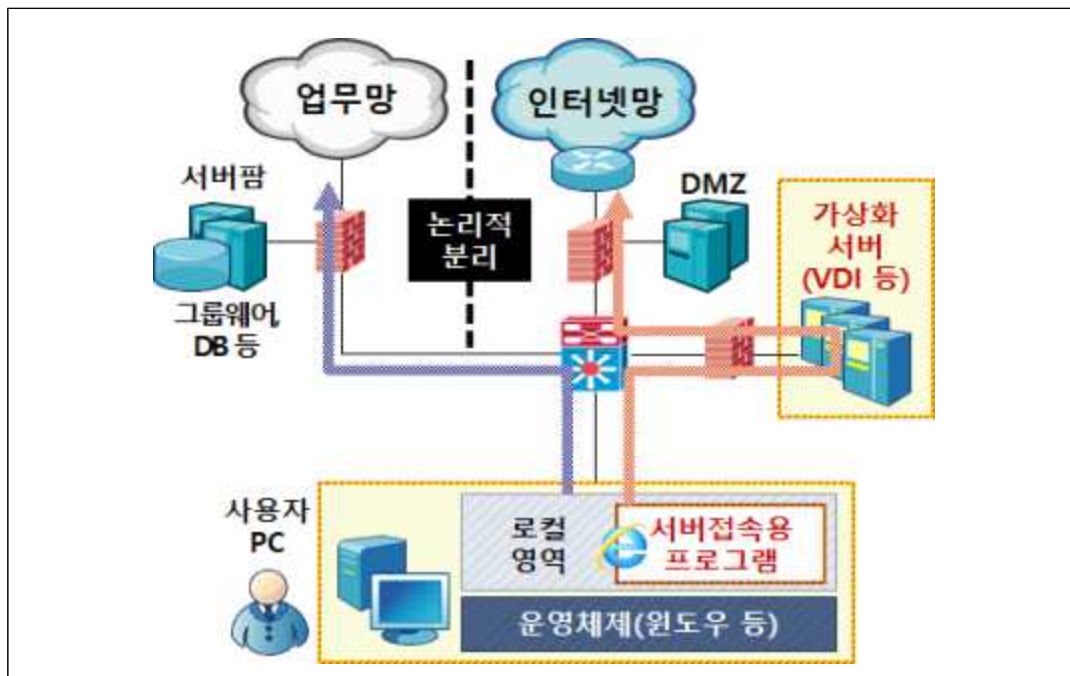
- 이 방식은 개인정보처리시스템의 직접 접속은 물리적으로 분리된 공간에서만 가능하게 함으로써 보안성을 향상할 수 있는 장점이 있는 반면에 물리적 공간 및 통제장치 마련에 따라 비용이 크게 소요될 수 있으며 업무 불편이 증가할 수 있다. 이는 폐쇄망 구성을 어떻게 하는지에 따라 매우 상이하므로 구축 방식에 따른 비용, 효과성 등을 사전에 충분히 검토 후 적용할 필요가 있다.

3. 논리적 망 분리

- 논리적 망 분리는 가상화 기술을 이용하여 서버 또는 컴퓨터를 가상화함으로써 논리적으로 업무망과 인터넷망을 분리하는 방식을 말한다.
 - 일반적으로 1대의 컴퓨터에서 일반 영역과 가상 영역을 접속하여 업무를 수행
 - 가상환경 접속용 전용 장치(Zero Client 등)를 사용 등
- 논리적 망 분리 방식은 ① [방식1] 서버기반 논리적 망분리(SBC, Server Based Computing), ② [방식2] 컴퓨터기반 논리적 망분리(CBC, Client Based Computing) 등으로 구분할 수 있다.
 - 이외에도 컴퓨터에 설치된 서버접속용 프로그램으로 인터넷망 터미널 서버에 접속하여 인터넷을 사용하는 터미널 서버기반 인터넷망 분리 방식이 있을 수 있다.
- 논리적 망분리는 일반적으로 물리적 망분리에 비해 상대적으로 보안성이 떨어질 수 있으므로, 논리적 망분리 방식을 적용할 때에는 가상화 기술에 관한 보안 위협 등에 대해 충분히 검토하고 대책을 수립하여야 하며, 이를 위해 다음과 같은 방법 등이 활용될 수 있다.
 - 가상화 기술(하이퍼바이저 등)의 취약점 확인 및 조치
 - 업무망과 인터넷망 간의 자료 전송이 필요할 때에는 안전한 방식 적용(망연계 시스템 등)
 - 외부 이메일 통한 악성코드 유입 및 개인정보 유출 차단(인터넷용 메일시스템 도입 등)
 - 논리적 망분리 설정 오류 등에 따른 업무망과 인터넷망 간의 접점 또는 우회접속 경로 차단
 - 동일한 네트워크 구간에 위치한 망분리 미적용 컴퓨터에 의한 침해 대책 마련
 - 가상화 되지 않은 영역(로컬 컴퓨터 등)에 대한 침해로 인해 가상화 영역이 동시에 침해 받을 수 있는 가능성 검토 및 대책 마련 등

① [방식1] 서버기반 논리적 망분리

- 서버기반 논리적 망분리는 인터넷 접속, 업무 수행 등 기존에 수행하던 작업을 가상화 서버, 터미널 서버 등에 접속하여 수행함으로써, 논리적으로 인터넷망과 업무망을 분리한다.
 - 세부적으로는 윈도우즈, 리눅스 등 운영체제(OS) 레벨에서 가상환경을 제공하는 VDI(Virtual Desktop Infrastructure, 데스크톱 가상화)와 특정 어플리케이션에 가상환경을 제공하는 어플리케이션 가상화 방식으로 구분될 수 있다.



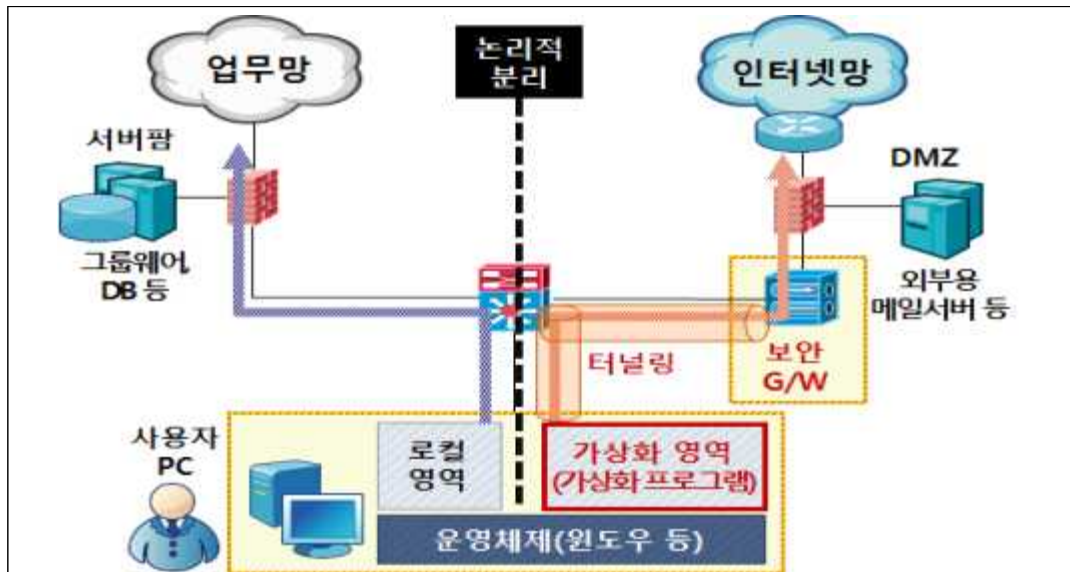
- 서버기반 논리적 망분리를 할 때 개인정보처리시스템의 운영·개발·보안을 목적으로 DB 서버 등에 접속하는 개인정보취급자(예시 : 데이터베이스 운영관리자)의 컴퓨터는 인터넷망 영역을 가상화 하는 방식을 적용하여야 한다. 업무망 영역을 가상화할 때는 사용자 컴퓨터(로컬영역)가 악성코드에 감염되거나 해킹을 당할 때, 업무망으로의 악성코드 유입 및 불법적인 침해 발생이 가능하기 때문이다.

- 인터넷망 가상화 방식과 업무망 가상화 방식은 다음과 같이 비교할 수 있다.

| 구 분 | 인터넷망 가상화 | 업무망 가상화 |
|-----|--|--|
| 특 징 | <ul style="list-style-type: none"> - 업무는 사용자 컴퓨터에서 직접 수행 - 인터넷은 컴퓨터에 설치된 서버접속용 프로그램으로 인터넷망 가상화 서버에 접속하여 사용 | <ul style="list-style-type: none"> - 인터넷은 사용자 컴퓨터에서 직접 사용 - 업무는 컴퓨터에 설치된 서버접속용 프로그램으로 업무용 가상화 서버에 접속하여 수행 |
| 장 점 | <ul style="list-style-type: none"> - 가상화 서버환경에 사용자 통제 및 관리정책 일괄적용 가능 - 가상화된 인터넷 환경 제공으로 인한 악성코드 감염 최소화 - 인터넷 환경이 악성코드에 감염 되거나 해킹을 당해도 업무 환경은 안전하게 유지 가능 | <ul style="list-style-type: none"> - 가상화 서버 환경에 업무정보가 저장됨에 따라 업무 데이터에 중앙 관리 및 백업 용이, 내부정보 유출 방지 효과 증가 - 사용자 통제 및 관리 정책 일괄 적용 가능 |
| 단 점 | <ul style="list-style-type: none"> - 가상화 서버 구축을 위한 비용발생 - 가상화 서버를 다수의 사용자가 동시에 사용함에 따라 컴퓨터와 가상화 서버간 네트워크 트래픽 증가로 인터넷망 트래픽 증가 및 속도 지연 가능 - 가상화 서버 환경에서 실행되는 보안 프로그램(인터넷 뱅킹 등)에 호환성 검토 필요 | <ul style="list-style-type: none"> - 가상화 서버 구축을 위한 비용발생 - 가상화 서버 성능 및 용량이 충분 하지 못할 때 속도 저하, 업무 지연 등 발생 - 가상화 서버 장애 발생 시 업무 중단 - 가상화 서버 환경에서 실행되는 업무 프로그램, 보안프로그램 등에 호환성 검토 필요 - 사용자 컴퓨터(로컬영역)가 악성코드에 감염되거나 해킹당한 때, 업무망으로의 악성코드 유입 및 불법적인 침해 발생 가능 |

② [방식2] 컴퓨터기반 논리적 망분리

- 컴퓨터기반 논리적 망분리는 인터넷 접속 등의 작업을 컴퓨터기반 가상화 기술(CBC, Client Based Computing)이 적용된 영역에서 수행함으로써 인터넷망과 업무망을 논리적으로 분리한다.
 - 세부적으로는 윈도우즈, 리눅스 등 운영체제(OS) 레벨에서 가상환경을 제공하는 OS커널 가상화와 웹 브라우저 등 특정 어플리케이션에 가상환경을 제공하는 어플리케이션 가상화 방식으로 구분될 수 있다.



- 이 방식은 사용자 컴퓨터의 영역을 분리하는 컴퓨터 가상화 전용프로그램을 설치하고, 분리된 가상영역에서 인터넷 등을 사용하도록 구성된다.
 - 서버가상화 기반 망분리 방식에 비해 별도의 가상화 서버 구축이 불필요함에 따라 비용이 상대적으로 절감되는 장점이 있는 반면에, 사용자 컴퓨터에 설치된 운영체제, 응용프로그램과의 호환성 등에 대해 충분한 검토가 필요하다.

| 구 분 | 설 명 |
|-----|--|
| 장 점 | <ul style="list-style-type: none"> - 가상화 영역에 사용자 통제 및 관리 정책 일괄 적용 가능 - 기존 업무용 단말기를 활용하여 상대적으로 도입 비용이 낮음 |
| 단 점 | <ul style="list-style-type: none"> - 운영체제(OS) 및 다양한 컴퓨터 환경, 응용프로그램에 호환성 확인 필요 - 사용 중인 운영체제, 응용프로그램, 보안프로그램의 패치 등 변경 발생 시 영향도에 따른 지속적인 관리 및 지원 필요 |

3.

망분리 적용 시 고려사항

- 망분리 구성 및 설정 상의 취약점을 이용한 업무망 침투, 대량의 개인정보 유출 사고 등이 발생하고 있으므로 망분리 적용 시 충분한 보안성 검토 등을 통하여 안전하게 구성하여야 한다.
- 또한, 망분리 적용자와 미적용자가 동일한 네트워크 구간에 존재하는 경우 망분리 미적용자의 컴퓨터를 경유하여 개인정보처리시스템에 침투하는 사례도 발생하고 있으므로 이에 필요한 대책을 수립·적용할 필요가 있다.

| 구 분 | 주요 고려 사항 | 보안기술 (예시) |
|------------------|--|--|
| PC 보안관리 | <ul style="list-style-type: none"> - 네트워크 설정 임의 변경 등 망 분리 우회경로 차단 (업무용 컴퓨터의 인터넷 연결, 추가 랜카드 설치 및 각 망에 동시 연결, 비인가된 무선인터넷 연결 및 스마트폰 테더링, IP주소 임의 변경 등) - 비인가자의 임의사용 금지를 위한 PC보안 상태 유지·관리 (로그온 암호설정, 화면보호기, 공유폴더 제한 등) - USB메모리 등 보조저장매체를 통한 정보유출 및 악성코드 감염 대책 마련 등 | <ul style="list-style-type: none"> - 컴퓨터보안 - NAC(Network Access Control) - IP관리 등 |
| 망간 자료전송 통제 | <ul style="list-style-type: none"> - 업무망 컴퓨터와 인터넷망 컴퓨터간 안전한 데이터 전달 방법 제공 - 인터넷망과 업무망, 전송통제서버 간 통신은 일반적인 형태의 TCP/IP 방식이 아닌 암호화된 전용프로토콜을 사용하고 일방향성을 유지(공유스토리지 연계방식, UTP기반 전용프로토콜 연계방식, IEEE1394 연계방식 등) - 망간 자료전송 시 책임자 승인절차, 사용자 인증 및 권한 관리, 전송내역 보존, 악성코드 검사 등 수행 등 | <ul style="list-style-type: none"> - 망연계솔루션 - 보안USB 등 |
| 인터넷 메일사용 | <ul style="list-style-type: none"> - 업무망 컴퓨터에서 외부 이메일 수신 차단 - 외부 이메일 송·수신을 위한 메일서버는 업무망과 분리하고 인터넷 컴퓨터에서만 접근가능 하도록 구성 등 | <ul style="list-style-type: none"> - 인터넷 전용 메일서버 등 |

| 구 분 | 주요 고려 사항 | 보안기술 (예시) |
|------------------------|--|--|
| 패치 관리 | <ul style="list-style-type: none"> - 인터넷 컴퓨터 및 업무용 컴퓨터에 신속하고 지속적인 보안 패치(보안업데이트) - 패치관리시스템 도입 시 외부 인터넷과 분리하여 운영 - 인터넷이 차단된 업무용PC에 패치관리 절차 수립 및 이행 (관리자가 수동으로 다운로드 후 무결성 검증 및 악성코드 감염여부 등을 확인하고 패치관리시스템에 적용 등) - 패치관리시스템에 보안관리 강화(인가된 관리자만 접속할 수 있도록 접근통제 등) 등 | <ul style="list-style-type: none"> - 패치 관리 시스템(인터넷망용, 업무망용) 등 |
| 네트워크 접근제어 | <ul style="list-style-type: none"> - 비인가된 기기(PC, 노트북, 스마트폰 등)는 인터넷망과 업무망에 접속할 수 없도록 차단 등 | <ul style="list-style-type: none"> - NAC - IP관리 등 |
| 보조저장 매체 관리 | <ul style="list-style-type: none"> - 인가된 보조저장매체(USB메모리, 외장하드 등)만 사용하도록 제한 등 | <ul style="list-style-type: none"> - 보안USB - 컴퓨터보안 - DLP 등 |
| 프린터 등 주변기기 운영 | <ul style="list-style-type: none"> - 프린터 등 주변기기는 인터넷용 또는 업무용으로 분리.운영 - 프린터를 공유할 때, 공유프린터에서 서로 다른 연결 포트를 사용하고 프린터 서버 등을 이용하여 접근통제 등 | <ul style="list-style-type: none"> - 복합기보안 등 |
| 기타 보안관리 | <ul style="list-style-type: none"> - 망분리 대상자에 인식제고 교육 수행 - 동일한 네트워크 구간에 망분리 대상자와 미대상자가 혼재되어 있을 때, 이에 따른 위험평가 및 대책수립 - 가상환경 및 시스템 접속 시 강화된 인증 적용(OTP, 보안토큰 등) - 서버 및 DB 레벨에서의 접근제어 (망 분리 환경을 우회한 서버.DB 접근 및 정보유출 차단) - 서버에서의 불필요한 인터넷 접속 차단 - 망 분리 상태, PC보안 관리 현황, 규정 준수 여부, 보안 취약점 등 정기점검 수행 등 | <ul style="list-style-type: none"> - NAC - OTP - 서버접근제어 - DB접근제어 등 |

II. FAQ

Q1

부가통신사업자로 신고하였으나 해당 사업에서 개인정보를 수집하지는 않고, 오프라인으로 컴퓨터를 판매하는 과정에서 고객의 개인정보를 수집하고 있는 때에도 이 기준을 이행하여야 합니까?

⇒ 부가통신사업자로 신고하여 “정보통신서비스 제공자등”의 범위에 속하더라도 정보통신서비스와 관계없이 오프라인에서만 고객의 개인정보가 처리된다면 이 기준이 적용되지 않습니다.

이러한 때에는 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치) 제1항에 따른 ‘개인정보의 안전성 확보조치 기준’을 이행하여야 합니다.

Q2

여행사입니다. 홈페이지를 운영하고 있지는 않지만 오프라인으로 여행상품의 계약 등을 하는 과정에서 고객의 개인정보를 수집하고 있을 때에도 이 기준을 이행하여야 합니까?

⇒ 정보통신서비스를 제공하고 있지 않은 사업자일 때에는 이 기준이 적용되지 않습니다. 이러한 때에는 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)제1항에 따른 ‘개인정보의 안전성 확보조치 기준’을 이행하여야 합니다.

Q3

회사에서 내부 직원의 인사관리에 사용되는 시스템을 보유·운영할 때에도 이 기준을 이행하여야 합니까?

⇒ 전기통신사업자의 전기통신역무를 이용하여 고객에게 정보를 제공하거나 정보의 제공을 매개하지 않고 회사 내부에서만 직원관리 용도 등으로 사용할 때에는 이 기준이 적용되지 않습니다.

이러한 때에는 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치) 제1항에 따른 ‘개인정보의 안전성 확보조치 기준’을 이행하여야 합니다.

Q4

금융 회사에서 개인정보 보호를 위한 기술적·관리적·물리적 보호조치를 이행하려고 하는데 이 기준을 이행하면 됩니까? 아니면 다른 기준을 이행하여야 합니까?

⇒ 금융 업종에 속하는 사업자일 때는 「신용정보의 이용 및 보호에 관한 법률」의 적용을 받습니다. 따라서 같은 법 제19조(신용정보전산시스템의 안전보호)에 따른 ‘신용정보업감독규정’을 이행하여야 합니다.

다만, 해당 사업자가 인터넷 홈페이지 등을 이용하여 정보 및 서비스를 제공할 때에는 영리 목적의 정보통신서비스 제공자에 해당하므로 ‘신용정보업감독규정’에서 정하지 않은 사항에 대해서는 이 기준을 이행하여야 합니다.

Q5

당사는 자동차판매회사로서 고객정보가 취득되는 경로를 보면 당사 차량구입고객정보, 오토카드, 정비고객, 영업사원 취득정보, 홈페이지 회원 정보, 이벤트 참여고객 등으로 나누어지는데 보호조치 기준을 이행하여야 하는 고객정보에는 홈페이지 회원 정보만 해당되는 건가요?

⇒ 자동차 판매회사는 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치)제1항에 따른 ‘개인정보의 안전성 확보조치 기준’을 이행하여야 합니다.

다만, 인터넷 홈페이지를 통해 서비스를 제공하는 부분에 대해서는 주된 사업 형태인지 여부, 인터넷 홈페이지를 통해서 처리되는 개인정보의 양 등을 고려하여 보호조치 기준 적용여부를 판단하여야 합니다. 오프라인 자동차 판매의 목적을 부수적으로 지원하는 것에 그친다고 볼 수 없고 처리되는 개인정보의 양이 적지 않다면 영리 목적의 정보통신서비스 제공자등으로 보아 이 기준을 이행하여야 합니다.

Q6

고시 제1조(목적)의 개인정보의 안전성 확보에 필요한 기술적·관리적 및 물리적 보호조치에 관한 최소한의 기준이란 무엇을 의미하는지?

⇒ 이 기준에서 정하는 사항은 정보통신서비스 제공자등이 개인정보의 안전성 확보를 위하여 반드시 준수하여야 하는 최소한의 기준입니다.

따라서 이외에도 정보통신서비스 제공자등은 사업규모, 서비스의 유형, 개인정보 보유 수, 처리하는 개인정보의 유형 및 중요도, 개인정보를 처리하는 방법 및 환경, 보안위험요인 등을 고려하여 스스로의 환경에 맞도록 필요시 추가적인 개인정보 보호조치 기준을 수립하고 시행하여야 합니다.

Q7

개인정보처리시스템의 범위는 어디까지를 말하는지요?

⇒ 개인정보처리시스템이란 일반적으로 데이터베이스(DB)와 데이터베이스 내의 데이터에 접근할 수 있도록 해주는 응용시스템을 의미하며, 데이터베이스를 구축하거나 운영하는데 필요한 시스템을 말합니다. 다만, 개인정보처리시스템은 정보통신서비스 제공자등의 개인정보 처리 방법, 시스템 구성 및 운영 환경 등에 따라 달라질 수 있습니다. 업무용 컴퓨터, 노트북도 데이터베이스 관련 응용프로그램이 설치·운영되어 개인정보취급자가 사용하거나, 웹서버라도 데이터베이스에 연결되어 개인정보를 처리하는 경우에는 개인정보처리시스템에 해당될 수 있습니다.

개인정보처리시스템 (예시)

- ☞ 데이터베이스를 구성·운영하는 시스템 그 자체
- ☞ 응용프로그램(Web서버, WAS 등) 등을 데이터베이스의 개인정보를 처리할 수 있도록 구성할 때
- ☞ 개인정보의 처리를 위해 파일처리시스템으로 구성할 때
- ☞ 업무용 컴퓨터, 노트북 등에 데이터베이스 관련 응용프로그램을 설치·운영하여 개인정보취급자가 개인정보를 처리할 수 있도록 구성할 때 등

Q8

이용자가 접속하는 웹페이지도 개인정보처리시스템 입니까?

⇒ 이용자가 접속하는 웹페이지를 통해 데이터베이스 내의 데이터(개인정보)에 접근하여 조회, 수정, 삭제 등 처리할 수 있다면 개인정보처리시스템에 해당됩니다.

Q9

내부관리계획에 출력·복사시 보호조치에 관한 사항도 포함하여야 합니까?

⇒ 제3조제1항제4호(개인정보의 기술적·관리적 보호조치 이행 여부의 내부 점검에 관한 사항)에 따라 이 기준에서 정하는 기술적·관리적 및 물리적 보호조치에 관한 사항은 모두 포함되어야 합니다. 결국 이 기준 제9조(출력·복사시 보호조치)에 관한 사항도 포함되어야 합니다.

Q10

내부관리계획의 변경·업데이트 주기는 어떻게 해야 합니까

⇒ 개인정보보호 관련 법·제도의 제·개정 여부를 정기적으로 확인하여 변경이 있을 때에는 변경 사항을 반영하고 개인정보 처리 방법, 처리 환경 및 보호조치 사항 등에 변경이 있을 때에도 변경사항을 내부관리계획에 반영하여 시행하여야 합니다.

Q11

개인정보 보호책임자는 새로운 임원으로 별도 채용해야 하나요?

⇒ 반드시 새로운 임원을 별도 채용하지 않아도 됩니다.

개인정보 보호책임자는 임원 또는 개인정보와 관련하여 이용자의 고충처리 담당부서의 장 등을 지정할 수 있으며, 별도로 새로운 인력을 채용하여 개인정보 보호책임자로 지정할 수도 있습니다.

다만, 개인정보 보호책임자는 「개인정보 보호법」 제31조(개인정보 보호책임자의 지정)에서 정하는 요건을 충족한 자로 지정하여야 합니다.

Q12

개인정보보호 교육은 누구를 대상으로 해야 하는 것인가요?

⇒ 고객의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하는 ‘개인정보 보호책임자’ 그리고 고객의 개인정보를 처리하는 ‘개인정보취급자’ (정규직, 비정규직, 파견직, 시간제 등 근로형태 불문) 등을 대상으로 개인정보보호 교육을 실시하여야 합니다.

Q13

정보보호 교육의 일부분으로 개인정보보호에 관한 사항이 포함되었다면 개인정보보호 교육을 실시한 것으로 볼 수 있나요?

⇒ 교육과정명이 ‘정보보호 교육’이라 하더라도 회사 내부의 ‘개인정보보호 교육 계획’에 의해 실시되었다면 개인정보보호 교육으로 볼 수 있습니다.

다만, 이러한 때에는 교육 목적, 대상, 내용, 일정, 방법 등이 개인정보보호 교육 계획과 맞아야 합니다. 교육 실시 결과는 문서화하여 보관하도록 합니다.

Q14

개인정보취급자의 접근권한 부여는 어떻게 해야 하나요?

⇒ 정보통신서비스 제공자등은 개인정보처리시스템에 접근권한을 서비스 제공을 위해 필요한 최소한의 인원에게 부여해야 합니다. 특히, 개인정보처리시스템의 데이터베이스(DB)에 직접 접속은 데이터베이스 운영·관리자에 한정하는 등의 보호조치를 적용할 필요성이 있습니다. 정보통신서비스 제공자등은 개인정보처리시스템에 열람, 수정, 다운로드 등 접근권한을 부여할 때에는 서비스 제공을 위해 필요한 범위에서 구체적으로 차등화 하여 부여하여야 합니다.

Q15

개인정보처리시스템에 접근권한의 변경·말소는 어떻게 해야 하나요?

⇒ 정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 합니다. 여기서, ‘지체 없이’란 정당한 사유가 없는 한 즉시 조치하여야 함을 의미합니다.

정보통신서비스 제공자등은 불완전한 접근권한의 변경 또는 말소 조치로 인하여 정당한 권한이 없는 자가 개인정보처리시스템에 접근될 수 없도록 하여야 합니다.

접근권한 변경·말소 미조치 사례 (예시)

- ☞ 다수 시스템의 접근권한 변경·말소가 필요함에도 일부 시스템의 접근권한만 변경·말소할 때
 - ☞ 접근권한의 전부를 변경·말소하여야 함에도 일부만 변경·말소할 때
 - ☞ 접근권한 말소가 필요한 계정을 삭제 또는 접속차단조치를 하였으나, 해당 계정의 인증값 등을 이용하여 우회 접근이 가능할 때 등
-

Q16

침입 탐지 및 유출 탐지 기능을 갖춘 접근통제 장치만 설치한다면, 이 기준에서 정한 접근통제 요구사항을 충족하나요?

⇒ 아닙니다.

단순히 방화벽 등 정보보호 솔루션을 구매 및 설치하는 것만으로는 부족하며 신규 위협 대응 및 정책의 관리를 위하여 정책설정의 지속적인 업데이트 적용 및 운영·관리, 이상행위 대응, 로그분석 등의 방법으로 체계적으로 운영·관리를 하여야 합니다.

Q17

현재 설치·운영중인 침입차단시스템, 침입탐지시스템을 교체·변경하려고 합니다. 시스템의 규격, 성능 등을 이 기준에서 정하고 있습니까?

⇒ 이 기준에서는 침입차단시스템, 침입탐지시스템 등의 설치 규격, 성능 등을 정하고 있지 않습니다.

다만, 이 기준에서 정하는 사항을 이행하기 위하여 필요한 기능이 해당 시스템에서 제공되는지 여부를 사전에 확인하기 바랍니다.

Q18

일정시간 이상 업무처리를 하지 않을 때 자동으로 시스템 접속이 차단되도록 하는 최대 접속시간은 어느 정도를 의미합니까?

⇒ 정보통신서비스 제공자등은 개인정보를 처리하는 방법 및 환경, 보안위험요인, 업무특성(DB 운영·관리, 시스템 모니터링 및 유지보수 등) 등을 고려하여 스스로의 환경에 맞는 최대 접속시간을 각각 정하여 시행할 수 있습니다.

(예를 들어, DB 운영·관리자일 때에는 10분 등)

최대 접속시간은 최소한으로 정하여야 하며 장시간 접속이 필요할 때에는 접속시간 등 그 기록을 보관·관리 하여야 합니다.

Q19

망분리 의무화 대상 사업자의 기준은?

⇒ 망분리를 하여야 하는 정보통신서비스 제공자등은 다음과 같습니다.

- ① 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상(제공하는 정보통신서비스가 다수일 때에는 전체를 합산하여 적용)
- ② 정보통신서비스 부문 전년도(법인일 때에는 전 사업연도를 말한다) 매출액이 100억원 이상(정보통신서비스와 그 외 서비스를 함께 제공할 때에는 정보통신서비스 부문을 합산한 매출액만 적용)

Q20

망분리 의무화 대상 개인정보취급자 단말기는?

⇒ 정보통신서비스 제공자등이 망분리를 할 때에는 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자(예시 : 데이터베이스 운영관리자)의 컴퓨터 등을 인터넷망으로부터 분리하여야 합니다.

Q21

온라인과 오프라인으로 서비스를 제공하고 있는 업체입니다. 오프라인으로만 수집한 고객의 개인정보가 100만명 이상이면 망분리를 적용해야 합니까?

⇒ 오프라인으로 수집한 고객의 개인정보도 온라인으로 서비스 된다면 이 기준을 이행하여야 합니다.

따라서, 수집 경로와 상관없이 정보통신서비스 부문에서 수집한 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 고객 수가 일일평균 100만명 이상일 때에는 망분리를 하여야 합니다.

Q22

망분리 방식에 세부 기준은 없습니까?

⇒ 이 기준 [부록] ‘정보통신서비스 제공자등을 위한 망분리 해설’ 등을 참고하시기 바랍니다.

Q23

소량의 개인정보를 다운로드하는 개인정보취급자도 망분리 대상인지요?

⇒ 망분리 적용 대상 여부는 개인정보를 다운로드하는 건수로 정하고 있지 않습니다. 따라서 망분리 적용 대상 정보통신서비스 제공자에 해당하는 이상 소량의 개인정보를 다운로드하는 개인정보취급자의 컴퓨터도 망분리 하여야 합니다.

Q24

오픈마켓 서비스에 상품을 등록·판매하는 판매업자도 반드시 망분리를 하여야 합니까?

⇒ 오픈마켓 서비스 제공자가 망분리 대상 사업자인지 여부와는 무관하게 오픈마켓 서비스에 상품을 등록·판매하는 판매업자가 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나

정보통신서비스 부문 전년도 매출액이 100억원 이상인 경우에는 망분리를 적용하여야 합니다.

Q25

오픈마켓 서비스 제공자가 정보통신망을 통해 오픈마켓 서비스에 상품을 등록·판매하는 판매업자에게 판매정보를 제공하는 경우 취해야 할 보호조치는?

⇒ 오픈마켓 서비스 제공자는 판매업자가 정보통신망을 통해 외부에서 개인정보 처리시스템에 접속이 필요할 때에는 사용자계정(ID)과 비밀번호를 입력하여 정당한 개인정보취급자 여부를 식별·인증하는 절차 이외에 본 해설서에서 안내하는 제4조 제4항에 따른 추가적인 인증수단을 적용하여야 합니다.

Q26

비밀번호와 관련된 다른 조치(5회 이상 비밀번호 입력 오류시 로그인 제한 등)를 적용할 때에도 개인정보취급자의 비밀번호 작성규칙은 반드시 8자리 또는 10자리로 이상으로 해야 하나?

⇒ 이 기준에서는 개인정보취급자를 대상으로 영문자(영대문자, 영소문자), 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성하도록 정하고 있으므로 이행하여야 합니다.

Q27

개인정보 수집이 필요한 웹기반 시스템을 개발 중인데 일방향 암호화를 어떻게 적용하라는 의미인지요?

⇒ 웹기반 시스템의 DB에 이용자의 비밀번호가 평문으로 저장되어 이용자가 입력한 비밀번호와 단순 비교하는 방식으로 인증 시스템 개발이 되지 않아야 한다는 의미입니다. 다시 말해, 개발 시 상용 암호 모듈을 이용하여 적용하는 방법, 자체 DB 시스템에서 제공하는 암호 모듈 활용 방법, 공개용 암호 라이브러리 등을 사용하여 프로그램을 직접 개발하는 방법이 있는데 이들 모두 일방향(해쉬 함수) 암호화 기능이 제공되는 라이브러리를 이용하여 개발하여야 합니다.

다만, 일방향 암호 알고리즘 중 보안수준이 떨어지는 MD5, SHA-1 등은 사용하지 않습니다.

Q28

비밀번호가 아닌 신용카드정보, 계좌정보 또는 기타 고객 정보도 일방향 암호화의 적용이 필요한가요?

⇒ 신용카드번호 및 계좌번호 등은 일방향(해쉬) 암호화하여 저장하지 않아도 되며, 본 해설서에서 권고하는 안전한 암호화 알고리즘으로 암호화하여 저장하면 됩니다.

Q29

개인정보취급자가 아닌 이용자의 접속기록은 보관하지 않아도 되나요?

⇒ 이용자의 접속기록 보관에 관한 사항은 이 기준에서 규정하고 있지는 않습니다.
다만, 이용자의 접속기록은 통신비밀보호법 제2조제11호마목 및 사목, 같은 법 시행령 제41조제2항제2호에 따라 3개월 이상 보관하여야 합니다.

통신비밀보호법

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

11. "통신사실확인자료"라 함은 다음 각목의 어느 하나에 해당하는 전기통신사실에 관한 자료를 말한다.
 - 마. 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료
 - 사. 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료

제15조의2(전기통신사업자의 협조의무) ① 전기통신사업자는 검사·사법경찰관 또는 정보

수사기관의 장이 이 법에 따라 집행하는 통신제한조치 및 통신사실 확인자료제공의 요청에 협조하여야 한다.

- ② 제1항의 규정에 따라 통신제한조치의 집행을 위하여 전기통신사업자가 협조할 사항, 통신사실확인자료의 보관기간 그 밖에 전기통신사업자의 협조에 관하여 필요한 사항은 대통령령으로 정한다.

통신비밀보호법 시행령

제41조(전기통신사업자의 협조의무 등) ① 법 제15조의2에 따라 전기통신사업자는 살인·인질강도 등 개인의 생명·신체에 급박한 위험이 현존하는 경우에는 통신제한조치 또는 통신사실 확인자료제공 요청이 지체없이 이루어질 수 있도록 협조하여야 한다.

- ② 법 제15조의2제2항에 따른 전기통신사업자의 통신사실확인자료 보관기간은 다음 각 호의 구분에 따른 기간 이상으로 한다.

2. 법 제2조제11호마목 및 사목에 따른 통신사실확인자료 : 3개월

Q30

개인정보처리시스템에서 개인정보의 출력시 용도에 따른 출력항목의 최소화가 무엇을 의미하는지?

⇒ 정보통신서비스 제공자등의 업무 수행 형태 및 목적, 유형, 장소 등 여건 및 환경에 따라 개인정보처리시스템에 대한 접근권한 범위내에서 최소한의 개인정보를 출력하도록 조치하라는 것입니다.

참 고

☞ 출력 시 주의사항

- * 오피스(엑셀 등)에서 개인정보가 숨겨진 필드 형태로 저장되지 않도록 조치
- * 웹페이지 소스 보기 등을 통하여 불필요한 개인정보가 출력되지 않도록 조치 등

Q31

정보통신서비스 제공자등은 개인정보를 의무적으로 마스킹 처리하여야 합니까?

⇒ 고시 제10조 및 관련 해설 내용은 정보통신서비스 제공자등이 이용자의 개인

정보 보호를 위해 개인정보를 마스킹 하여 표시하는 조치를 취할 때 마스킹 방식에 관한 일관된 기준을 따를 수 있도록 권고하는 사항으로서 의무적으로 마스킹 처리를 적용해야 하는 것은 아닙니다.